SENATE……..No. 2376

The Commonwealth of Massachusetts

Report of the Special Senate Committee
on
Net Neutrality
entitled:

Net Neutrality and Consumer Protection: A Commonwealth Concern

(pursuant to Senate Order - Senate, No. 2263)

March 2018

Net Neutrality and Consumer Protection: A Commonwealth Concern

Report of the Special Senate Committee on Net Neutrality and Consumer Protection

March 23rd, 2018

Massachusetts Senate
Harriette Chandler
Senate President

Senator Cynthia Stone Creem, Chair
Senator Bruce E. Tarr, Vice Chair
Senator Mike Barrett
Senator Jamie Eldridge
Senator Eric Lesser
Senator Barbara L'Italien
Senator Patrick O'Connor

Senate Committee on Net Neutrality and Consumer Protection

Senator Cynthia Stone Creem, Chair

It shall be the duty of the Senate Committee on Net Neutrality and Consumer Protection to coordinate a policy response to the federal government's decision to repeal rules on net neutrality. The committee shall review the Federal Communications Commission's order entitled "Restoring Internet Freedom", which was adopted on December 14, 2017. The committee shall make recommendations concerning the Senate response to this order, with the goal of protecting Massachusetts consumers. The committee may file its recommendations including, but not limited to, legislation, with the clerk of the Senate no later than April 13, 2018.

This report was prepared by Senator Creem with input by other members of the Special Committee.

The Committee would like to acknowledge the assistance of Senator Creem's staff, Staff Attorney Sarah Chase and Chief of Staff Richard Powell.

TABLE OF CONTENTS

Executive Summary

This report will examine, first, the history of the Federal Communication Commission's actions on net neutrality and broadband privacy and the effect of the Federal regulatory retreat from these important legal protections. The report will outline the history of this Committee, including its scope and methodology. Then, the report will assess the Federal legal issues inherent in any state action in this area, including a summary of the multi-state litigation surrounding the repeal of the net neutrality rules. Finally, the report will provide a legislative proposal for Massachusetts, with lessons learned from other states along with some original ideas.

How This Report Was Developed

The Committee was created to coordinate a thorough and thoughtful investigation on the impacts of the recent Federal Communication Commission ("FCC") repeal of certain consumer protection regulations with a view toward thoroughly understanding this nuanced and technically complex issue. The Committee's examination of the regulatory landscape involved a February 6th, 2018, public hearing, at which numerous stakeholders testified; review of relevant statutes and regulations, both Federal and state; study of the FCC's "Restoring Internet Freedom Order" of 2017 along with the FCC's "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services Order" of 2016 and the FCC's "Open Internet Order" of 2015; numerous meetings with state agencies, consumer advocacy groups, industry representatives, and other relevant stakeholders; and informal discussions with these entities and with technology personnel.

Key Findings

Based on testimony heard at an informational hearing, written testimony received by the Committee and numerous meetings with stakeholders and experts, the Committee finds that the FCC repeal of net neutrality protections opens the door to network management practices that could harm consumer choice, technological innovation and the free flow of information on the internet. These would be significant harms to the Commonwealth, which prides itself on its strong consumer protection laws, its expanding high-tech business sector and a vibrant democracy of engaged citizens. The Commonwealth has already devoted considerable resources to promoting broadband access for all residents and should strive to maintain its commitment to high-quality universal internet service. The Committee also finds that state action is required to ensure the privacy of consumers is protected from any misuse of data by internet service providers.

Recommendation of the Committee

The Committee considered many options to achieve its mission of protecting consumers and the open internet in Massachusetts. Some of these approaches have been proposed in other states [see Legislative Options Section]. In the end, the Committee recommends that the Massachusetts Senate should take legislative action and hereby proposes legislation to address the findings contained within this report [see Appendix II]. The Committee will hold a public hearing on this legislative proposal and seek feedback from any interested parties [see Legislative Proposal Section for a summary of each section of the bill].

Introduction

Committee Scope

The Massachusetts Senate Special Committee on Net Neutrality and Consumer Protection was established on January 18th, 2018, to coordinate a policy in response to the federal government's December, 2017, decision to repeal rules on net neutrality. The Committee also heard testimony and conducted research on the related issue of broadband privacy during the course of its work.

