Net neutrality, privacy and VoIP: tension between US federal and state enforcers

John Nakahata, Adrienne Fowler and Stephanie Weiner
Harris, Wiltshire & Grannis LLP

In the wake of the 2016 election of President Trump and Republican majorities in both houses of Congress, US telecommunications policy has seen a profound change in direction toward deregulation. In a classic action-reaction frequently seen in the United States, as the Federal Communications Commission (FCC) has taken deregulatory steps, states – and even some local governments – have looked for ways to reinstitute at least some of the withdrawn protections. We focus here on some examples of the interaction between deregulatory telecommunications policy at the federal level and the reaction in the states.

Specifically, we focus on changes surrounding 'net neutrality' rules, communications privacy and data security, and the regulatory status of Voice over Internet Protocol (VoIP) services. Net neutrality and communications privacy rules adopted in the Obama Administration were overturned in the last year. For VoIP, although not an area where FCC policy has shifted, a couple of states have pushed forward to assert regulatory authority over 'fixed VoIP', with the matter now before the courts.

For parties considering deals in the telecommunications and internet space, this activity reinforces the need to pay attention to state, and even local, regulatory structures, as well as those of the FCC and other federal government entities such as the Committee on Foreign Investment in the United States.

Net neutrality

In the past year, after a change of leadership resulting from the inauguration of President Trump, the FCC dramatically reversed its regulatory approach to residential broadband internet access service and net neutrality. Just a few years earlier, in 2015, the FCC had held that broadband service should be treated as a 'telecommunications service', which under the relevant statute permitted the FCC to regulate it as a common carrier service. The FCC has the authority to apply myriad regulatory obligations to common carrier services. While the FCC forbore from, and thus declined to apply, many of the common carrier obligations the FCC had historically applied to voice services, the FCC adopted strong net neutrality rules, including:

- bright line rules against broadband provider blocking, throttling or entering pay-for-priority traffic arrangements;
- a general conduct standard preventing broadband providers from unreasonably interfering or disadvantaging communications between online companies and consumers; and
- oversight over broadband providers' interconnection practices for their residential networks.

In December 2017, however, the FCC adopted a new decision that reversed – in nearly all respects – the Commission's prior approach. Instead of classifying broadband internet access service as a common carrier service, the FCC reclassified broadband as an 'information service' – returning to a classification the FCC had applied from 2005 to 2015. Under the relevant statute, an information service cannot be treated as a common-carrier service – in other words, the FCC can impose fewer regulatory obligations on information services than it can on common carrier services. The FCC also rescinded the 2015 rules against blocking, throttling, pay-for-priority arrangements and unreasonable interference and disclaimed any statutory authority for oversight over interconnection practices. The Commission retained a scaled-back version of the transparency rule, requiring broadband providers to disclose information about their service, including the extent to which the provider is engaged in blocking, throttling and paid prioritisation. The FCC concluded that this rule combined with existing antitrust and consumer protection laws would be sufficient to protect against any broadband provider conduct that would harm net neutrality. Finally, the FCC stated that it was pre-empting any state or local measures inconsistent with this federal deregulatory approach (ie, the FCC asserted that its removal of rules precluded states or localities from adopting new net neutrality rules).

The FCC's retreat from its prior net neutrality rules led many states to seek to put in place net neutrality protections for consumers and businesses in their states, notwithstanding the Commission's language on pre-emption. Some of these approaches utilise the state's power as a purchaser of services, rather than its utility regulation powers. At the time of writing, the governors of five states (Montana, Hawaii, New Jersey, New York and Vermont) have signed executive orders stating that an Internet Service Provider (ISP) (ie, a broadband provider) with a government contract with the state must not block, throttle or degrade internet content and must not engage in paid prioritisation, including in some cases a prohibition on requiring consumers to pay different rates to access specific kinds of content or applications online.

Moreover, 25 states have introduced legislation to support some form of net neutrality protection for consumers in their state. These state bills range from resolutions in support of undoing the FCC's decision, to bills that would impose net neutrality conditions on broadband providers doing business with state agencies or participating in state programmes, and bills that would make broadband provider practices, such as blocking, throttling and paid prioritisation, unlawful under existing state consumer protection laws. On 7 March 2018, Washington state enacted the first of these bills into law, providing that broadband providers that block content, impair or degrade traffic, or engage in paid prioritisation violate the state's law against unfair or deceptive acts in trade or commerce or unfair methods of competition. The Oregon legislature has also passed a bill that requires the state to contract only with broadband providers that comply with net neutrality protections. Other state bills are moving through various stages of the state legislative process; in some cases, quite quickly.

