ML STRATEGIES

Understanding the American Data Privacy and Protection Act

June 08, 2022 | | By **Christian Tamotsu Fjeld**, **Cynthia J. Larose**

On Friday, June 3, Representative Frank Pallone (D-NJ), Chairman of the House Energy & Commerce Committee, Representative Cathy McMorris Rodgers (R-WA), the committee's Ranking Member, and Senator Roger Wicker (R-MS), Ranking Member of the Senate Commerce, Science and Transportation Committee, released to the public a draft discussion federal privacy bill. The "American Data Privacy and Protection Act" (ADPPA) is a comprehensive bill that touches all facets of the privacy debate that has been ongoing in Congress for well over 20 years. Some of the provisions in the discussion draft are bracketed, indicating those provisions are still under discussion and are not subject to agreement between the authors. In their press release, the three authors thanked Consumer Protection and Commerce Subcommittee Chair, Jan Schakowsky (D-IL), and Ranking Member Gus Bilirakis (R-FL), as well as Members of the Senate Commerce Committee for their input and leadership on the discussion draft. However, of note, Senator Maria Cantwell (D-WA), the Chair of the Senate Commerce Committee, is not an author of the bill.

Last Congress, Senator Cantwell introduced the **Consumer Online Privacy Rights Act**, which was cosponsored by Senators Schatz, Klobuchar and Markey. While the bipartisan, bicameral ADPPA is ambitious and comprehensive, reflecting bipartisan agreement on crucial issues hereto elusive to compromise, its prospects for moving forward remain unclear. And without Senator Cantwell's support, the discussion draft's fate in the Senate is further complicated.

The House Energy & Commerce Committee is scheduled to hold a full committee legislative hearing next Tuesday, June 14, on the American Data Privacy and Protection Act. Christian Fjeld, ML Strategies Vice President, and former Senior Counsel and subcommittee staff director of the Senate Commerce Committee prepared a detailed summary of the bill.

1. Scope:

The scope of the discussion draft is striking and categorizes affected data and entities into tiers or subsets. The bill generally defines "covered data" as any "information that identifies or is linked or reasonably linkable to an individual or a device", which includes "derived data" and "unique identifiers", which would include persistent digital markers such as cookies and IP addresses. In addition, the discussion draft delineates a subset of "sensitive covered data" which includes information such as government identifiers (*e.g.*, social security numbers and drivers' license numbers), as well as sensitive categories such as health, geolocation, financial, log-in, racial, and sexual information. Sensitive covered data also covers, among other things, private communications, personal digital media such as photos and videos, and, notably, web-browsing activity. The Federal Trade Commission (FTC) is authorized to add additional categories of data to the definition of sensitive covered data through rulemaking proceedings under the Administrative Procedures Act (APA).

In general, the bill applies to a "covered entity", which includes any entity that "collects, processes, or transfers covered data…" In so doing, the bill also identifies a subset of covered entities as "large data holder[s]", which is an entity with gross annual revenues of $250 million or more "and" has collected covered data on more than 5 million individuals or devices "or" has collected sensitive covered data on more than 100,000 individuals or devices. It's worth noting that the $250 million figure is bracketed, indicating that the authors of the draft have yet to reach a final agreement on that threshold figure. Moreover, the conjunctions "and" and "or" are also bracketed, indicating a lack of agreement on whether a large data holder must meet some or all of the above criteria.

2. Consent:

Within this regulatory scope, the discussion draft lays out numerous restrictions and requirements based on the nature of the data and entity. Under section 203, all sensitive covered data is subject to "opt-in" consent by individuals. That is, a covered entity may not "collect or process" such data, nor transfer such data to a third-party, without first receiving an individual's "affirmative express consent". With regard to covered data that is not sensitive, an individual has the right to "opt out" of a covered entity transferring that data to a third party. Individuals also have the right to opt out of receiving targeted advertising. In addition to establishing these specific opt out rights, section 210 of the discussion draft directs the FTC to study the feasibility of a "unified opt-out mechanism", which would allow "individuals to exercise all such [opt out] rights through a single interface". Such a mechanism might include a "do-not-track" feature on a web-browser or refer to self-regulatory opt-out regimes offered in the online marketplace, or perhaps an acceptance of the emerging **Global Privacy Controls** as seen recently in California. Notably, if the Commission determines that such a unified opt-out mechanism is feasible, the bill directs the FTC to promulgate a rule under the APA that designates such a mechanism.