Members

The Committee was chaired by Senator Cynthia Stone Creem (D-Newton), with Senator Bruce E. Tarr (R-Gloucester) serving as Vice Chair, and Senators Mike Barrett (D-Lexington), Jamie Eldridge (D- Acton), Eric Lesser (D- E. Longmeadow), Barbara L'Italien (D-Andover) and Patrick O'Connor (R- Weymouth) as members.

Authority: Establishing Order

Offered by Senator Cynthia S. Creem relative to forming a special senate committee on net neutrality and consumer protection

Ordered, that there shall be a special committee on the part of the Senate on net neutrality and consumer protection. The committee shall consist of 7 members of the Senate, 5 of whom shall be appointed by the senate president and 2 of whom shall be appointed by the senate minority leader. The committee shall review the Federal Communications Commission's order entitled "Restoring Internet Freedom", which was adopted on December 14, 2017. The committee shall make recommendations concerning the Senate response to this order, with the goal of protecting Massachusetts consumers. The committee may file its recommendations including, but not limited to, legislation, with the clerk of the Senate not later than April 13th, 2018.

Committee Process

Informational Hearing

The Committee held a hearing on February 6th, 2018 at 11:00am during which the Committee heard testimony by invitation only. The invited guests included Senator Markey, United States Senate; Senator Warren, United States Senate; Dennis McDermitt, Massachusetts Executive Office of Technology and Security Services, Chief Security Officer;

Massachusetts Attorney General Maura Healey; Professor David Choffnes, Northeastern University; Professor Daniel Lyons, Boston College Law School; Ari Glantz, New England Venture Capital Association; Matt Wood, Free Press; Gerry Keegan, CTIA; Sarah Morris, Open Technology Institute; Tim Wilkerson and Matt Brill, New England Cable & Telecommunications Association; and Kade Crockford, ACLU of MA.

A complete recording of the hearing can be viewed at:
https://malegislature.gov/Committees/Detail/S63/Hearings

Full copies of all written testimony received by the Committee have been filed with the Senate Clerk's office and will be provided upon request.

Legal History

Although there has been some variation in definitions, net neutrality is generally considered to encompass a ban on three practices by internet service providers (ISP) as they manage internet traffic passing through their networks. The three disfavored network management practices are:

(1) "Blocking," in which an ISP completely prevents a customer from accessing certain websites or content;

(2) "Throttling," in which an ISP slows down the speed that a customer can connect to certain websites and content; and

(3) "Paid Prioritization," in which an ISP accepts a fee or other compensation in exchange for sending some content to consumers faster than other content.

The following is a history of the Federal legal history of net neutrality regulation.

History of FCC Action on Net Neutrality

In 2005 the Federal Communications Commission ("FCC") unanimously adopted a bipartisan Internet Policy Statement, which was enforceable for only certain broadband providers. They relied on ancillary jurisdiction under Title I of the Communications Act of 1934. The American Library Association ("ALA") sued the FCC in 2005 for their broadcast flag regulations.[1] The court ruled in favor of ALA that the FCC had overextended its authority and stated that: "the FCC has no authority to regulate consumer electronic devices that can be used for receipt of wire or radio communication when those devices are not engaged in the process of radio or wire transmission."[2]

Several Comcast subscribers filed a complaint with the FCC in 2007 that Comcast was violating the FCC's Internet Policy Statement on peer-to-peer networking applications.[3] The FCC in response created an order that Comcast had to disclose the company's new approach to managing bandwidth demand.[2] Comcast then sued the FCC in 2010 saying that the FCC did not have authority over the company's management practices under Section 4 (i) of the Communications Act of 1934.[4] Furthermore, Comcast took the position that the FCC's adjudicatory action bypassed the rulemaking requirements of the Administrative Procedure Act, violated the notice requirements of the Due Process Clause,

[1] Am. Library Ass'n v. FCC, 406 F.3d 689, 692 (D.C. Cir. 2005).
[2] *Id*.
[3] In re Formal Compl. of Free Press & Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications, 23 F.C.C.R. 13,028 (2008) (Order).
[4] *Comcast Corp v. FCC,* 600 F.3d 642 (D.C. Cir. 2010).

and that the order was arbitrary and capricious. The court ruled in favor of Comcast that Title I does not give the FCC ancillary authority over Comcast's network management practices.