The FCC's pre-emption decision and these state actions evince plainly different views with respect to the line between federal and state authority to regulate net neutrality and, more generally, ISPs. As a result, this issue will be litigated from both sides. With respect to federal deregulation, 22 state attorneys general, Santa Clara County, California (the home of Silicon Valley) and the California Public Utilities Commission, are among the many parties that have already sought judicial review of the FCC's decision to scale back federal net neutrality protections and pre-empt state and local net neutrality regulation. Court challenges are also expected with respect to the state actions that impose regulations. Although no party at the time of this writing has challenged either the state executive orders or legislation on net neutrality, broadband providers or their trade associations are expected to bring such challenges to forestall a patchwork of state-by-state regulation. While the outcome of both the federal litigation and any state challenge remains unclear, these net neutrality developments illustrate the US telecommunications policy dynamic of federal deregulation followed by state regulation that has recurred on several fronts.

Communications privacy and data security

As a precursor to its reversal of policy on net neutrality, the federal government has made several notable retreats in its regulation of communications privacy and data security. In April 2017, the US Congress passed, and President Trump signed, legislation to rescind regulations that the Obama-era FCC had adopted to govern broadband providers' use, disclosure and protection of subscribers' personally identifiable information. As a result of this Congressional action, it was unclear whether the FCC retained the power to adopt any replacement regulations regarding ISP privacy. The FCC's subsequent reversal of net neutrality cleared up any ambiguity on that score: by reclassifying broadband as an information service, the FCC relinquished any remaining ability it had to regulate ISPs' data privacy and security practices. Instead, at the federal level, oversight of ISPs' privacy and data security practices will fall to a different agency, the Federal Trade Commission.

This shift has a number of practical implications. The FTC has decades of experience in bringing privacy and data security-related enforcement actions, and so brings considerable substantive expertise to the table. But Congress has put very strict limits on the FTC's ability to adopt ex-ante regulations, with a few exceptions. (As of writing, both houses of the US Congress have introduced legislation that would give the FTC the authority to promulgate regulations regarding ISPs' privacy and data security practices; these bills appear unlikely to pass.) As a result, we expect that the FTC will continue to act by bringing enforcement actions that react to any alleged bad practices that ISPs commit after the fact and evaluate ISP privacy and data security practices on a case-by-case basis.

The Federal Trade Commission Act, however, does not pre-empt state privacy and consumer protection laws. In most states, attorneys general already have broad authority to bring enforcement actions in order to protect consumers within their states from unfair or deceptive commercial practices. Many attorneys general have taken the position that certain data practices can be unfair and deceptive; more attorneys general may be considering using this general power against ISPs and voice communications providers in the near future. Accordingly, state attorneys general can and do enforce state privacy and consumer protection laws, including with respect to data security and breaches.

Moreover, legislators in many states see the FTC's current authority as insufficient to protect broadband subscribers' privacy. Before Congress rescinded the FCC's ISP privacy rules, only two states (Minnesota and Nevada) had laws on the books that regulated ISPs' privacy and data security practices. Since Congress's rescission, 24 states and the District of Columbia have introduced legislation designed to limit ISPs' ability to collect or disclose subscribers' personal information without express permission or impose data security requirements on ISPs' treatment of subscribers' personal information. Certain local governments have been even more aggressive. Regulators in Seattle adopted a rule requiring ISPs who have been granted franchise authority (ie, an authorisation to utilise public rights of way controlled by the local government) to operate in the city to notify and get opt-in permission from subscribers before disclosing subscribers' personal information, such as their web browsing histories, to a third party. The township of Falls, Pennsylvania adopted a similar measure, although companies who currently have a franchise agreement to operate in the city are entitled to delayed implementation.

In a less-publicised change, through the same legislation that rolled back the FCC's broadband privacy rules, Congress also significantly curtailed federal regulation of privacy and data security for voice communications by rescinding updates to the FCC's voice privacy rules. Under these updates, the FCC would have limited voice providers' use of virtually any personally identifiable information collected from subscribers. As a result of Congressional action, however, the FCC's voice privacy rules only cover a relatively narrow segment of subscriber data known as 'customer proprietary network information' (CPNI). Subscriber name, contact information, social security number, birthday and other forms of personal data do not qualify as CPNI – and, thus, are not subject to FCC regulations. Ten states and the District of Columbia are considering legislation or regulations that would limit voice communications providers' data practices with respect to any personally identifiable information, not just CPNI.

If ISP-specific or voice-communication-provider-specific laws pass in a given state, communications companies can expect to come under scrutiny for their privacy practices and, in some instances, face enforcement action. Even absent the passage of specific legislation, however, state attorneys general may increase their focus on communications privacy.

