Excerpt from FPF Blog, "Closer than Apart: Comparing Senate Commerce Committee Bills" (Dec. 2, 2019) - Pollyanna Sanderson

Comparison of the Consumer Online Privacy Rights Act (COPRA) & Sen. WIcker Staff Discussion Draft

Significant Commonalities (with some differences):

Covered Data – Both bills define covered data as "linked or reasonably linkable," including inferences or derived data; both *exclude* employee data, de-identified data, and public records. The Wicker draft would also broadly exempt publicly available information from regulation (a key difference below).

Covered Entities and Small Business Exemption – Both bills would govern commercial businesses, either those already governed by the FTC Act (Cantwell), or those "affecting interstate commerce" (Wicker). Both contain a small business exemption, from the entire bill (Cantwell), or from the bulk of core obligations (Wicker).

Transparency – Both would require detailed public privacy policies, including: categories of data collected/transferred, processing purposes, retention practices, and how to exercise rights. Cantwell additionally would require disclosure of the ***specific identities*** of all third parties to which data is transferred (102(b)(3)(B)).

Access – Both would require companies to provide individuals with a copy "or accurate representation" of their data upon "verified request" and the names of third parties to whom it has been transferred (and, in Wicker, the names of service providers), free of charge (although Wicker limits free requests to 2/year).

Deletion, Correction & Portability – Both bills would require companies, upon "verified request" to correct or delete covered data of an individual and inform service providers and third parties of the request, although the Wicker draft uses the phrase "delete or deidentify." Both would require that data be provided upon request "in a structured, interoperable, and machine-readable format," "without licensing restrictions," although to this list Wicker adds the term "standards-based." Both exclude inferred or derived data from portability requests.

Opt-Outs for Non-Sensitive Data – Cantwell would establish a right to object to data transfers, subject to a process established by FTC rulemaking, within guidelines (clear and conspicuous, centralized, with the ability for individuals to view and change the status of their objection, and informed by the Do Not Call Registry) (105(b)). Wicker would more broadly allow individuals to "object to the processing and transfer" of data, but would not require specific rulemaking on this point (104(d)).

Opt-In for Sensitive Data – Both bills would require "prior, affirmative express consent" for processing of sensitive data, including biometric data (with restrictions on what consent must require, in definitions for Cantwell, and in the text of Sec. 105 for Wicker). The definition of "sensitive data" in the Cantwell bill is significantly broader, containing "browsing history," "email," and "phone number" (these are not included in Wicker).

Commercial IRBs for Ethical Research – Among similar lists of enumerated exceptions to individual rights (for e.g. product recalls, audits, etc.), both bills contain an exemption for research governed by commercial IRBs or similar oversight entities meeting standards promulgated by the FTC (Cantwell 110(d)) (Wicker 108(a)).

Privacy and Security Officers & Risk Assessments – Both bills would require companies to appoint a designated privacy officer and security officer, with responsibilities to facilitate compliance with the Acts. In addition, the Cantwell bill would create specific responsibilities to implement and oversee a comprehensive data privacy and security program, including annual "privacy and data security risk assessments," among their other quality control responsibilities (Sec. 202). Wicker would only require "large data holders" to undergo similar internal "privacy impact assessments" (Sec. 107).

Deepfakes / Digital Content Forgeries – Both bills would require federal agencies (NIST, and in Wicker, NIST and the FTC) to study and produce reports on the definition, assessments and analysis, of "digital content forgeries."

Algorithmic Bias & Civil Rights – Cantwell would require companies to conduct annual algorithmic decisionmaking impact assessments for bias, and both bills would require the FTC to publish a report (Cantwell) or a report every 5 years (Wicker) examining the uses of algorithms to process covered data in ways that may violate anti-discrimination laws. In addition, Cantwell goes significantly further by directly prohibiting covered entities from processing or transferring covered data on the basis of protected characteristics for specified purposes (Sec. 108).

Significant Differences:

Publicly available information – While both bills would exclude "public records" from covered data, Cantwell would still govern "publicly available information" (although excluding it from deletion and correction obligations). In contrast, the Wicker draft would exclude all data "widely available to the general public" from the definition of covered data, thus exempting it from all regulation.

Enforcement – While both bills situate the FTC and State AGs as enforcers, the Cantwell bill would also create a broad private right of action for individuals to bring civil actions, and receive penalties of $100-$1,000 per violation per day, or actual damages, whichever is greater; punitive damages; reasonable attorney's fees and litigation costs; and/or any other judicial relief deemed appropriate.

Preemption – The Wicker bill would preempt very broadly (any state "law, regulation, rule, requirement, or standard related to the data privacy or security and associated activities of covered entities.") In contrast, the Cantwell bill would not preempt any state laws beyond those "directly conflicting," to the extent of the conflict.

Children's Data (Wicker Only) – While the Cantwell bill does not contain any special protections for children's data, the Wicker draft would require affirmative consent prior to any transfers of data from children under 16. (Wicker 104(c)).

Certification Programs (Wicker Only) – The Wicker draft would allow the FTC to approve self-regulatory "certification programs" developed by businesses or industry associations, so long as they meet certain requirements for eligibility (Sec. 403).

Data Broker Registration Requirements (Wicker Only) – The Wicker draft would require data brokers (a "data broker" is an entity that "knowingly collects or processes on behalf of, or transfers to, third parties the covered data of an individual with whom the entity does not have a direct relationship") to register basic contact information annually with the FTC, with civil penalties for failing to register.

Executive Responsibility (Cantwell only) – The Cantwell bill would require the CEO or top officer, and the privacy and data security officers, of "large data holders," to make annual certifications to the FTC regarding adequate internal controls.

Whistleblower Provisions (effectively Cantwell Only) – The Cantwell bill would create robust protections for whistleblowers (defined broadly) against any retaliatory action (also defined broadly), including civil remedies of reinstatement, back pay and damages. In contrast, the Wicker draft defines "whistleblower" narrowly (provider of "original information" to an agency), and provides no legal remedies to individuals; instead, it provides only that the FTC may take into account any retaliation against a whistleblower when assessing penalties.