



## **The FCC Broadband Privacy Proceeding**

At its March 2016 open meeting the FCC adopted a Notice of Proposed Rulemaking (NPRM) on “Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.” The NPRM builds on last year’s Open Internet Order when the FCC rightly reclassified broadband Internet access as a telecommunications service under Title II of the Communications Act. As part of the Open Internet Order, the Commission also recognized these telecommunications carriers’ duty under Section 222 of that law “to protect the confidentiality of” their customers’ “proprietary information.” Both that Order and an FCC enforcement advisory put broadband ISPs on notice, for more than a year now, that a privacy rulemaking would soon commence. Internet users want and need these kinds of updated consumer privacy safeguards to protect their private information from unauthorized disclosure and abuse.

### **The FCC Has Clear Statutory Authority for Broadband Privacy Rules.**

When Congress updated the Communications Act in 1996, with overwhelming bipartisan majorities in both chambers, it added Section 222. That statute contains unambiguous directives for telecom carriers to protect consumers’ private information. The statute requires customers’ opt-in approval – with very few exceptions – before a carrier can use this information for reasons other than providing the underlying telecom service. The law protects both “customer proprietary network information” (CPNI) metadata about the use of the network and other private information too.

### **Clear Privacy Harms and Threats from Broadband Providers.**

By providing Internet access, ISPs have the ability to surveil almost all unencrypted Internet traffic — from the websites we visit and the apps and services we use to the messages we send across the Internet. ISPs have insight into extremely sensitive information, and they can and do seek to profit in a big data marketplace that denies consumers control of their private information. At its worst, this perpetuates a system where people can be denied social and economic opportunities based on stereotypes, racial profiling, and other potentially discriminatory determinations.

### **The FCC’s NPRM Proposes Measured Approaches for Addressing These Harms.**

Currently, consumers have little knowledge of and no control over how companies like AT&T, Verizon, Comcast and other ISPs use their personal information. The proposed rules create a framework by which broadband providers must obtain their users’ affirmative consent in most cases before sharing or selling their private information, especially to third parties with whom those consumers have not entered a commercial relationship.

### **The Law Is Imperative, Not Comparative; The FCC Doesn’t Need to Find That ISPs Are a Bigger Threat to Act.**

Broadband ISPs have compared themselves to other players in the “Internet ecosystem,” arguing that treating ISPs differently than content or “edge” providers disadvantages them in the personal information and advertising market. It is true that ISPs and edge companies alike can sell personal information to the same kinds of data brokers, and ISPs’ use of that information implicates many of the same concerns that edge providers’ use does. However, the clear language of the statute directs the FCC to safeguard this information from misuse by ISPs – regardless of what other Internet companies may do with it. In light of ISPs’ privileged position as gatekeepers for all Internet traffic, plus the lack of competition in the broadband market the limits people’s ability to choose more privacy protective ISPs, this separate privacy law for broadband providers makes sense. As the FCC has recognized, consumers can choose not to visit websites or use services that market their personal information, but Internet access service providers’ view into personal data is pervasive. People who need ISPs to connect them to the Internet should not be required to give up their privacy without informed consent.