Bloomberg Law®

bloombergbna.com

INSIGHT: Digital Privacy Requires a Cohesive Federal Solution

The FTC has re-assumed jurisdiction over the privacy practices of broadband service providers, but there is still a need for a unified legislative privacy regime in the digital space, says Lawrence J. Spiwak, President of the Phoenix Center for Advanced Legal & Economic Public Policy Studies.

BY LAWRENCE J. SPIWAK

As most people have discovered by the avalanche of compliance emails flooding their in-boxes, the European Union's General Data Protection Regulation (''GDPR'') has now gone into effect. But because the United States always wants to lead on the world stage, there is growing talk in Washington about the need for our own privacy legislation. While the debate over the exact contours for any potential privacy legislation is in the very early stages, there are nonetheless two overarching jurisdictional concerns which need immediate Congressional attention:

First, given the intertwined nature of the modern internet ecosystem, an asymmetrical approach to digital privacy makes little sense. As such, any proposed legislation must provide a cohesive policy framework to deal with consumer privacy concerns that applies uniformly to all internet companies—both ''edge'' companies such Google and Facebook and ''core'' network providers such as AT&T and Comcast. Moreover, to ensure cohesiveness, this framework should be administered by a single federal agency rather than by a hodge-podge of different federal agencies with assorted statutory mandates.

Second, enforcement of digital privacy cannot be left to the individual states. Accordingly, any proposed legislation must also make clear that the exclusive jurisdiction to evaluate privacy issues is left to the Federal government; the internet is too vast to be subject to multiple state privacy regimes.

Lawrence J. Spiwak is the President of the Phoenix Center for Advanced Legal & Economic Public Policy Studies (www.phoenix-center.org), a non-profit 501(c)(3) research organization that studies broad public-policy issues related to governance, social and economic conditions, with a particular emphasis on the law and economics of the digital age. The views expressed in this article are those of the authors and not necessarily those of Bloomberg Law.

The Obama Administration's Asymmetrical Approach to Digital Privacy The jurisdictional problems in the privacy debate can be traced directly back to the Federal Communications Commission's controversial 2015 decision to reclassify broadband internet access as a common carrier ''telecommunications'' service under Title II of the Communications Act of 1934. By virtue of this reclassification, broadband service providers (BSPs)—whether wireline, cable or wireless—suddenly found themselves subject to the Customer Proprietary Network Information (CPNI) statutory framework contained in Section 222 of the Communications Act (added by the Telecommunications Act of 1996)—rules

which were designed for pre-internet services offered by the handful of telephone companies in existence at the time. Adding to the legal morass, Obama Administration's decision on reclassification essentially stripped the Federal Trade Commission (''FTC'')—the agency that traditionally has jurisdiction over digital privacy concerns for the entire internet ecosystem—from bringing a privacy enforcement action against Broadband Service Providers (''BSPs'') because the FTC has no jurisdiction over firms which provide a ''common carrier'' service.

While the FCC could have incorporated lessons from the FTC's extensive experience in dealing with the complexities of online privacy, the Commission refused. Instead, as lamented by both the FTC's staff and FTC Commissioner Maureen Ohlhausen, the FCC chose to forge its own path. Rather than create a harmonized industry-wide regulatory approach to digital privacy, the FCC's actions created asymmetrical regulatory regimes: a restrictive *ex ante* regime specifically for BSPs with rules enforced at the FCC, and an *ex post* case-by-case regime enforced by the FTC for everybody else.

Fortuitously, a series of events help right the ship. First, Congress passed—and President Trump signed—a Congressional Review Act (CRA) discharge petition against the Obama Administration's ill-formed privacy rules. Second, the FCC—now under the leadership of Chairman Ajit Pai—reversed the Obama Administration's reclassification decision and returned broadband internet service to a more flexible, lighter-touch regime. And, just to make sure there were no legal ambiguities remaining about the FTC's privacy enforcement authority, the full Ninth Circuit Court of Appeals ruled *en banc* this February in *FTC v. AT&T Mobility* that the FTC Act's ''common carrier'' exemption would be based upon a firm's activities, not upon a firm's status. For both edge and core providers, the FTC is now back on the beat.

The Need for Federal Privacy Legislation But if the FTC is back on the privacy beat and can provide a holistic approach to edge and core alike, then why do we need legislation? As noted above, there are two important jurisdictional reasons.

First, responding to the now-majority-Republican FCC's rollback of the Title II order (and still stinging from a Congressional Resolution voiding the prior Commission's enactment of asymmetrical privacy rules), Congressional Democrats are attempting to pass their own CRA discharge petition to reverse the Trump Administration's *Restoring Internet Freedom Order*. Should they succeed, or should the Democrats win the Presidency in 2020, it would surprise no one if their first priority were to seek to re-reclassify broadband internet access as a common carrier service and restore some form of the *2015 Open Internet Rules*.

But here's the rub: Because the Obama Administration's privacy rules were struck down by an act of Congress, under the express terms of the Congressional Review Act the FCC would be prohibited from enacting ''substantially similar'' privacy rules on Broadband Service Providers. Thus, in the event of any re-reclassification of broadband internet access, we would ironically find ourselves with a gaping privacy enforcement hole in the internet ecosystem: that is, any attempt to re-reclassify broadband internet access will mean that all BSPs—wired and wireless alike—will have no privacy oversight from either the FCC or the FTC. By any account, clear privacy legislation with defined enforcement roles and oversight authority is a far better system than the regulatory chaos we just endured.

Moreover, we need privacy legislation to solve the looming federalism problem. Egged on by pro-regulatory advocates and playing on the fears of local constituents, multiple states are now considering enacting their own local version of digital privacy laws (often pairing such legislative efforts with individual state net neutrality laws). Even embracing such efforts as altruistic, having each state think it can regulate the internet raises serious concerns.

A 2008 paper published in CommLaw Conspectus explains the source of the problem. When state law applies to a product or service that is actually national in scope, even if each state acts with the purist of intentions to protect their respective constituents' privacy, there is the risk of harmful conflicts in the rules, as the states will inevitably vary in their legal regimes. As a result, there will be *extra-jurisdictional effects* of state-by-state regulation on a national service, making society worse off. To quote former FCC Chief Economist Michael Katz on state-level business rules, ''policies that make entry difficult in one geographic area may raise the overall cost of entering the industry and thus reduce the speed at which entry occurs in other areas.'' When state and local regulation can spill across borders, society is typically better off with a single national framework.

The logic holds true in the digital privacy context. Privacy is not a state problem, it is a national problem. The significant extra-jurisdictional effects from a hodge-podge of state privacy legislation on the internet at large will greatly complicate compliance for internet businesses. Digital privacy augurs for a cohesive federal solution.

Accordingly, only a clear statement by Congress that digital privacy will appropriately be handled at the federal level will nip this misguided digital federalism movement in the bud. The internet cannot wait years for preemption challenges (which will likely ultimately prove successful) to work their way through the courts. Congress needs to act quickly and decisively to avoid further damage to the internet's evolution.

Conclusion Information is the currency of the modern internet ecosystem. Given the dynamism of the market, therefore, any proposed legislation must somehow balance consumers' privacy and simultaneously, in the words of FTC Commissioner Maureen Ohlhausen, provide for ''maximum flexibility.'' To achieve this goal, difficult questions must be asked, even though many of the answers are not yet readily apparent. Still, as the internet continues to evolve faster than government can keep up, Congress must put aside partisan bickering and start this discussion immediately.