

Clients & Friends Memo

Broadband Internet Service Providers In Regulatory Limbo After Repeal of FCC Privacy and Data Security Rules

April 20, 2017

Potentially signaling the end of the short-lived stint by the Federal Communication Commission (“FCC”) to regulate consumer data privacy on the internet, the Trump Administration recently repealed Obama-era data privacy and security rules for broadband providers. The action, passed by Congress and signed by President Trump pursuant to the Congressional Review Act, completely rescinds the rules that would have gone into effect later this year. While the move has been welcomed by industry insiders, it leaves broadband providers in regulatory limbo as the Trump Administration seeks to determine which agency and what rules will oversee data protection in this sector going forward.

The FCC’s Privacy Order and Its Repeal

In November 2016, the FCC released comprehensive consumer privacy and data security rules (the “2016 Privacy Order”) for broadband internet access service (“BIAS”) providers.¹ BIAS providers offer consumers high-speed, continuous access to the internet, typically through cable, telephone, wireless, or fiber-optic connections. They are different from entities such as Amazon and Facebook, which do not provide connections to the internet but rather offer internet services such as cloud storage, messaging, news, video streaming, and online shopping and are regulated, with respect to data privacy matters, by the Federal Trade Commission (“FTC”).

The 2016 Privacy Order would have, among other things, required BIAS providers to obtain affirmative customer consent (“opt-in” consent) prior to using and sharing, for commercial purposes, confidential customer data, such as a user’s web browsing history, application usage history, or geo-location information, and prohibited them from refusing to serve customers who did not provide such consent. It also required BIAS providers to adopt “reasonable measures” to protect customer data from unauthorized disclosure, and required them to give notice to customers affected by any data breach “without unreasonable delay” but not later than 30 days after determining that a breach had occurred.

¹ *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, 31 FCC Rcd 13911 (2016), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf.

Repeal of the 2016 Privacy Order comes as a welcome development for industry groups, which vigorously opposed them both prior to and subsequent to their finalization. In January 2017, the FCC received multiple petitions to reconsider and stay the order.² The BIAS industry complained that some of the new rules – particularly the opt-in rule for the use of sensitive customer information – put BIAS providers at a competitive disadvantage because the rules were more restrictive than FTC rules that applied to other internet entities such as Amazon and Facebook and, further, would have required costly updates to BIAS providers' systems. In response, the FCC – now with a Chairman appointed by President Trump and a majority of Republican-appointed commissioners – reversed course and, on March 1, 2017, voted to stay some of the provisions of the 2016 Privacy Order that had been due to come into effect.³ Shortly thereafter, Congress and President Trump used their authority under the Congressional Review Act to completely rescind the 2016 Privacy Order.⁴

Is Net Neutrality Next?

To answer the question of where the Trump Administration might go from here first requires an explanation of how the FCC came to be responsible for regulating data privacy and security for BIAS providers in the first place.

Until 2015, BIAS providers, like other internet service and content providers, were not considered to be “common carriers” by the FCC and, thus, were not subject to data privacy regulation by the FCC. Instead, for matters concerning data privacy and protection, BIAS providers looked to the FTC. That changed in 2015, when the FCC issued the “Open Internet Order,”⁵ which reclassified BIAS providers as “telecommunications services” and, therefore, subjected them to common carrier regulation by the FCC under Title II of the Communications Act of 1934 (“Title II”). Among other things, Title II requires “telecommunications services” to furnish services to customers “upon reasonable request” and prohibits “unjust and unreasonable discrimination” in the services that common carriers provide. Title II further provides that “telecommunications services” have a duty to protect the privacy of customer data.⁶

This reclassification was necessary for the FCC to promote and establish, as the centerpiece of the Open Internet Order, “net neutrality” rules for BIAS Providers. “Net neutrality” rules require BIAS

² See, e.g., Joint Petition for Stay, available at <https://ecfsapi.fcc.gov/file/101270254521574/012717%20Petition%20for%20Stay.pdf> (“Stay Petition”).

³ See Order Granting Stay Petition, available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-19A1.pdf.

⁴ See S.J. Res. 34 – 115th Congress, available at <https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34/text>.

⁵ See *Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rcd 5601 (2015), available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf.

⁶ See 47 U.S.C. § 222(a) (“Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers.”).

providers to allow users equal access to all otherwise lawful internet websites, content, and services, without favoring or restricting access, whether the websites are owned or controlled by the service providers' affiliates, business partners, or competitors. For example, absent net neutrality rules, a BIAS provider might, in exchange for a fee or other consideration, agree with a video sharing website, such as YouTube, to provide its customers with faster and better access to YouTube than to a rival video sharing website, such as Vimeo.

Previous attempts by the FCC to impose net neutrality rules on BIAS providers had been rejected by the Court of Appeals for the D.C. Circuit. Most recently, in 2014, the D.C. Circuit held that the FCC did not have the authority to impose net neutrality rules on BIAS providers because they were not subject to the common carrier rules under Title II.⁷ In response, the FCC reclassified BIAS providers as common carriers in its Open Internet Order. The 2016 Privacy Order was an attempt by the FCC to further define the data privacy and protection rules that applied to BIAS providers under Title II.

