



Consumer Privacy and Data Security

Rural Carrier Commitment

Small, rural broadband providers live and work in the areas they serve and are committed to protecting their customers' personal information, guided by the hallmarks of notice, choice and security for the consumer and industry best practices. Marketplace experience indicates that regulation of consumer data practices is most effectively led by the Federal Trade Commission (FTC) through dynamic, market-driven standards that are flexible, scalable and able to rapidly respond to evolving threats.

Consumer-Oriented Framework

- Consumers need and benefit from a uniform expectation of privacy and security for their online activities, and risk harm if the levels of protection for their data differ among broadband, app, device and edge providers.
- Any framework for consumer privacy and data security should therefore:
 - » Promote standards that apply equitably across sectors without regard to the line of business of a particular holder of data;
 - » Balance consumer interests in privacy protection and a flourishing market by recognizing various layers of data sensitivity and differences in the categories of affiliates and third parties with which it may be shared; and
 - » Rest upon three principles:
 - **Notice:** Clear, conspicuous explanation of privacy practices
 - **Choice:** Consumer determines which entities can access various levels of sensitive data
 - **Security:** Holders protect data in accordance with best practices

FTC Experience

- Fundamental consumer protection and retail marketplace competition issues are more appropriately overseen by the FTC, which is far better versed in such issues, is an expert in the oversight of mass-market services generally (as well as privacy more specifically), and can “see across industries” better than other agencies.
- The FTC already accords consumer broadband data privacy the same scrutiny that applies to guard against unfair or deceptive trade practices—regulating obligations of providers to maintain confidentiality; to collect data only in a manner consistent with stated policies; and to protect that data.

Conclusion

A uniform approach to consumer privacy that treats all online data consistently will ensure consumers enjoy a consistent expectation of privacy, while a level playing field among market players will promote innovation and competition. The FTC, pursuant to its statutory authority and the principles of Section 5 of the FTC Act, is best positioned to oversee this market and safeguard the principles of notice, choice, and security that are essential to consumer confidence and safety.

Finally, several recent legislative proposals included narrowly drawn exemptions or safe harbors for small businesses that hold or sell very little consumer data, and such carefully-targeted relief should remain part of the privacy debate to avoid disproportionate impacts on entities with limited resources that pose limited risks.