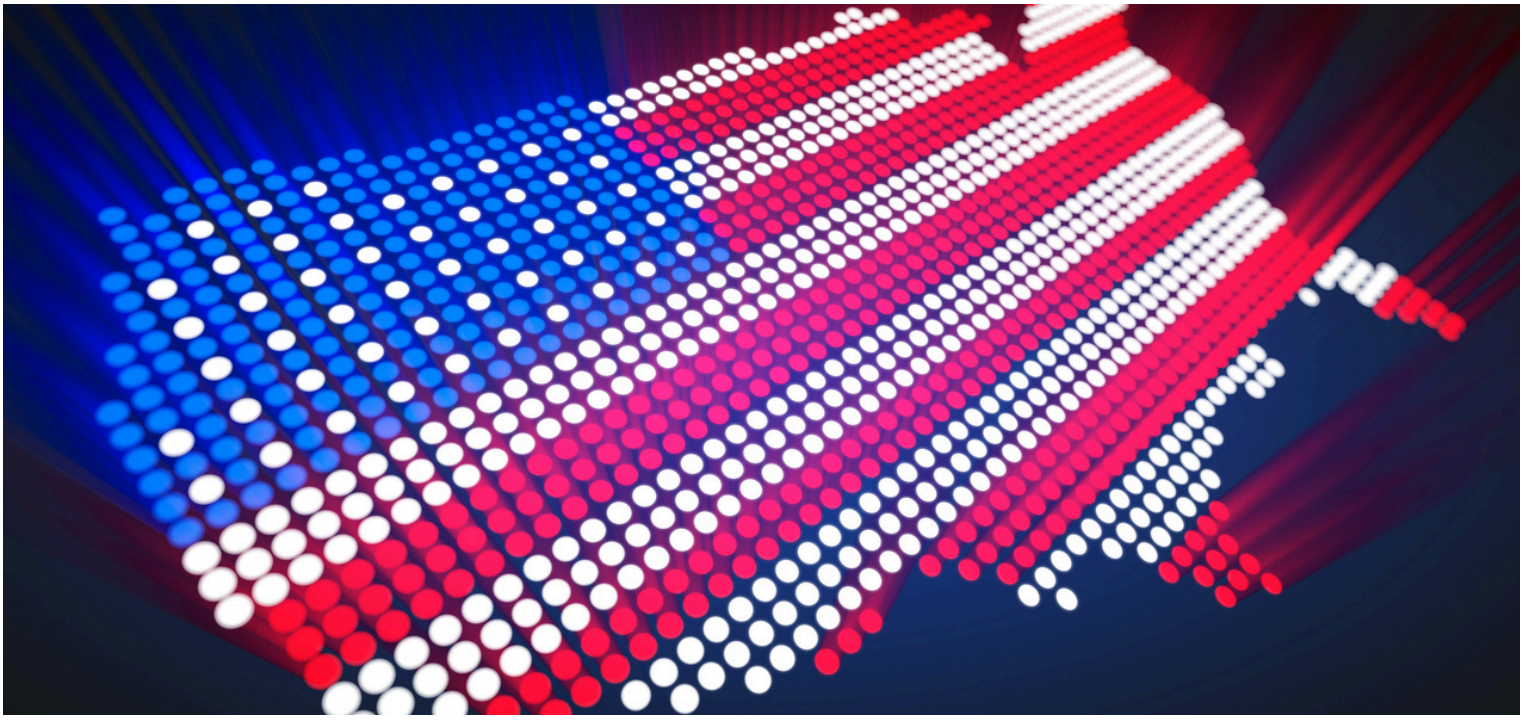
Apr 2024

USA: American Privacy Rights Act - Q&A

On April 7, 2024, U.S. Representative Cathy Rodgers and U.S. Senator Maria Cantwell introduced the American Privacy Rights Act 2024 (the Bill), aimed at establishing robust national data privacy standards with a focus on consumer control over personal information. In this Insight Q&A article, Billee Elliott McAuliffe and Jacquelyn H. Sicilia, from Lewis Rice LLC, delve into key provisions, limitations, and implications of this proposed legislation. They address frequently asked questions, offering valuable insights into how the Bill could reshape data privacy regulations in the US.



Henrik5000 / Signature collection / istockphoto.com

Which provisions of the Bill will have the biggest impact on businesses?

First, if passed, the Bill will have a significant impact on a majority of US businesses because most of these businesses have not yet had to comply with any of the international or 16 US state comprehensive laws (which will soon be 17 as Maryland's law has been passed by its legislature and is waiting for Governor action). The Bill, like nearly all of the international and US state comprehensive privacy laws that have been enacted, includes requirements for both data controllers (defined in the Bill as 'covered entities') and their service providers or processors. This means that even if a given entity does not fit the criteria for a covered entity, it could still be subject to the Bill because it provides services for a covered entity. This will result in millions of US businesses now being subject to a comprehensive privacy law. Therefore, the Bill could fundamentally change how most businesses in the US collect, use, and protect data.