Later in 2010, the FCC released new net neutrality rules that built off of the previous ones. These new rules ensured an open Internet with transparency, no blocking, no unreasonable discrimination, and reasonable network management. Verizon then sued the FCC saying these rules extended beyond their authority.[5] The court ruled in favor of Verizon, striking down the rules. Due to this ruling, the FCC issued new rules (known as the Open Internet Order of 2015) on March 12th, 2015. The rules included no blocking, no throttling, no paid-prioritization, and no unreasonable interference or unreasonable disadvantage standard for internet conduct. The rules also outline the formal complaint procedures and issues of confidentiality of proprietary information. This time the orders were under Title II of the Communications Act of 1934, reclassifying broadband service as a telecommunications service.

The Telecomm Association, along with other providers, filed a law suit against these new rules shortly after.[6] They claimed that some of the rules violated the First Amendment and that the FCC lacks statutory authority to reclassify broadband service. Furthermore it was argued that, even if they could reclassify broadband service, these new rules were arbitrary and capricious. In addition, the Telecomm Association claimed that the FCC could not classify mobile broadband as a commercial mobile service and impermissibly forbore from certain provisions of Title II of the Act. In the end, the court ruled in favor of the FCC and upheld the rules in full.

On December 14th, 2017, the FCC voted to repeal the 2015 Open Internet Order. The new Restoring Internet Freedom Order contains language reclassifying broadband services back under Title I, and thereby removing the extra common carrier requirements of the 2015 Order.[7] This newest Order, officially filed in the Federal Register on February 22nd, 2018, relies on a transparency regime in which ISPs are required to make certain disclosure which will thereby give consumers and related business the ability to make choices as to the ISPs with which they will do business. The FCC's rationale for removing many of the 2015 requirements was that the industry had become overregulated and this was stifling innovation and growth. Significantly for the purposes of this Committee, the 2017 Order also contains sweeping preemption language that is designed to prevent the states from legislating in this area. Unless stayed by a court as part of lawsuits filed challenging the Order's validity, the new rules will go into effect April 23rd, 2018.

---

[5] *Verizon v. FCC.,* 740 F.3d 623 (D.C. Cir. 2014).
[6] *U.S. Telecom Assoc. V. FCC*., No. 15-1063 (D.C. Cir. 2016).
[7] For full text see: https://www.fcc.gov/document/fcc-releases-restoring-internet-freedom-order

History of FCC Action on Broadband Privacy

In 1996 President Clinton signed the Telecommunications Act of 1996 into law. This new law updated the Communications Act of 1934, however it maintained the important distinction between Title I "information services," which were regulated more loosely, and Title II "common carriers," which were regulated more strictly. An important requirement imposed on common carriers under section 222 of Title II, *Privacy of Customer Information,* provides that:

> "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."[8]

Specifically the legislation, with exceptions, permits telecommunication carriers which receive or obtain customer proprietary network information (CPNI) through the provision of telecommunications services to only use, disclose, or permit access to individually identifiable CPNI in its provision of such telecommunications service, and that telecommunication carriers shall disclose CPNI, upon the written request by the customer, to any person designated by the customer.

Based on its authority under the Telecommunications Act, the FCC has attempted to protect the privacy of customer CPNI on several occasions. First, in 1998, the FCC released rules interpreting Title II, Section 222, to clarify the definition of telecommunication carriers. These rules contained guidelines which specified that a carrier must obtain permission to use, disclose, or permit access to a customer's CPNI for marketing purposes in all instances where the customer does not already subscribe to the specific customer service through that carrier.

U.S. West filed a lawsuit against the FCC to challenge these rules in the Tenth Circuit Court[9]. U.S. West stated that having customers "opt in" for approval violated the First Amendment by restricting carrier's ability to engage in commercial speech with customers. Furthermore, they argued that the 5th Amendment was violated because CPNI is the property of the carriers and these regulations would diminish their property values.[10] The court ruled in favor of U.S. West and argued that an "opt out" approach would be a less restrictive alternative.[11]

---

[8] 47 U.S.C. § 222.
[9] *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999).
[10] Julie Tuan, *U.S. West, Inc. v. FCC*, 15 Berkeley Tech. L.J. 353 (2000).
[11] *Id.*

To circumvent these legal challenges, the FCC in 2015 adopted a new approach. Prior to 2015, internet service providers were regulated under the authority of the Federal Trade Commission and were excluded from section 222 of the Communications Act. When the FCC released the *2015 Open Internet Order* the FCC reclassified internet service providers as telecommunication services, which made them now subject to all Title II requirements, including section 222. The FCC decided to make separate rules for net neutrality and internet privacy.

