Insight

The BROWSER Act Explained

WILL RINEHART | JUNE 14, 2017

Late last month, Representative Blackburn introduced the "Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017," known colloquially as the BROWSER Act. The concepts in this bill are the source of continued controversy in the privacy and Internet community. They include requiring both Internet service providers (ISP) and edge providers, such as social platforms, digital publishers and mobile app providers, to obtain opt-in consent from people to use their information.

The idea is to set up a two-tiered system for privacy regulation, a system for sensitive information and another for non-sensitive information. For sensitive information, all providers of a covered service to get opt-in approval from users to use, disclose, or permit access to it. In other words, before any service could be rendered, explicit approval would have to be given. In the case of the BROWSER bill, sensitive information includes:

- Financial information,
- Health information,
- Information pertaining to children under the age of 13,
- Social Security number,
- Precise geo-location information,
- Content of communications, and
- Web browsing history and the history of using a software program.

For all other non-sensitive information, companies would have to allow consumers an easy way to opt-out. The bill would also put the Federal Trade Commission as the cop on the beat, which is a natural fit since this agency has been doing yeoman's work on privacy for years.

What would this bill mean for the Internet ecosystem? Nearly everyone would be covered, including ISPs, social platforms, digital publishers, mobile app providers, and a bevy of other Internet content providers, as well as government web sites. Practically speaking, the part of the Internet that runs on ads, including Facebook and Google, would face considerable headwinds as consumers are presented with government mandated roadblocks in the form of opt-in decisions.

As AAF has explained, opt-in mandates present three hurdles for consumers in their decision-making process. First, they would have substantially less information about decisions they make. Before any additional service can be provided, consumers would have to imagine all of the potential benefits, a difficult if not impossible task. Second, consumers may think that that defaults are company policy, even though they are mandated choices by the government. Lastly, these defaults will become the assumed status quo for all kinds of information, not just sensitive information. All combined, the expansion of services that aren't sensitive but use this data will become extremely difficult. As psychologists and behavioral economists have found, people prefer to avoid loses rather than making equivalent gains. If the gains are difficult to express, then consumers will prefer the baseline. In the terminology of Nicklas Lundblad and Betsy Masiello, the effect would be an opt-in dystopia.

The downsides of an opt-in system are well worn territory. Economists, the FTC, and privacy professionals

largely agree that an opt-in system would harm innovation. While this particular bill's future is uncertain, one thing is clear: it's driving an important Internet privacy conversation involving both policymakers and stakeholders.