Secondly, the inclusion of a private right of action in the Bill will undoubtedly have an important impact on how, how often, and in what manner this Bill is enforced. As proposed, the Bill may be enforced by the Federal Trade Commission (FTC), the State Attorneys General (AGs), and individual consumers. Including within the Bill, a right for individuals to bring privacy lawsuits against covered entities for violating the consumer's rights under the Bill is significant. Currently, California is the only state that includes a private right of action by consumers in its comprehensive privacy law, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (CCPA). Washington also has a consumer private right of action in its consumer health data privacy act, the Washington My Health My Data Act (MHMD). Having a right to pursue action to protect their own privacy and data protection rights will be something new for most Americans and could change the face of data protection in the US, just like the private right of action under the EU General Data Protection Regulation (GDPR) has been continually used to strengthen data protection in Europe.

Lastly, the explicit preemption language in the Bill will have a substantial impact on most businesses in the US. Thus far, 16 US states have enacted state comprehensive privacy laws with one more (Maryland) on its Governor's desk ready to be signed. While these state laws are largely similar, each contains nuances that have created a patchwork system of laws that can make compliance with more than one of them difficult for businesses engaged in interstate commerce. The clear preemptive intent language of Section 20 of the Bill could offer relief for these businesses. Within Section 20 of the Bill, the drafters directly address preemption by stating the purposes of the Bill is to provide a 'uniform national data privacy and data security standard in the United States' and to 'expressly preempt laws of a State or political subdivision thereof' covered by the Bill. From this language and additional commentary from House Energy and Commerce Committee Chair Cathy McMorris Rodgers and Senate Commerce Committee Chair Maria Cantwell, the two members of Congress who released the discussion draft of the Bill, it is clear that the drafters were intending to address some of the concerns raised about whether the language of the American Data Privacy and Protection Act (ADPPA), which was a comprehensive privacy bill proposed in 2022 that had strong support and even passed the House committee. However, key Congressional leaders, including Senator Cantwell and former House Speaker Nancy Pelosi, criticized the bill for many reasons including the lack of clarity around preemption.

Notwithstanding the clear statement about preemption, the Bill does contain a defined list of state laws that are not preempted. This list includes but is not limited to, consumer protection laws, civil rights laws, employee privacy rights laws, student privacy laws, data breach notification laws, contract or tort laws, criminal data privacy statutes, cyberstalking and blackmail laws, public safety law, wiretapping laws, and banking and financial records laws.

What are the limitations (if any) of the Bill, and which provisions would benefit from further clarification?

Certain US state and international privacy laws include heightened privacy protections for children. For example, the CCPA has a number of additional protections for children including an opt-in requirement for the sale of personal information of a consumer under the age of 16 with children aged 13 to 16 being able to provide their own opt-in, and parental opt-in being required for children under the age of 13. The Bill does not provide any type of more robust or heightened protections for children (beyond the impact assessment requirements for algorithms involving information related to minors and the prohibition of privacy action by a minor through mandatory arbitration). Of course, there are still other federal statutory protections for children, like the Children's Online Privacy Protection Act of 1998 (COPPA), that are still in effect. In fact, the Bill specifically states that nothing in the Bill will relieve or change any obligations related to COPPA. However, many critics have already indicated that the failure to include robust protections for children's privacy within the Bill is a significant hole in the compliance regime, especially given that children and minors are prolific users of technology and their personal information is being collected and used by many businesses without much oversight.

The Bill specifically grants the FTC rulemaking authority and even directs the FTC to provide guidance on a number of items. One such area where FTC guidance or regulations will be helpful involves the opt-out rights related to certain 'consequential decision-making' that uses an algorithm. Consequential decisions are determinations or offers, including through advertisements, that use personal data and relate to an individual's access to or equal enjoyment of housing, employment, education, healthcare, insurance, or credit opportunities, or access or use of public accommodation. Pursuant to Section 14 of the Bill, covered entities are to provide notice of such consequential decision-making and its potential outcomes and grant individuals the opportunity to opt out of the use of their personal data for such decision-making. However, it is unclear from the proposed language how this opt-out opportunity is to be presented to individuals or how the individual's choice is to be facilitated. Guidance from the FTC regarding this requirement would assist businesses in their compliance efforts.