In 2016 the FCC released its proposed rules on internet privacy, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* which focused on transparency, choice, and security. The rules specified that customers, with exceptions, must be notified of their carrier's privacy policies, which must include:

> (1) the types of Customer Proprietary Information (CPI)[12] they collect and how the information is used;
>
> (2) the circumstances and categories of entities to which carriers disclose or permit access to each type of CPI collected and the purpose for which the information will be used by each category of entities;
>
> (3) customers' opt-in/opt-out approval rights with respect to CPI;
>
> (4) the mechanism for customers to grant, deny, or withdraw approval for the telecommunication carriers to use, disclose, or provide access to CPI;
>
> (5) the timing of notification to customers; and
>
> (6) how existing customers are notified in advance of material changes to carrier's privacy policies.

Further, the rules included provisions requiring that carriers must take reasonable measures to protect CPI from unauthorized use, disclosure, or access, and if there is a data breach the rules described how customers, the FCC, and federal law enforcement should be notified of the breach. Finally, the rules include a section outlining the effect on state laws:

> "The rules set forth in this subpart shall preempt any State law only to the extent that such law is inconsistent with the rules set forth herein and only if the Commission has affirmatively determined that the State law is preempted on a case-by-case basis. The Commission shall not presume that more restrictive State laws are inconsistent with the rules set forth herein."

[12] CPI includes: individually identifiable customer proprietary network information (CPNI), personally identifiable information, and content of communications.

These rules were set to go into effect in December 2017. However, they were prevented from being implemented by a Congressional Review Act Resolution introduced into the Senate and House on March 3rd, 2017 by Senator Jeff Flake (R-AZ) and Representative Marsha Blackburn (R-TN-7).[13]

The joint resolution passed the Senate on March 23rd, 2017, and the House on March 28th, 2017, and was signed into law by President Donald Trump on April 3rd, 2017. [14] The rules were therefore never implemented. In response, at least 19 states and the District of Columbia have introduced measures to adopt the repealed rules into state law.[15] For summaries of the ISP privacy bills introduced in Massachusetts, see Bills Filed in Massachusetts section below.

[13] *A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,"* S.J.Res.34 and H.J.Res.86, 115th Congress (2017-2018).
[14] Joint Resolution Disapproving FCC "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," Pub. L. 115–22, 131 STAT. 88 (2017).
[15] National Conference of State Legislatures, Privacy Legislation Related to Internet Service Providers (2/08/2018) http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx

Multistate Attorney General Lawsuit

States Involved

A multistate lawsuit has been filed by a consortium of state Attorney's General challenging the 2017 FCC *Resorting Internet Freedom Order* in the U.S. District Court of Appeals in D.C by the Attorneys General from California, Connecticut, Delaware, Hawaii, Illinois, Iowa, Kentucky, Maine, Maryland, Massachusetts, Minnesota, Mississippi, New Mexico, North Carolina, Oregon, Pennsylvania, Rhode Island, Vermont, Virginia, Washington and Washington, D.C.

Status of Lawsuit

The multistate lawsuit was filed by the parties mentioned above on January 16, 2018. The plaintiffs at first filed short statements of their intent to sue. Fuller complaints are expected to be filed within 60 days of the rule being officially entered into the Federal Register. Briefing in the case is expected in the summer and oral arguments will likely not be held until the fall with any decision not being reached until after that.

Grounds for Challenging FCC Action

Although full briefs have not been filed yet, the two general arguments that the Attorneys General may use to attack the order are both procedural and substantive. For procedure, the two large issues concern the notice and timing of the Order. The Attorneys General are likely to argue that any portions of the Act that were not noticed to the public with sufficient time to comment would be invalid. If a court invalidates the Order on procedural grounds, this would delay the implementation of all or some portion of the Order, but there is nothing to prevent the FCC from going through the proper procedure and then re-issuing the same order.

On substantive grounds, the Attorneys General will likely seek to permanently prevent the FCC's new Order from taking effect, by arguing that the FCC's actions were not sufficiently grounded in the record. Here, the argument will be that the Order is arbitrary, capricious, and an abuse of discretion under the Administrative Procedure Act.[16] A favorable finding on these grounds could prevent the Order from ever taking effect. However, this is all uncharted legal territory and the answers must be decided in court.

