

Reproduced with permission from Privacy & Security Law Report, 16 PVLR 833, 6/19/17. Copyright © 2017 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

BROWSER Act

The Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017, or the BROWSER Act, would establish uniform privacy rules governing how online service providers throughout the internet ecosystem may use, disclose, or permit access to the consumer information they collect. Whether or not it passes, it is possible that the BROWSER Act will serve as the new baseline to measure the strength or weakness of any future legislative efforts seeking to create a federal privacy regime for the digital economy, the authors write.

Browsing the New Contours of the Online Privacy Debate



BY SHAWN CHANG AND HAP RIGBY

Merely six weeks after Republicans in Congress successfully used the Congressional Review Act (CRA) to overturn the Federal Communications Commission’s (FCC) 2016 Broadband Privacy Order, Representative Marsha Blackburn (R-TN), Chairman of the Communications and Technology Subcommittee and leader of

the CRA effort in the House, introduced the Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017, or the BROWSER Act, on May 18. The bill would establish uniform privacy rules governing how online service providers throughout the internet ecosystem may use, disclose, or permit access to the consumer information they collect.

The bill’s introduction caught stakeholders across the political spectrum and the internet ecosystem by surprise. It challenges the conventional wisdom about the politics of the online privacy debate: that Republicans are satisfied with the Federal Trade Commission’s (FTC) current privacy enforcement approach and that Democrats want to replace the FTC’s privacy model with something similar to the FCC’s 2016 Order and apply it to all stakeholders. It also challenges how advocates have approached federal protection of online user’s private information: that businesses making money from using information collected about internet users will welcome the elimination of patchwork regulation at state and local levels, especially since such laws have proliferated in the wake of the passage of the CRA resolution, and that consumer advocates would support a federal privacy regime that not only meets, but arguably goes beyond, the standards created by the FCC’s 2016 Broadband Privacy Order, regardless of which agency is given the authority to enforce. The BROWSER Act appears to directly confront each of these conventional assumptions.

Whether the surprise it caused upon introduction was due to its sponsorship, its novel approach, or both, the

Shawn Chang is a partner at Wiley Rein LLP in Washington and is a former chief counsel in the U.S. House of Representatives.

Hap Rigby is a senior policy advisor at Wiley Rein LLP in Washington and former advisor on the U.S. Senate Committee on Commerce, Science, and Transportation.

BROWSER Act is now a significant—perhaps the most significant—contribution to the ongoing public policy debate about the appropriate framework for the privacy of internet user information in the digital age. Here are some of the reasons why.

The FTC Would Cover All Online Services Again Republicans were already opposed to the Wheeler FCC’s reclassification of broadband internet access service (BIAS) as a common carriage service because they felt the prior light-touch information service classification had served all players of the internet economy, including internet users, well. In the privacy context, common carriage classification effectively prohibited the FTC from policing the practices of BIAS providers because of the FTC Act’s common carrier exception. When the Wheeler FCC adopted privacy rules for BIAS providers that did not completely reflect FTC’s approach to how information should be treated as sensitive or non-sensitive, Republicans felt the Commission created a second part to the already existing reclassification problem.

By repealing the FCC’s 2016 Broadband Privacy Order, the Trump Administration and Republican majorities in Congress took the initial step to return internet privacy regulation to the FTC-enforced framework that largely permits the collection, sharing, and use of internet users’ personal information, so long as such information does not belong to narrow categories of “sensitive” personal information such as financial and health information. The next step to return the FTC cop to the privacy beat would be to have the Republican FCC majority, led by now-Chairman Ajit Pai, reverse the Wheeler FCC’s classification of BIAS as a common carriage service. At that point, all would be well following conventional Republican wisdom. The introduction of the BROWSER Act, however, places a fork in that path for Republicans. In addition to removing the common carrier exception and restoring the FTC’s authority over broadband service providers, the bill’s introduction of a different regime for empowering consumer choice suggests that the FTC’s current approach to privacy is insufficient to protect internet users.

Federal Privacy Regulations Would Increase The BROWSER Act embraces much of the FCC regulation centered on principles of transparency and consumer choice. Despite removing the FCC’s jurisdiction to police the privacy practices of broadband service providers and consolidating such authority with the FTC, the legislation mimics the “opt-in”-centric regime and scope of covered data favored by the Wheeler FCC’s Democratic majority and treats browser history, app usage data, and the content of online communications as sensitive information requiring service providers to obtain “opt-in” consent from their customers in order to use, disclose, or permit access to such data. Furthermore, the bill would increase federal privacy regulations by extending these rules to all online service providers, including edge providers like Alphabet Inc.’s Google and Facebook Inc., thus addressing the lack of a level playing field caused by the FCC’s 2016 rules.

Consumer Would Have More Control Over Their Information The BROWSER Act is notable not only because of how it resembles the 2016 FCC broadband privacy rules, but also how it differs. Whether by accident or by

design, the legislation does not contain several elements of the FCC’s 2016 rules that would seem to alleviate online service providers’ compliance burdens.

For example, the 2016 FCC rules permitted providers to use and disclose de-identified customer information without consent, following a fact-based three-part test. The FCC also sought to utilize its Consumer Advisory Committee’s multi-stakeholder process to develop a standardized “safe harbor” privacy notice format providers could voluntarily use to inform customers about the collection, sharing, and use of their data. Neither of these features are part of the BROWSER Act, but will no doubt be considered should the bill move through the legislative process.

Instead, the legislation incorporates some of the more draconian aspects of the 2016 rules such as the prohibition on “take-it-or-leave-it” offers. Under the rule, a covered service provider cannot refuse to serve customers who do not consent to the use and sharing of their information for commercial purposes, even if the service is made available at no charge to the customer. While the provision may have limited application to an internet service provider, the extension of such prohibition to edge providers under the BROWSER Act could fundamentally disrupt the very business model that drove the growth and adoption of the internet: the provisioning of a free service paid for by the provider’s ability to monetize the personal information of its customers.

Patchwork and Conflicting Privacy Rules Would Cease The BROWSER Act explicitly preempts state and local laws related to online service providers and the privacy of internet user information, unlike the FCC’s 2016 Order. BIAS providers and internet edge companies alike have long advocated for preemption of state and local privacy laws. Preemption has often been a sticking point in policy debates about any interstate commercial activity and consumer protection, and there may be no activity both so interstate and consumer-centric in nature than modern internet usage. The question for traditional opponents of preemption will be whether privacy protections have been raised high enough by the BROWSER Act to give them a reason to accept a uniform federal regime in this case.

A New Baseline? It is extremely difficult to successfully legislate these days on any matters, much less an issue as emotional and complex as online privacy, so it is unlikely that the BROWSER Act will arrive at the President’s desk any time soon. Nevertheless, by including a bit of something for everyone as an initial position, the BROWSER Act has breathed new life into an otherwise stale privacy debate. Rep. Blackburn has provided the new contours of the privacy discussion—opt-in and opt-out control for consumers, uniform treatment of all online services, and general preemption of state, local, and FCC privacy activities. It remains to be seen whether the legislation will attract the support of Congressional Democrats or Senate Republicans, but it is possible that the BROWSER Act will serve as the new baseline to measure the strength or weakness of any future legislative efforts seeking to create a federal privacy regime for the digital economy.