3. Children and Minors:

Section 205 of the discussion draft expressly prohibits serving targeted advertisements to youth under the age of 17. Furthermore, it prohibits the transfer of covered data on individuals aged 13 – 17 without opt-in consent. These prohibitions apply to covered entities that have "actual knowledge" (which is bracketed) that the targeted individuals are underage. It's worth noting that the **Children's Online Privacy Protection Act (COPPA)** applies to internet services "directed to children under 13 years of age", and the FTC considers numerous factors, including actual knowledge, in determining whether an entity is covered under COPPA. Furthermore, COPPA prohibits the *collection* of information from children under 13 without parental consent. Section 205 of the bill only places restrictions on the *use* of data collected from 13 – 17 year olds, *i.e.*, serving targeted ads and transferring data to third-parties.

4. Data Brokers:

Section 206 of the discussion draft places specific obligations, including third party audits on data disclosure practices, on "third-party collecting entities" colloquially known as data brokers. Such entities must inform individuals on their website or mobile application that they are data brokers, and large data brokers that process information on more than 5,000 individuals – which is in brackets – must register with the FTC. The Commission, in turn, shall establish a searchable public registry of all data brokers and provide individuals with the ability to request that all of their data be deleted by the registered entities. The data brokers must comply with this request within 30 days, which is bracketed. Failure to register will be met with penalties, not to exceed $10,000 per year and a "pay back" of the registration fees due ($100 per year) for each year it failed to register.

5. Civil Rights and Algorithmic Decision-making:

Under section 207, the discussion draft broadly prohibits the collection, processing, or transfer of covered data "in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the bases of race, color, religion, national origin, gender, sexual orientation, or disability." This provision is not tied to existing civil rights laws and, thus, may create a new federal prohibition on discriminatory practices. However, if the FTC becomes aware of discriminatory practices that are in violation of the subsection, the agency is directed to notify "any Executive agency with authority to initiate proceedings relating to such violation." This language seemingly confines federal enforcement actions to authority already wielded by relevant federal agencies.

In addition, section 207 requires large data holders to conduct annual "impact assessment[s]" on algorithms that large data holders use "solely or in part, to collect, process or transfer covered data…" This impact assessment must also "describe steps the large data holder has taken or will take to mitigate potential harms to an individual…" Such harms include those that affect youth under 17, advertising for various commercial activities, public accommodations, and any "disparate impact on the basis of an individual's or class of individuals' race, color, religion, national origin, gender, sexual orientation, of disability status." Any covered entity that "knowingly develops an algorithm" shall be required to "evaluate the design of the algorithm, including any training data used to develop the algorithm, to reduce the risk of the potential harms" identified above. This section also requires "to the extent possible" that independent and external auditors or researchers conduct these assessments and evaluations.

The FTC is directed to provide guidance on compliance with section 207 and is further granted APA rulemaking authority to establish the process by which large data holders can submit their impact assessments to the FTC.

6. Data Security:

Section 208 of the discussion draft establishes data security requirements on covered entities. Specifically, covered entities are required to "establish, implement, and maintain reasonable administrative, technical, and physical data practices and procedures to protect and secure covered data against unauthorized access and acquisition." In so doing, what constitutes reasonable data practices is dependent on the size and nature of both the covered entity and the covered data, similar to the factors the FTC considers under the **Safeguards Rule** pursuant to the Gramm-Leach-Bliley Act (GLBA). Furthermore, section 208 specifically requires covered entities to conduct vulnerability assessments, maintain preventive and corrective action plans, develop protocols for data retention and disposal, train employees on safeguarding data, and designate personnel to implement these policies. Finally, it's worth noting that GLBA and **Health Insurance Portability and Accountability Act (HIPAA)** covered entities do not receive a straight carve out under section 208. Rather, such entities are "deemed to be in compliance" with the bill if they are in compliance with those respective laws. Consequently, this will allow the FTC to bring enforcement actions against entities that are not in compliance with GLBA or HIPAA as violations of section 208 of the discuss draft.

7. Duty of Loyalty:

Under Title I and the heading "Duty of Loyalty", the discussion draft imposes data minimization requirements on covered entities, prohibiting such entities from collecting, processing or transferring covered data that is "beyond what is reasonably necessary, proportionate, and limited to" a product or service provided by the covered entity. The bill directs the FTC to issue guidance on compliance with this data minimization requirement and, similar to the data security section, requires the Commission to consider the scope, nature and complexity of the covered data and covered entities. Section 103 of the bill also requires covered entities to implement "privacy by design" protocols that "establish and implement reasonable policies, practices, and procedures regarding the collection, processing and transfer of covered data…"

The bill specifically prohibits certain data practices such as transferring social security numbers, geolocation information, biometric data, and passwords. These prohibitions and restrictions are all subject to caveats and exceptions. The bill also prohibits covered entities from conditioning their services or charging different prices based on individuals exercising their privacy rights under the bill. There are two notable exceptions to this "non-discrimination" provision: (1) the relating of price or level of service to "financial information" provided by the individual that is necessary for initiating, rendering, billing for, or collecting payment; and (2) loyalty programs.