[16] 5 U.S.C. § 701 *et seq*.

Legal Issues Concerning State Action

The regulation of telecommunication services is predominately guided by the Communications Act of 1934, which was subsequently amended by the Telecommunications Act of 1996. As discussed above, the regulatory regimes established by the Communications Act that are significant here are simply called "Title I" and "Title II." Internet Service Providers ("ISPs") were briefly classified by the Open Internet Order of 2015 as a Title II "common carrier," subjecting them to more stringent regulations to ensure fairness and equity for all consumers of the internet. Also as a consequence, regulation of the internet moved wholly under the jurisdiction of the FCC, whereas regulatory jurisdiction of Title I services is traditionally exercised by the Federal Trade Commission ("FTC") with an ancillary role for the FCC.

These net neutrality rules were rescinded, however, by the Trump administration in late 2017, reclassifying ISPs again as a Title I "information service" and assuming a "light touch" regulatory approach to the internet. This reclassification also returned federal regulatory jurisdiction to the FTC, a role the agency has historically conducted alongside the states through shared enforcement of Unfair and Deceptive Acts and Practices (UDAP) laws. Although the FTC is the primary enforcer of Title I services, there have been instances in the past where the FCC has exercised its ancillary role to preempt patchwork state regulatory regimes. Sometimes the FCC has been successful, sometimes it has failed. The question then becomes: would a Massachusetts net neutrality law, which would almost certainly trigger a challenge from the FCC on preemption grounds, represent a regulatory regime that could withstand legal challenge?

Concerning the legal landscape surrounding such a potential law, it is key to note that preemption challenges to state-level regulations to telecommunication services, both Title I and Title II, are far from settled. There is precedent for both preemption success and failure for the FCC, and arguably the preferable course of action is not to look for any per se rules in the past (or expect any in the future), but to distinguish each service on a case-by-case basis.

Before addressing the questions outlined above, our attention must turn to the other legal argument the FCC will very likely use to challenge a potential state law: the Dormant Commerce Clause. In fact, it may be reasonable to expect that a Dormant Commerce Clause argument will constitute a more significant portion of the challenges to any state net neutrality law than preemption. For reasons to be explained below, it is reasonable to believe that a state net neutrality law can withstand both a preemption and Dormant Commerce Clause challenge.

Preemption

There are 3 general types of preemption: (1) express preemption; (2) field preemption; and (3) conflict preemption, also known as the "impossibility exception." For reasons outlined below, it is reasonable to believe a state net neutrality law can overcome all three prongs of a preemption attack.

Express Preemption

Express preemption occurs when a federal statute or regulation explicitly states that it shall preempt state and local law. In repealing the net neutrality rules issued under the Open Internet Order of 2015, the FCC has explicitly stated that its new rule preempts any state net neutrality laws. However, this is not the end of the inquiry. More is involved in federal preemption than an agency's own pronouncement. Express preemption is authorized only when the explicit language confirms Congressional intent to preempt state law.[17] "If a federal law contains an express pre-emption clause, it does not immediately end the inquiry because the question of the substance and scope of Congress' displacement of state law still remains."[18]

Has Congress communicated its intent to preempt state net neutrality laws? There is no substantive evidence of this, and the most relevant statutory evidence, Section 253 of the Communications Act of 1934, iterates precisely the opposite intent. Section 253 preserves the authority of states and municipalities to promulgate "requirements necessary to preserve and advance universal service, protect the public safety and welfare, ensure the continued quality of telecommunications services, and safeguard the rights of consumers[.]"[19] Furthermore, this policy is consistent with the historic regulatory regime of Title I services: partnership of the FTC with the 50 states, with the FCC exercising ancillary jurisdiction to preempt regulations only in occasional circumstances. Thus, it seems that a state net neutrality law could overcome a challenge on express preemption grounds.