In addition to the grant of rulemaking authority to the FTC, the Bill provides for the FTC to develop a couple of opportunities for covered entities to gain approval of their compliance efforts. In Section 15, a covered entity (which is not a large data holder or a data broker) may apply to the FTC for approval of its compliance

guidelines governing its collection, processing, retention, and transfer of personal data. These applications for approval must identify an independent organization responsible for administering the guidelines. Participation in approved guidelines gives the covered entity a rebuttable presumption of compliance with the Bill. Additionally, in Section 16, the FTC is required to establish a pilot program for entities to deploy privacy-enhancing technologies as part of their data security measures. These entities may petition to be accepted with privacy-enhancing technology that meets or exceeds the data security requirement of the Bill. Participation in the pilot program also entitles the covered entity to a rebuttable presumption of compliance with the Bill's data security requirements.

How would the Bill interact with the Executive Order on preventing access to sensitive personal and government-related data?

As proposed, the Bill would work in tandem with the Executive Order to prevent access to sensitive personal and government-related data (the Executive Order). In fact, the Bill explicitly states that it will not limit the authority of any other Executive agency or federal law or regulation (other than the FTC's Rulemaking on Commercial Surveillance and Data Security which is to be specifically terminated on the date of enactment of the Bill). The Executive Order is intended to limit and restrict foreign 'countries of concern' from getting access to and using Americans' sensitive personal data and government-related data. In the Executive Order, the President indicates that these countries of concern 'rely on advanced technologies, including artificial intelligence (AI), to analyze and manipulate bulk sensitive personal data to engage in espionage, influence, kinetic, or cyber operations or to identify other potential strategic advantages over the United States. Countries of concern can also use access to bulk data sets to fuel the creation and refinement of AI and other advanced technologies, thereby improving their ability to exploit the underlying data and exacerbating the national security and foreign policy threats.' To prevent these countries of concern from getting this sensitive personal or government-related data, the Executive Order requires the U.S. AG and the Department of Justice (DOJ) to issue regulations that prohibit or restrict US businesses from engaging in transactions with foreign countries or their nationals involving bulk sensitive personal data or government-related data. The Bill requires covered entities to state in their privacy policies whether any covered data is made available to any 'foreign adversary' as defined by the Secretary of Commerce in §7.4 of Title 15 of the Code of Federal Regulations. Presently, the Executive Order, along with the DOJ's framework (and the forthcoming regulations), would outright prohibit transactions with certain countries of concern unless certain security practices and/or licenses are in place. Under the Bill, covered entities are required to have certain levels of data security to protect covered data, regardless of whether they are dealing with a foreign adversary or not. Presumably, the DOJ regulations will have heightened requirements for countries of concern, which would include some or all foreign adversaries. As a result, if a covered entity wishes to provide covered data, including sensitive personal data or government-related data to one of the countries described as a foreign adversary and that country is also considered a country of concern, the covered entity would need to have appropriate safeguards in place in accordance with the Executive Order/DOJ regulations and disclose that the for-

eign adversary has access to the covered data in its privacy policy. This interaction between the Bill and the Executive Order is another area of the Bill where FTC guidance and regulations would be helpful to explicitly describe what will be expected of businesses who would like to enter into transactions with and/or provide data to these types of countries.

Are there any key similarities and/or differences to the ADPPA?

The Bill was clearly based on the ADPPA. Each of these proposed acts is based upon granting individuals certain consumer privacy rights and allowing the consumer to control how businesses collect and use their personal data. Crucial to these consumer privacy rights is the obligation for businesses (and their service providers) to be transparent about their privacy practices and each of these proposed regulations accomplishes this by including a requirement that all covered entities and their service providers prepare, and make available to the public, privacy policies detailing their data privacy and security practices. Data minimization is a fundamental component of each regulation, and both impose requirements for reasonable and appropriate security measures. Regarding enforcement, the Bill, like the ADPPA, allows for both federal and state enforcement actions, and each includes a private right of action for consumers. Lastly, both regulations provide for federal preemption of state and law privacy laws and grant the FTC rulemaking authority.

There are, however, key differences between the Bill and the ADPPA. The first is the preemption provisions. Section 20 of the Bill directly addresses preemption by stating the purposes of the Bill are to provide a 'uniform national data privacy and data security standard in the United States' and to 'expressly preempt laws of a State or political subdivision thereof.' Critics of the ADPPA raised questions as to whether or not it preempted state law, especially the CCPA. Section 20 makes the intent clear that the Bill is meant to preempt all other comprehensive privacy laws in the US.