Broad-based federal consumer data privacy and security legislation could overtake the recent reduction in federal oversight of communications privacy. The US has traditionally had specific federal rules only for relatively narrow categories of information, such as certain types of financial information held by financial institutions and healthcare information held by certain types of entities. Consumer advocates have for many, many years pushed for baseline consumer data privacy and security legislation, which would mandate certain minimum protections that would apply to all personally identifiable information that entities gather from consumers, including communications-related data. In the wake of several high-profile data-related events, including the Cambridge Analytica controversy, some members of Congress are renewing calls for such baseline legislation. At the time of writing, it is difficult to assess the likelihood that legislation will garner significant support.

VoIP

Unlike net neutrality and consumer privacy and data security, the latest developments with respect to state regulation of VoIP are not the result of new federal deregulatory actions. Instead, they are the latest phase in a long-running tussle between some state public utility commissions and VoIP providers as to whether VoIP providers must comply with at least some state regulations applicable to traditional telephone companies. In general, stretching back to 2004, the FCC has preferred to chart a nationwide course for what is termed 'interconnected VoIP' – a VoIP service capable of placing calls to and receiving calls from traditional, circuit-switched telephones. The FCC has selectively imposed on interconnected VoIP a variety of regulatory duties, including emergency calling, consumer privacy, law enforcement access, intercarrier compensation payments, universal service and other regulatory fees, and service discontinuance regulation. However, the FCC has done so without classifying interconnected VoIP as either a 'telecommunications service' subject to common carrier duties, or as an 'information service' that cannot be subject to common carrier duties.

While it has been clear since 2007 that the FCC has pre-empted state regulation of 'nomadic' interconnected VoIP – which is usually an 'over-the-top' service delivered over an internet access service – the law has been less clear with respect to 'fixed' interconnected VoIP. Unlike nomadic services, which can change locations, fixed VoIP services are usually facilities-based and provided from a fixed, known location. In 2013, the Vermont Supreme Court upheld a Vermont Public Service Board ruling that a company providing a fixed interconnected VoIP service was a 'telecommunications service' under state law, although it remanded for further consideration as to whether the service was a telecommunications service or information service under federal law. In February 2018, the Vermont Public Service Board concluded that fixed interconnected VoIP was also a telecommunications service under federal law, and not pre-empted, although it continues to consider the extent of state regulation of fixed interconnected VoIP. In 2015, the Minnesota Public Utilities Commission held that a fixed interconnected VoIP service provided by a cable company was a local telephone service under state law, and thus subject to state regulation, and was not pre-empted by federal regulations. In 2017, a United States federal court in Minnesota concluded that the Minnesota Public Utilities Commission was wrong, and that the cable provider's fixed interconnected VoIP service was an 'information service' under federal law, and that state regulation was therefore pre-empted. An appeal to the United States federal appeals court followed.

As of this writing, that case remains pending before the federal appeals court. The court could decide that fixed interconnected VoIP is a telecommunications service, an information service, not pre-empted regardless or classification, or, as the FCC has suggested, pre-empted regardless of classification. While a federal court classification decision that fixed interconnected VoIP was a telecommunication service or that state regulation was not pre-empted would not necessarily preclude a future FCC decision reaching a different conclusion – as occurred previously with respect to the classification of broadband internet access – it could create greater regulatory uncertainty in those states in which legislatures have not removed VoIP from the

jurisdiction of state regulatory commissions. Of particular significance for parties contemplating a transaction, if the court rules that fixed interconnected VoIP is a telecommunications service for which state regulation is not pre-empted, state prior approval of transactions involving transfer of control could be required, depending upon which state is involved. Depending upon the state's processes, because the FCC does not require prior approval of transfer of control of interconnected VoIP providers, this could lengthen the period needed between signing a deal and close.

Conclusion

These are just three examples of the ongoing push and pull between federal and state telecommunications regulation in the United States. Whenever the FCC has acted to deregulate, proponents of a particular regulation have turned to the states. This tension over the respective federal and state or local roles is not limited to deregulation, however. Over the coming years, it is likely that this tension will continue to play out, including in areas such as wireless tower siting for 5G. The FCC has made clear that it views 5G deployment as a priority and that it seeks to streamline the barriers to erecting the thousands of small cells needed to densify wireless networks for 5G, especially in urban areas. Existing statutes give the FCC some limited authority to pre-empt local restrictions or failures to act with respect to tower siting applications.

Accreditation: Reproduced with permission from Law Business Research Ltd. This article was first published in Getting the Deal Through – Telecoms & Media 2018 (Published: July 2018). For further information please visit www.gettingthedealthrough.com.

HWG | HARRIS, WILTSHIRE & GRANNIS LLP

John Nakahata **jnakahata@hwglaw.com**
Adrienne Fowler **afowler@hwglaw.com**
Stephanie Weiner **sweiner@hwglaw.com**

1919 M Street NW, Suite 800
Washington, DC 20036-3537
United States

Tel: +1 202 730 1300
Fax: +1 202 730 1301
www.hwglaw.com