Field Preemption

Much like express preemption, Congressional intent is the operative component of a field preemption challenge. Field preemption is unlike express preemption only in that there is no explicit language in a federal statute or regulation authorizing preemption over state and local laws. In this absence, state law is preempted where it regulates conduct in a field that Congress intended the federal government to occupy exclusively. This intent is

[17] *English v. General Elec. Co*., 496 U.S. 72 (1990).
[18] *Altria Group v. Good*, 555 U.S. 70 (2008).
[19] 47 U.S.C. § 253(b).

often inferred by looking to the regulatory schemes the federal government puts in place over the given field, and if the regime is "so pervasive as to make reasonable the inference that Congress left no room for states to supplement it, or where [an] act of Congress touches [a] field in which federal interest is so dominant…" then preemption will be authorized.[20]

Again, this does not square with the history of internet regulation, and certainly does not square with the FCC's declared "light touch" regulatory policy that historically has been synonymous with shared regulatory authority with the states. In such a case where the regulation of a field of conduct has been traditionally occupied or shared with the states, congressional intent to supersede state law must be "clear and manifest."[21] Such a strong intent has not materialized in any substantial way from the U.S. Congress. In fact, as mentioned in the section above, evidence of congressional intent on the regulation of Title I telecommunication services points much more strongly to shared regulatory authority with the states. For these reasons, it again appears that a state net neutrality law could overcome a challenge on field preemption grounds.

Conflict Preemption

The third type of preemption, conflict preemption, is known as the "impossibility exception." As the name suggests, preemption occurs here where it is impossible to comply with both state and federal law. In such a case, the obligations imposed by the federal law will supersede those imposed by the state. The details of any state legislation will be very important to a court seeking to determine whether a state law is truly in conflict with the Federal law or whether the statutes may be read together harmoniously.

The odds of withstanding a challenge on conflict preemption grounds are harder to predict than those on express or field preemption grounds. The main reason is that these cases are much more reliant on technological particularities. The fact that the Telecommunication Act has not been updated since 1996 leaves the courts with limited guidance on Congressional intent since the internet was only in nascent stages at that time of its enactment. Conflict preemption analysis requires the court to ask questions such as: what burdens are placed on the service providers? Are those burdens legally permissible? If so, why or why not? These open questions will have to be answered by the courts.

Dormant Commerce Clause

The other legal ground that a state net neutrality bill will almost certainly be fought on is the Dormant Commerce Clause. This is a doctrine that prohibits states from imposing inappropriate burdens on interstate commerce. Determining what is "inappropriate"

[20] *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218 (1947).
[21] *Id.*

largely rests on three potential prongs of attack: (1) the state law has purely extraterritorial application; (2) the burdens of the law are disproportionate to the local benefits it provides; or (3) state net neutrality laws expose ISPs to conflicting duties and obligations across the country that are impractical to comply with.

The first prong of attack—the extraterritoriality doctrine—does not appear to apply to state net neutrality laws because the regulated activity is found safely within the state's borders. This would be a law that applies to transactions between ISPs and consumers who are located within Massachusetts, as identified by their IP addresses. The very essence of the law is to protect Massachusetts consumers, and its application will take place physically within Massachusetts. For this reason, it appears likely that the law is safeguarded from a Dormant Commerce Clause challenge on the extraterritoriality doctrine.

The second prong is a balancing test which weighs the benefits the law provides against the burdens imposed on commerce. Consumers and business both benefit from the free exchange of internet content as well as an equal playing field in the internet marketplace. These benefits would be measured against the burdens imposed on internet service providers. In the area of privacy law, courts have held that state laws imposing telecommunications regulations on a business's interactions with consumers do not inherently offend the Dormant Commerce Clause.[22] Overall, a state wishing to pursue net neutrality legislation may argue that such requirements are workable and that the burden on internet service providers does not outweigh the legitimate local benefits such regulations provide. The courts will have to measure the benefits and burdens.

The third prong of the dormant commerce clause analysis poses a significant hurdle to state net neutrality regulation. However, a strong argument can still be made that such a law can overcome this test. The arguments in favor of invalidating state laws on this prong essentially claim that the state with the strictest regulations in effect set the policy for the whole nation. For example, separate state laws regulating the length of train box cars were struck down under the Dormant Commerce Clause because, quite literally, train box car lengths cannot be altered every time trains cross state lines.[23] What is distinguishable about a state net neutrality law is that for as long as the internet has been classified as a Title I "information service," ISPs have had to comply with the dual enforcement scheme of both FTC and state regulation. Now that the FCC has relinquished its two-year stint as the primary enforcer in this area, the pre-2015 status quo is back in force. Split enforcement authority between the FTC and the states has long been commonplace under the Telecommunications Act, for example in the early days of cable television. This dual role arrangement is arguably the statutory preference of the U.S. Congress and has been in existence for decades with little legal objection. For these reasons, there is a strong

[22] *Ades v. Omni Hotels Mgmt. Corp*., 46 F. Supp. 3d 999, 1011– 16 (C.D. Cal. 2014).
[23] *Southern Pacific Co. v. Arizona*, 325 U.S. 761 (1945).

argument that a state net neutrality law would overcome this prong of the dormant commerce clause test.

