How Federal Data Privacy Bill Would Affect Businesses

By **Brandon N. Robinson and Kelsi Long** (July 6, 2022)

Brandon N. Robinson

Kelsi Long

On June 3, Sen. Roger Wicker, R-Miss., and Reps. Frank Pallone, D-N.J., and Cathy McMorris Rodgers, R-Wash., released a bipartisan discussion draft of a comprehensive federal privacy framework entitled the American Data Privacy and Protection Act.[1]

After a June 14 hearing, the act was introduced as H.R. 8152 on June 21.[2] Following the committee's markup session on June 23, the subcommittee voted favorably to introduce an amendment as substitute to the full committee.[3]

The following represents a detailed summary as well as thoughts on its impacts on businesses and current compliance with other laws.

Title I — Duty of Loyalty

The duty of loyalty addresses data minimization by limiting the collection, processing and transfer of covered data to that which is reasonably necessary, proportionate and limited to the information needed to provide requested products or services.

Title I includes restricted and prohibited data practices regarding the processing of certain sensitive information, e.g., social security numbers, biometric and genetic information, sexual orientation information, geolocation information, calendar information on a device, or physical and mental health information.

Privacy by design requires reasonable policies, practices and procedures regarding data collection, processing and transfer that consider mitigating certain privacy risks in design, development and implementation, as well as privacy risks for individuals under the age of 17.

However, it allows for flexibility commensurate with the entity's size, the complexity of its activities, the number of individuals/devices involved and other factors.

Finally, Title I defines loyalty in regard to pricing by prohibiting businesses from conditioning pricing or availability of a product or service on an individual's agreement to waive privacy rights protected by the act, with exceptions related to billings and collections, loyalty discount programs and market research.

Title II — Consumer Privacy Rights

Title II sets out various individual rights protected by the act, and requires the Federal Trade Commission, following enactment, to publish on its website such rights as well as related remedies, exemptions and protections. These rights include:

Transparency

The entity must publish "in a clear, conspicuous, and readily accessible manner," a privacy policy describing its information activities. The act specifies content to be included and in

what languages, as well as how notifications of material changes must be made.

At a minimum, the policies must notably include instructions for exercising privacy rights, description of data security and privacy practices, and if information is processed in Russia, Iran, China or North Korea, among other requirements.[4]

Individual Data Ownership and Control

Entities must provide verified individuals the right to request access, correction, deletion and portability of covered data.

For large data holders, this must be done within 30 days from verification of the request. Small data holders have 90 days, and all other covered entities have 60 days.

Right to Consent and Object

Entities may not collect, process or transfer to a third party any sensitive covered data without affirmative express consent, which can be withdrawn.

Individuals may also opt out of covered data transfers and targeted advertising.

Data Protection for Children and Minors

Entities may not, with actual knowledge, engage in targeted advertising to minors under the age of 17, nor transfer their covered data without affirmative express consent of the minor's parent or guardian.

The act also establishes the FTC's Youth Privacy and Marketing Division for addressing the privacy of and marketing directed at children and minors, and requires congressional reports from the division and the FTC inspector general.

Third-Party Collecting Entities

Third-party collecting entities must register with the FTC and have clear and conspicuous notices on websites and mobile apps that: identify themselves as such, and include a link to a searchable registry to be developed by the FTC that includes a "do not collect" link, whereby the FTC can direct all such entities to delete covered data and discontinue collection of covered data without affirmative express consent.

Exceptions exist for service providers.

Civil Rights and Algorithms

Covered entities may not collect, process or transfer covered data in a manner that discriminates on the basis of certain civil rights, with certain exceptions. Large data holders are required to annually conduct assessments of its algorithms for any discriminatory impacts related to:

- Minors;
- Advertising for housing, education, employment, health care, insurance or credit opportunities;

- Determining access to or restrictions on the use of public accommodations, particularly related to protected characteristics; and

- Disparate impacts on protected statuses.

Such assessments must be submitted to the FTC. The FTC shall examine best practices for such assessments and remedies.

Data Security and Protection of Covered Data

Covered entities must maintain reasonable administrative, technical and physical data security practices and procedures to protect against unauthorized access and acquisition, that take into account certain specified considerations.

