Analysis: U.S. Data Protection Bills

In the wake of the Cambridge Analytica scandal, members of Congress are either introducing or reviving proposals for new data protection legislation. Some proposals now on the table would only further entrench the prevailing business models that reward unchecked data collection and opaque data exploitation, to the detriment of consumer rights and our democratic processes. Others are a solid starting point for a conversation about what is necessary to provide the meaningful data protection that people in the U.S. and around the world desperately need. Following is our analysis:

- **Consumer Privacy Protection Act (S. 2124; H.R. 4081)**

Lawmakers introduced the Consumer Privacy Protection Act in 2017 with Senator Leahy as the primary sponsor. The bill would do several things. It would expand the reach of the the Computer Fraud and Abuse Act ("CFAA"), which the U.S. Department of Justice has frequently interpreted over-broadly, and also increase the reporting on prosecutions under that law. With regard to privacy protections, it would provide for the creation of "comprehensive consumer privacy and data security" programs, as well as risk assessments and other internal controls and testing for privacy and security. It would grant more authority to the Federal Trade Commission ("FTC") and allows for investigations by state Attorney Generals. Finally, it includes a section to provide for federal data breach notification for breaches involving sensitive personally identifiable information.

Unfortunately, this approach has several shortcomings. It extends the CFAA without necessary reforms. In some respects, it invokes protections that the FTC has included in consent orders with companies that have engaged in unfair or deceptive trade practices. While this approach isn't bad in theory, it has limited efficacy; Facebook was already subject to many of these provisions under a 2011 consent order. A "self-regulatory" approach fails to provide the rights and obligations that will fully protect users. Further, the law is limited in scope, applying only to entities with data about more than 10,000 U.S. persons, with a carve out for service providers. Finally, while the provisions for data breach notification are welcome and this is one of the most progressive approaches that we've seen, they can be improved, including by giving the FTC the authority to develop regulations on the types of information that would trigger notification requirements.

- **BROWSER Act (Balancing the Rights of Web Surfers Equally and Responsibly, H.R. 2520)**

Representative Blackburn introduced the BROWSER Act in 2017. Blackburn is known for her opposition to the Federal Communications Commission's ("FCC") open internet rules to protect Net Neutrality and the privacy of broadband customers, among other things. The act requires that internet service providers (ISPs) and "edge" providers (also known in some contexts as "over the top" or "OTT" providers, meaning that they operate over the internet) provide notice of their privacy policies. The bill then provides for opt-in approval for the use, disclosure, or permit access to sensitive information, with opt-out approval for all other information (notably, there is no approval necessary — opt-in or opt-out — for the collection of data). There are several exemptions from these requirements, including a broad one related to "providing" the service or "services necessary to, or used in, the provision of such service."

This is one of the least protective approaches that we have seen in the bills that have been introduced. Privacy policies have proven, time and time again, not to be effective vehicles for protecting privacy. Additionally, the protections given are narrow and the exceptions largely swallow the rule. In addition, the proposal expressly prevents any state from implementing a stronger protection, effectively cutting state regulators off at the knees. However, there are some minor positive elements that are worth noting. First, the bill applies evenly to both ISPs and edge providers without exceptions for size or user base, although it doesn't apply to the range of other entities that collect or rely upon massive amounts of

sensitive data. Additionally, and most positively, the bill prevents provision of any service from being conditioned or terminated on the basis of a person's privacy decisions.

- **CONSENT Act (Customer Online Notification for Stopping Edge-provider Network Transgressions, S.----)**

Senators Markey and Blumenthal recently introduced the CONSENT Act. It requires, within a year, for the FTC to promulgate privacy rules for edge providers. The rules must include notification requirements for collection, use, and transmission of certain sensitive data, including personally identifiable information, specification of how data are used and transmitted, and to whom, and protection of de-identified data. The rules also must include opt-in consent for use, transmission, or sale (but not collection) of sensitive information. While it prohibits refusal of service based on unwillingness to provide consent, it does seem to anticipate that other conditions could be imposed by directing the rules to address the reasonableness of prices or discounts related to consent. The bill also requires reasonable data security practices and data breach notification, though only for sensitive information and only if harm is likely.

There is a lot of good in this bill, including a positive notion of opt-in consent. However, it fails to apply to ISPs or any other entity that collect massive amounts of personally identifiable information, making it inherently narrow. Further, outside of the requirement for opt-in consent, it fails to provide adequate guidance in its direction to the FTC, meaning the bill allows for the promulgation of weak or perfunctory rules. Finally, the data breach notification requirement is a positive step, but by tying it to harm it's potentially too narrow to encompass the full range of risks to user information.

- **MY DATA Act of 2017 (Managing Your Data Against Telecom Abuses Act, S. 964; H.R. 2356)**

Senators Blumenthal and Representative McNerney introduced the MY DATA Act in early 2017. The bill generally states that it is unlawful for a broadband provider or edge provider "to use an unfair or deceptive act or practice relating to privacy or data security," while directing the FTC to develop implementing regulations and otherwise enforce the Act. This bill, while positive in its expansion of the FTC's authority, represents a marginal improvement at best. It doesn't specify any specific rights or standards to guide the FTC in its promulgation of rules, leaving broad space for ineffective regulations.

- **Secure and Protect Americans' Data Act (H.R. 3896)**

Representative Schakowsky has led the introduction of the Secure and Protect Americans' Data Act for the past two congresses. Among other things, the bill provides for the FTC to promulgate regulations on reasonable information security practices, to include regulations on the collection, use, sale, dissemination, and maintenance of personal information, the retention and destruction of personal information, and access to such information. Companies are required to review their policies every year and submit them to the FTC in the case of a data breach, with special requirements for "information brokers" -- companies whose business is based around the collection and use of personal data. Additionally the bill has a data breach notification requirement, with notice required within 30 days, and a prohibition on "pre-texting" practices.

While the bill appears at first glance to be a comprehensive approach to data protection, its biggest limitation is that it applies only to "personal information," which is very narrowly defined within the bill. Most notably it excludes some of the most sensitive information that people tend to identify, including photos, personal communications, or the vast scope of information collected by new and developing Internet of Things devices. Further, the bill places too much responsibility for the protection of data on the user themselves, particularly vis-a-vis information brokers, companies which rarely directly interface with users though the bill mostly requires users to visit their websites to exercise their rights.