It's worth noting that the "duty of loyalty" laid out in the discussion draft differs from a "duty of care" or "fiduciary duty" contemplated in other bills, the most prominent example being the **Data Care Act**, introduced by Senator Schatz, which imposes much broader duty of care obligations on covered entities to not misuse data to the detriment of consumer well-being.

8. Data Access and Portability:

Section 203 of the discussion draft requires covered entities to provide individuals, upon a valid request, with access, correction, deletion and portability rights similar to the rights established under the **California Consumer Privacy Protection Act (CCPA)** and the European Union's **General Data Protection Regulations (GDPR)**.

9. Corporate Accountability:

Title III of the discussion draft imposes a set of internal controls upon covered entities and large data holders, as established by the FTC in regulations promulgated under the APA. The chief executive officer and privacy and security officers of large data holders must annually certify to the Commission that they have adequate internal controls and review mechanisms in order to be in compliance with the provisions of the bill, similar to the **certifications required for public companies** under Sarbanes-Oxley. Large data holders are also required to biennially "conduct a privacy impact assessment that weighs the benefits of the large data holder's covered data collecting, process, and transfer practices against the potential adverse consequences of such practices to individual privacy."

Section 303 of the bill also directs the FTC to promulgate regulations that approve technical compliance programs. Such programs would presumably be designed to act as safe harbors that can provide covered entities with clear compliance guidelines and regulatory certainty.

10. Enforcement & Private Right of Action:

The discussion draft empowers the FTC to enforce against violations of the bill as violations of a rule promulgated under Section 18 of the FTC Act. This allows the Commission to seek civil penalties for any violations of the bill. The discussion draft creates a new bureau, comparable in size and structure to the current Bureaus of Consumer Protection and Competition, to implement and enforce the Act. State attorneys general (and related consumer protection officials) are also authorized to enforce the provisions of the bill, including the authority to seek civil penalties, subject to FTC intervention.

The discussion draft creates a new private right of action, allowing an individuals or individuals to file a civil suit in federal court, although such private right of action does not kick in until four years after the ADPPA takes effect. Such actions and their relief would be limited to compensatory damages, injunctive or declaratory relief, and reasonable attorney's fees and litigation costs. Notably, plaintiffs would not be able to seek civil penalties or punitive damages, and covered entities can shield themselves from actions seeking injunctive relief if they cure the violations within 45 days of notice. The discussion draft prohibits subjecting potential plaintiffs under the age of 18 to pre-dispute arbitration proceedings or to a pre-dispute joint-action waiver. And general arbitral or administrative pre-dispute joint-action waivers are generally prohibited. Nonetheless, arbitration proceedings are still generally permissible upon agreement among disputed parties (except for plaintiffs under 18).

11. Preemption and Effects on Other Laws:

The discussion draft's preemption provision, section 404, largely preempts those state privacy laws and regulations that are covered by the discussion draft or by any regulation promulgated under the draft. Thus, CCPA and the upcoming California Privacy Rights Act, along with the **five other state privacy laws** just enacted this year will be largely preempted. However, there are a myriad of exceptions to the preemption provision, the most notable being CCPA's private right of action for data security violations, the **Illinois Biometric Information Privacy Act** (along with **its accompanying litigation**…), facial recognition laws, the **Genetic Information Privacy Act**, and any common law or statutory causes of action. State breach notification laws are also preserved from preemption. The preemption provision also explicitly carves out a slew of state laws from its preemptory effect – laws such as civil rights laws, employment laws, and laws of general applicability (to just name a few.)

As noted earlier, other federal privacy laws – such as GLBA and HIPAA – are left unaffected, but their covered entities are not carved out from the ambit of the discussion draft but rather are deemed to be in compliance if they comply with those separate laws. As such, such covered entities could be subject to both FTC enforcement actions and the enforcement actions of their functional regulators. However, in contrast, the discussion draft largely preempts any privacy related provisions under the Communications Act or administered by the Federal Communications Commission (FCC). This straight preemption of FCC authority leaves the FTC as the sole agency with jurisdiction over those affected entities. Satellite carriers, cable operators, and ISPs are specifically listed – in brackets – as such covered entities under the bill.

There are many other sections of this bill, and numerous requirements – such as the appointment of privacy officers, transparency and privacy policies, data ownership – that will require further scrutiny. The Mintz Privacy Team and ML Strategies will continue to watch this and other important privacy legislation and will bring updates. Stay tuned.

Authors

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Vice President of ML Strategies in the firm's Washington, DC office. He assists a variety of clients in their interactions with the federal government.

Cynthia Larose