Scope of the draft American Data Privacy and Protection Act

By IAPP Managing Director, D.C., Cobun Zweifel-Keegan, CIPP/US, CIPM, and IAPP Westin Research Fellow Amy Olivero

On June 21, the American Data Privacy and Protection Act, a federal comprehensive data privacy bill, was introduced in the House by Reps. Frank Pallone, D-N.J., Cathy McMorris Rodgers, R-Wash., Janice Schakowsky, D-Ill., and Gus Bilirakis, R-Fla. The legislation was voted out of the House Energy and Commerce Committee on July 20.

The current draft bill divides covered organizations into categories that determine their compliance obligations. Depending on their size, "covered entities" may have enhanced ("large data holders") or relaxed ("small businesses") compliance requirements. The bill also specifies requirements based on an organization's relationship to covered data, such as whether it was a "third party," "third-party collecting entity" or "service provider."

As the bill continues its way through the legislative process, tracking how the bill applies to different types of organizations helps us understand how policymakers are thinking about the privacy landscape.

This IAPP table aims to present a high-level breakdown of the bill's structure and a snapshot of how various types of covered entities are mentioned in each section of the bill. A check mark (✓) indicates explicit coverage for the entity type. A plus (+) or minus sign (−) indicates additions or subtractions in prescribed requirements compared with other entity types. "X" (✗) indicates an explicit exemption. An empty cell indicates the entity type is likely to be required to comply with the section's requirements (as a "covered entity," in general).

	Covered entity (in general)	Small business	Large data holder	Third-party collecting entity	Service provider	Third party
TITLE I—DUTY OF LOYALTY						
Section 101. Data minimization.	✓				− Only mentioned in 101(d), prohibiting deceptive marketing.	
Section 102. Loyalty Duties.	✓				−	
Section 103. Privacy by design.	✓				✓	
Section 104. Loyalty to individuals with respect to pricing.	✓				− Not mentioned.	
TITLE II—CONSUMER DATA RIGHTS						
Section 202. Transparency.	✓		+ Log of material changes to privacy policy. Short-form notice.		− Not mentioned in (likely exempted from) from 202(a) "readily accessible" policy, (e) material changes, and (f) short-form notice.	
Section 203. Individual data ownership and control.	✓ Rights of access, correction, deletion and portability. Timing: No more than 60 days from request verification.	− No portability; correction requests can be deleted instead. Timing: No more than 90 days from request verification.	+ Timing: No more than 45 days from request verification. Annual report of request metrics.	+ Timing for deletion requests via Do Not Collect Registry, Section 206 (b)(3)(c): 30 days.	✗ Exempt, but must assist covered entity in fulfilling request.	
Section 204. Right to consent and object.	✓				− Exempt from 203(a) and (b), but must assist covered entity in fulfilling request. Targeted advertising opt-out rights still apply.	✗
Section 205. Data protections for children and minors.	✓		+ Lower knowledge standard ("knew or acted in willful disregard").		− Unclear. Specified only in exception for data related to missing and exploited children.	
Section 206. Third-party collecting entities.	✗	✗	✗	✓	✗	✗
Section 207. Civil rights and algorithms.	✓		+ Must conduct algorithm impact assessments.		✓	
Section 208. Data security and protection of covered data.	✓	− Exempt, except for retention and deletion rules.	+ Bug bounty requirement.		+ Delete/return covered data to covered entity.	
Section 209. Small business protections.	✗	✓	✗	✗	✗	✗
Section 210. Unified opt-out mechanisms. (Once established by FTC.)	✓				✓	
TITLE III—CORPORATE ACCOUNTABILITY						
Section 301. Executive responsibility.	✓ Must designate privacy and security officers if more than 15 employees. Privacy impact assessment every 2 years.	✗	+ Annual certification by CEO, privacy officer and data security officer. One officer must report directly to CEO and sign off on biennial privacy impact assessment. Also implement review process and training program, maintain records, and serve as point of contact with regulators.		− Must designate privacy and security officers if more than 15 employees. Not mentioned in 301(e), biennial privacy impact assessment.	
Section 302. Service providers and third parties.	+ Contracts required between covered entities and service providers. Reasonable due diligence in decisions relating to service providers and third parties.				+ Processing limited to direction of covered entity. Must demonstrate compliance to covered entity upon request.	+ Processing limited to purposes disclosed by covered entity. If sensitive data, must have consent or purposes 101(b) (1), (3) or (5).
Section 303. Technical compliance programs.	✓				− Not mentioned.	
Section 304. Commission-approved compliance guidelines.	✗	✓	✗	✗	✗	✗

Published September 2022

iapp.org