Another key difference between these two proposed laws relates to impact assessments. Privacy impact assessments in the data privacy context are basically a requirement that businesses take an in-depth look into the risks and benefits of certain higher-risk activities (or algorithms) before engaging in those activities. If, after taking into account all of the security measures and other protections that the business will implement regarding the given processing, the risks to the individual providing their data (risks like identity theft, consequences from the release of sensitive data (like health information or biometric data, risks of discrimination, etc.) are higher than the benefits to the business of the given activity, the business is not to engage in the given activity. Under the ADPPA, impact assessment were required when the activity/algorithms posed a 'consequential risk of harm' without a whole lot of detail as to what constituted a consequential risk of harm. This lack of specificity was questioned by many critics as holding the potential for being overly burdensome which could, in turn, restrict innovation. The Bill addresses that lack of specificity by requiring impact assessments for algorithms that post a consequential risk and also adding five specific categories of algorithms for which businesses must perform impact assessments; thus, giving us examples of the lens of consequential

risk through which to view other activities when determining whether or not the business is required to perform an impact assessment. The five delineated categories are algorithms involving minors, housing, education, employment, healthcare, insurance, or credit opportunities, public accommodations based on protected characteristics (e.g., race, color, religion, national origin, sex, or disability), disparate impacts based on race, color, religion, sex, or disability, and disparate impact based on political party registration. In addition to the impact assessment requirements, the Bill also includes a requirement that businesses offer consumers the right to opt out of algorithms for consequential decisions related to housing, employment, education, health care, insurance, credit, or access to places of public accommodation (a subset of those algorithms requiring impact assessments).

The language in the Bill surrounding the private right of action, which can be brought by the FTC, the US state AGs, and individual consumers, also reflects changes based upon criticisms of the ADPPA. The ADPPA provided a two-year grace period following passage before the private right of action applied. This was criticized. So, the Bill reduces the grace period to six months.

How would State-level enforcement and preemption work under the Bill?

As noted above, the Bill includes federal, state, and individual enforcement opportunities. The Bill authorizes enforcement by the states through the AG of the state, the consumer protection office of the state, or any other office of the state authorized to enforce privacy or data security laws through civil action in an appropriate federal district court of the US. But, if one of those enforcement individuals brings an action, no other officer of that state may institute a civil action against the same defendant for the same violation of the Bill or under any regulation promulgated thereunder. If a state official is going to bring an action, it must notify the FTC prior to initiating the action. States may seek injunctive relief, civil penalties, damages, restitution, and other compensation. There are provisions for recovery of attorneys' fees and other litigation costs. Since this is part of the law, it is not covered by preemption and since consumer protection laws are specifically exempted from the preemption, there may be the possibility for the state officials to also bring actions under their own consumer protection statutes.

As the Bill was just unveiled what are the next steps and likelihood that the Bill will pass?

The Bill is presently in the draft stages. It has yet to be officially introduced, and there does not appear to be an official date to do so. However, given the quickly approaching presidential election in November, it is likely that House Committee on Energy and Commerce Chair Cathy McMorris Rodgers and Senate Committee on Commerce, Science and Transportation Chair Maria Cantwell will move quickly to get this ready for a vote. Unlike the ADPPA, which did not have support from Senator Cantwell, this Bill was drafted bipartisan and bicameral. The draft Bill already appears to have bipartisan support and, as discussed above, addresses

several of the issues in the ADPPA related to broad language on AI technologies and the grace period given before the private right to action. The Bill, though, still targets big tech and creates regulations around data minimization and consent requirements which were other areas of concern with the ADPPA. There is a strong chance this Bill will pass, but timing may be the biggest obstacle to its passage.

Additional comments

There are a couple of other points worth mentioning.

First, the patchwork of state comprehensive privacy laws has been split on whether these laws would cover nonprofits. This Bill would include certain nonprofits under 'covered entities.' Small businesses (businesses having $40 million or less in any revenue, processing 200,000 or fewer individuals, and do not earn revenue from the transfer of personal data to third parties), Federal, State, Tribal, territorial, and local governments, entities working on behalf of governments, the National Center for Missing and Exploited Children (NCMEC), and, except for data security obligations, fraud-fighting non-profits are also excluded. Second, the Bill will require covered entities to designate at least one employee as a privacy or data security officer. Large data holders will be required to have both a privacy and a data security officer as well as make annual certifications with the FTC. This is a new concept for US-based comprehensive privacy laws.

In an effort to ensure the rights of consumers are protected, the Bill prohibits most arbitration agreements from interfering with the Bill and the privacy rights of consumers. This means that contracts may not include mandatory arbitration provisions that can be used as a means of circumventing the enforcement of the Bill or any action to enforce it. Lastly, the Bill is set to take effect 180 days after enactment. The GDPR came into effect more than two years after it was passed. Most of the US state comprehensive laws have had at least a year for businesses to make the necessary compliance changes before their provisions become enforceable. The 180-day period in the Bill is a very short period for businesses to take all of the steps necessary to provide appropriate notices to consumers and to implement the processes and procedures necessary to comply with the Bill, especially to effect consumer rights requests like deletion of all of an individual's personal data. This means that businesses should follow this Bill very carefully and be ready to act promptly if it is enacted.

Billee Elliott McAuliffe Cybersecurity & Data Privacy Practice Group Leader
bmcauliffe@lewisrice.com
Jacquelyn H. Sicilia Associate
jsicilia@lewisrice.com
Lewis Rice LLC, Missouri