Covered entities subject to and in compliance with the Gramm-Leach-Bliley Act or the Health Information Technology for Economic and Clinical Health Act shall be deemed in compliance.

Unified Opt-Out Mechanisms

The FTC must issue regulations that create one or more acceptable centralized privacy protection mechanism — i.e., browser or device privacy settings — for individuals to opt out through a single interface for the covered entity.

Exceptions and Exemptions

General Exceptions

Notwithstanding these restrictions and obligations, a covered entity may collect, process or transfer data if reasonably necessary, proportionate and limited to initiating or completing a requested transaction or order, detecting or responding to a security incident, and conducting a product recall, among others.

Small Business Exceptions

A covered entity may be exempt from the portability request requirement and certain data security requirements, does not have to designate a privacy and data security officer, and — at its sole discretion — may comply with the correction requests by deleting the data entirely if it can establish that:

- Its average annual gross revenues during the last three years did not exceed $41 million;

- It did not annually collect or process covered data of more than 200,000 individuals beyond fulfilling transactions and data is deleted within 90 days; and

- It did not derive more than 50% of revenue from transferring covered data during any year.

Title III — Corporate Accountability

Designated employees must implement privacy and security compliance programs.

Officers of large data holders have specific executive reporting, auditing or internal controls and training obligations, and must conduct biennial privacy impact assessments with specified requirements.

Service Providers and Third Parties

The act restricts service providers and third parties with respect to data minimization, transfer and retention.

Covered entities may exercise reasonable due diligence subject to FTC guidance on selecting a service provider or transferring covered data to a third party, but as long as the covered entity complies with the act when transferring data, then it will be not liable for service providers' violations.

Technical Compliance Programs and Compliance Guidelines

The FTC must establish a process for the proposal and approval of technical compliance programs used by covered entities specific to any technologies, products, services or methods to collect, process or transfer covered data.

Similarly, a covered entity may apply to the FTC for approval of one or more sets of compliance guidelines.

Digital Content Forgeries

The FTC must report on digital content forgeries, including definitions and descriptions, assessments of uses, application and harms, methods and standards to identify them, countermeasures, and other information.

Although not defined, digital content forgeries are commonly understood as the process of manipulating documents, images or other content for financial, social or political gain.

With the growth of artificial intelligence applications and capabilities, sophisticated digital content forgeries such as deepfakes have experienced significant growth, as well as increased attention and concern.

Title IV — Enforcement, Applicability and Miscellaneous

Enforcement

The act establishes a new FTC bureau for enforcing this act. Violations shall be treated as unfair or deceptive acts or practices.

It also establishes a victim relief fund, into which civil penalties shall be deposited, to provide redress, payments, compensation or other monetary relief to certain individuals that cannot be located, or where payment through other means may not be practicable.

The act also provides for enforcement by state attorneys general or consumer protection officers, in coordination with the FTC.

Finally, the act provides for a private right of action, beginning four years after enactment.

To bring an action, one must give written notice to the company — applies only to small data companies or if a person is seeking injunctive relief — or send a demand letter to the company if a person is seeking monetary damages and notify the FTC and their state attorney general of the desire to bring suit.

The act also restricts and prohibits the ability of predispute arbitration agreements or joint action waivers to limit rights.

Preemption

This act does not preempt several federal laws, including existing FTC authority, Federal Communications Commission security breach rules on common carriers, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health, the Family Educational Rights and Privacy Act, the Fair Credit Reporting Act, and other specified federal laws and regulations.

States may not enact future laws that are covered by this act or FTC regulations, but the act does not preempt certain state laws such as fraud, personal injury/wrongful death and data breach notification.[5]

Contrastingly, Pallone made clear in the subcommittee meeting that these exceptions will be changing before the final draft. However, he did not make any statements to which specific exceptions will be eliminated.

Implications for Businesses

The act places significant obligations on businesses, particularly those that are not currently subject to European privacy law or state comprehensive privacy laws such as the California Consumer Privacy Act, or CCPA, and the California Privacy Rights Act — or those soon to be in effect in states such as Colorado, Connecticut, Virginia and Utah.

