Blackburn Introduces Sweeping Internet Privacy Reform Legislation

May 26, 2017

On May 19, 2017, House Communications and Technology Subcommittee Chairman Marsha Blackburn (R-TN) introduced the Balancing the Rights of Web Surfers Equally and Responsibility Act of 2017 (the Browser Act or the bill), which overhauls privacy requirements for both Internet service providers (ISPs) and edge providers (e.g. Facebook, Netflix) (collectively, service providers). The bill adopts policies similar to the broadband privacy rules adopted by the Federal Communications Commission (FCC or the Commission), which were overturned by a Congressional Review Act resolution in late March of this year.

The Browser Act would require service providers to provide their users with notice of the provider's privacy policies; require user opt-in for sensitive information and an opt-out option for non-sensitive information; prohibit the conditioning of service on waivers of privacy rights; and specifically authorize the Federal Trade Commission (FTC) to oversee the privacy practices of ISPs. Co-sponsor Rep. Brian Fitzpatrick (R-PA) said in a statement the bill is intended to "introduce comprehensive internet privacy legislation that will more fully protect online users in their use of Internet service providers, search engines and social media." The bill is likely to face an uphill battle in both the House and the Senate, and has drawn mixed reviews from industry and public interest groups.

- **Notice of Privacy Policies**. The bill would require service providers to offer users notice of their privacy policies. The notice would need to be made available at the point of sale, at the establishment of an account for a service, or if there is no such process, before the user first uses the service. Notice would also need to be persistently available. If there are any "material changes" to the privacy policies, the provider must give users advance notice in a clear and conspicuous manner. The bill defines a "material" change as "any change . . . that a user of the service, acting reasonably . . . would consider important to the decisions of the user regarding the privacy of the user."

- **Opt-In and Opt-Out Approval.** The Browser Act would require providers to obtain opt-in approval from a user to use, disclose, or permit access to the sensitive information of the user. The Browser Act defines "sensitive information" as financial information, health information, information pertaining to children under the age of 13, social security numbers, precise geo-location information, the content of communications, web browsing history, history of usage of a software program (including mobile apps), and the functional equivalents of either. The bill also would require providers to make available a "simple, easy-to-use mechanism for users to grant, deny, or withdraw opt-in approval or opt-out approval at any time."

- **Exemptions from Opt-In or Opt-Out Approval.** The Browser Act would exempt certain uses of information from the consent requirement. For example, consent would not be required if sharing the information is required to provide the service, to bill for the service, to protect the

rights or property of the provider, to protect users from fraudulent use of the service, or to provide location information to a public safety answering point (PSAP), emergency first responders, a medical facility or medical professional. The bill also allows the sharing of location information with the user's legal guardian or immediate family member if there is an emergency situation that involves the risk of death or serious physical harm.

- **Prohibition on Conditioning Service on Waiving Privacy Rights**. The Browser Act would prohibit a service provider from conditioning (or effectively conditioning) provision of a service on the user agreeing to waive privacy rights guaranteed by law or regulation, or terminating the service a consequence of the user's refusal to waive any privacy rights.
- **Clear FTC Authority over Privacy.** The Browser Act addresses the perceived enforcement gap between FTC and FCC jurisdiction over broadband privacy by making clear that the FTC will be the consumer protection agency responsible for enforcing the protections in the bill, including over broadband providers "notwithstanding the exception in [the FTC Act] for common carriers."
- **Pre-emption of State Law**. The bill would preempt all state laws "relating to or with respect to the privacy of user information," as well as any federal statutes, including the Communications Act of 1934, unless the regulations pertain to emergency services.

Mixed Reactions

The bill has drawn mixed reactions. While trade associations representing edge providers have come out against the bill, large ISPs like AT&T have been supportive of its comprehensive and uniform approach. The Electronic Privacy Information Center (EPIC) has raised concerns that the bill lacks a private right of action, and is skeptical that the FTC will adequately protect consumers' privacy. EPIC is also opposed to the legislation overwriting stronger state privacy laws. The Association of National Advertisers (ANA) has said the bill "goes substantially too far," arguing that most browser and app usage data is "innocuous" and "treating too many categories and issues as sensitive will undermine the ability of consumers to focus on what is truly significant in regard to their privacy." Ultimately, this bill faces a steep uphill climb. We will continue monitoring the Browser Act as it works its way through the legislative process.