The Trump Administration now seeks to return the BIAS industry to privacy oversight by the FTC, as both the current FCC and FTC Chairpersons have indicated that "jurisdiction over broadband providers' privacy and data security practices should be returned to the FTC, the nation's expert agency with respect to these important subjects."⁸ However, this is easier said than done, as it would require that the FCC revoke the Open Internet Order and its accompanying net neutrality rules. Such a move would be favored by the BIAS industry and the new Chairman of the FCC, Ajit Pai, who regards the net neutrality rules as a "mistake,"⁹ but would be met by criticism from many major internet content providers and services, such as Amazon, Google, and Facebook.¹⁰

In the meantime, the FTC is without authority to regulate BIAS providers regarding data privacy, as the FTC Act contains an express exemption of FTC jurisdiction for common carriers.¹¹ Further complicating matters is an August 2016 decision of the Court of Appeals for the Ninth Circuit, which interpreted the FTC's common carrier exemption as including *all* activities of any entity designated as a common carrier, even those activities that are unrelated to the entity's common carrier business and which otherwise might be subject to FTC jurisdiction if they were carried out

⁷ See *Verizon v. F.C.C.*, 740 F.3d 623 (D.C. Cir. 2014).

⁸ See *Joint Statement of Acting FTC Chairman Maureen K. Ohlhausen and FCC Chairman Ajit Pai on Protecting Americans' Online Privacy*, available at <https://www.ftc.gov/news-events/press-releases/2017/03/joint-statement-acting-ftc-chairman-maureen-k-ohlhausen-fcc>.

⁹ See *Remarks of Federal Communications Commission Chairman Ajit Pai at the Mobile World Congress* (February 28, 2017), available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-343646A1.pdf.

¹⁰ See *Google, Facebook and Amazon write to FCC demanding true net neutrality*, *The Guardian* (May 7, 2014), available at <https://www.theguardian.com/technology/2014/may/08/google-facebook-and-amazon-sign-letter-criticising-fcc-net-neutrality-plan>.

¹¹ See 15 U.S.C. § 45(a)(2).

by a separate entity.¹² If the Ninth Circuit position were to stand and be adopted by other Circuits – the FTC is currently seeking a rehearing *en banc* – the FCC suddenly might find itself responsible for regulating a host of non-common carrier related business activities merely because they are provided by entities that have been designated as common carriers under Title II.

Many large BIAS providers have faced this uncertainty by pledging to take “reasonable measures to protect customer information” and notify “consumers of data breaches as appropriate” in accordance with the existing FTC data privacy framework (*i.e.*, ensuring that their data security practices are not “unfair or deceptive” in contravention of Section 5 of the FTC Act).¹³

BIAS providers are also presently subject to a host of state laws concerning data privacy and protection, including at least 48 state data breach notification laws, the most recent of which was enacted in New Mexico.¹⁴ These laws typically require businesses to notify the state authorities, affected customers, and major credit reporting agencies when the state’s residents’ confidential personal information, such as social security or driver’s license numbers, credit card numbers, and passwords, have been exposed through a data breach. In addition, some states, such as Massachusetts¹⁵ and California,¹⁶ also require businesses to implement and maintain reasonable security procedures and practices to protect customer information. Finally, some states maintain consumer protection laws, which, similar to the FTC Act, generally protect against unfair or deceptive trade practices and have been used by state attorney generals to penalize companies that fail to protect customer data.¹⁷

Conclusion

The Trump Administration’s repeal of the 2016 Privacy Order has provided a respite for the BIAS industry from vigorous new requirements that would have gone into effect this year. However, it also has created a period of regulatory uncertainty as regulators determine the way forward, including the fate of the Open Internet Order. In the meantime, BIAS providers should, as they have promised, continue to follow reasonable data privacy and protection practices, consistent at least with those required by the FTC, and also carefully consider whether any other applicable federal or state data privacy laws apply to their business.

¹² See *F.T.C. v. AT&T Mobility LLC*, 835 F.3d 993 (9th Cir. 2016). The FTC has sought rehearing *en banc*.

¹³ See Stay Petition, ISP Privacy Principles.

¹⁴ See New Mexico H.B. 15, Data Breach Notification Act (2017).

¹⁵ See Mass Gen. Laws Ann. ch. 93H, § 2.

¹⁶ See Cal. Civ. Code § 1798.81.5(b).

¹⁷ See, e.g., Press Release, A.G. Schneiderman Announces \$100K Settlement with E-Retailer after Data Breach Exposes Over 25K Credit Card Numbers, N.Y. State Attorney General’s Office (Aug. 5, 2016), available at <https://ag.ny.gov/press-release/ag-schneiderman-announces-100k-settlement-e-retailer-after-data-breach-exposes-over>.

If you have questions, please contact any of the following attorneys or your Cadwalader contact:

Joseph Moreno	+1 202 862 2262 +1 212 504 6262	joseph.moreno@cwt.com
Joseph Facciponti	+1 212 504 6313	joseph.facciponti@cwt.com
Keith M. Gerver	+1 202 862 2381	keith.gerver@cwt.com
Peter Carey	+1 202 862 2339	peter.carey@cwt.com