Even those subject to such laws may have to add key aspects into their privacy policies and procedures, such as requirements to:

- Publish annual impact assessments disclosing methods taken to minimize data risks, particularly with respect to algorithms.
- For certain businesses, appoint a data security or privacy officer.
- Modify privacy policies to ensure required information is disclosed, and make the policy available in applicable languages.
- Conduct audits to ensure reasonable internal controls related to individual's data and compliance with the act.

In theory, businesses operating in multiple states might welcome a unified federal privacy law on some issues, as opposed to managing compliance with multiple similar but differing state laws.

Unfortunately, the preemption section is limited and does not provide the relief from multiple laws, such as data breach notification, that one might expect could be harmonized.

It should be noted that three representatives supported refining customer loyalty programs, stating that individuals shouldn't be discriminated against for choosing to exercise one of their privacy rights. If refined, the outcome could be that businesses cannot offer loyalty programs incentivizing individuals to share data.

Further, while the act does make exceptions for small businesses discussed above, the statutory language is unclear as to whether a business must meet one or all three criteria to qualify for the exemption.[6]

Similar applicability criteria in comprehensive state laws such as the CCPA would suggest that business must meet all three, but it is possible that later drafts of the bill may clarify this question.[7]

Another significant impact pertains to the private right of action.

Many state data breach notification and comprehensive privacy laws may only be enforced by the state attorney general. In contrast, the act allows for a private right of action as well as state enforcement, but requires significant preliminary steps and coordination with the FTC, and so this represents compromise as well.

Conclusion

In summary, the act represents a significant, although nuanced and compromised, step toward the protection of individual privacy rights at the federal level.

This bipartisan effort indicates more momentum toward such a goal than we have seen in several years, but one should expect additional amendments and refinements as it works its way through passage, with significant deference toward FTC rulemaking if enacted.

Brandon N. Robinson is a partner and Kelsi Arrinel Long is an attorney at Balch & Bingham LLP.

[1] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (as submitted for discussion, June 3, 2022).

[2] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (as reported by the House Comm. on Energy and Commerce, June 21, 2022).

[3] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (as forwarded from subcommittee to full committee, June 23, 2022).

[4] Such other requirements include: (i) Business name and contact information for questions; (ii) Business name and contact information for any parent, subsidiary, or affiliate that is transferred a person's data; (iii) Categories of data collected and processed and the purpose for each category; (iv) Duration of time for retaining the data; (v) Whether data is transferred to a third party and its identity and the purpose; and (vi) the effective date of

the policy.

[5] Preemption also does not apply to the following: (i) General consumer protection; (ii) Civil rights; (iii) Student and employee privacy; (iv) Contract or tort law; (v) Criminal laws governing fraud, theft (including identity theft), unauthorized access to electronic devices, and similar provisions; (vi) Cyberstalking, cyberbullying, nonconsensual pornography or sexual harassment; (vii) Public safety or sector specific laws unrelated to privacy or security; (viii) Criminal public records; (ix) Banking or financial records, tax records, social security numbers, credit cards, credit reporting and repairs, etc.; (x) Facial recognition, electronic surveillance, wiretapping and telephone monitoring; (xi) Illinois's Biometric Information Privacy Act (BIPA) and Genetic Information Privacy Act (GIPA); (xii) Unsolicited e-mail messages, telephone calls, or caller ID; (xiii) Health and medical information and records, HIV status or testing; and (xiv) Confidentiality of library records.

[6] Specifically, section 209(a)(1) of the bill states that a covered entity or service provider is partially exempt if it "can establish that it met the requirements described in paragraph 2" for the three preceding calendar years. Section 209(a)(2) simply states that "the requirements of this paragraph are … the following", and includes neither "and" nor "or" after the second criteria.

[7] Under CCPA, a covered entity is subject to CCPA if it "does business" in CA and meets any of the following: (a) gross annual revenue of over $25 million; (b) bus, receives, or sells personal information of over 50,000 California residents, households or devices; or (c) derives 50% or more of annual revenue from selling California residents' personal information. Therefore, if meeting any of these criteria would make a business subject to CCPA, a similar approach would be require a business to meet all three Congressional criteria in order to be exempt. However, it is not clear that Congress intended to follow this same approach.