Relying on the distinguishable features of net neutrality from the precedential cases given above, it appears reasonable to believe that a state net neutrality law could overcome all prongs of attack under the Dormant Commerce Clause.

Conclusion

There is significant uncertainty surrounding the outcome of the multistate Attorneys General lawsuit challenging the FCC's net neutrality repeal, including the Order's preemption section. These questions of federal law will eventually be settled by the courts. Any state action on net neutrality will likely be challenged as well. However, there are strong arguments to support state action in this area and the uncertainty of the Federal legal landscape should not prevent states from acting.

Legislative Options

Despite the uncertain legal landscape surrounding the FCC's authority to prevent the states from taking action on net neutrality, many states have nonetheless taken action on this issue in several common ways. Legislators in 27 states have introduced 61 bills requiring internet service providers to ensure various net neutrality principles.[24] The two most common approaches will be discussed in this section. For a more comprehensive chart see Appendix I. Summaries of the Net Neutrality and ISP Privacy bills filed here in Massachusetts are also included in this section.

Washington State Model Legislation

The first bill to be enacted into law was from the State of Washington, which has served as the model for many other state bills. The final version of Washington HB.2282, which was filed on December 13th, 2017, and signed into law on March 6th, 2018, sets out a three pronged definition of net neutrality.[25] A person engaged in the provision of broadband internet access service in Washington, with some exemptions, is prohibited from:

(1) blocking lawful content, applications, services or non-harmful devices, subject to reasonable network management;

(2) impair or degrade lawful internet traffic on the basis of internet content, application or service, or use of a non-harmful device, subject to reasonable network management; and

(3) engage in paid prioritization.

These three prohibited practices are generally referred to as: blocking, which means preventing access to content, throttling, which means slowing delivery speeds of certain content, and paid prioritization, which means expedited delivery of certain content for a fee. Washington's law provides for enforcement of the new section by the Attorney General through Washington's consumer protection statute.[26] The law also sets up an Internet Consumer Access Account to received funds recovered by the Attorney General in lawsuits for the further enforcement of the new chapter.[27]

---

[24] http://www.ncsl.org/ncsl-in-dc/publications-and-resources/net-neutrality-legislation-in-states.aspx
[25] https://www.theverge.com/2018/3/6/17084246/washington-state-laws-protecting-net-neutrality-fcc-internet
[26] R.C.W. 19.86.010, *et seq*.
[27] http://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/House%20Passed%20Legislature/2282-S.PL.pdf#page=1

Montana State Model Executive Order

The other common approach that states have used in an attempt to reinstate net neutrality is through the power of the state purse. This is known as the "procurement approach." Under this approach, the state requires any ISP that has a state government contract to provide broadband service must agree to do so in compliance with the principles of net neutrality.

There are two possible ways to structure this contract term. The first approach is to limit the scope of the net neutrality promise to just state contracts, meaning that the ISP only commits to net neutrality for one customer, the state government. The second approach would be to require the ISP who does business with the state government to provide net neutral service to all of its customers in the state.

The first state to implement the procurement approach was Montana, whose Governor signed a net neutrality executive order on January 22nd, 2018.[28] This order took the second, broader approach to the procurement method. Under the order:

> "After July 1, 2018, to receive a contract from the State of Montana for the provision of telecommunications services, a service provider must publicly disclose to all of its customers in the State of Montana (including but not limited to the State itself): accurate information regarding the network and transport management practices (including cellular data and wireless broadband transport), performance and commercial terms of its broadband internet access services sufficient for consumers to make informed choices regarding use of such services and for content, application, service, and device providers to develop, market, and maintain internet offerings.
>
> After July 1, 2018, to receive a contract from the State of Montana for the provision of telecommunications services, a service provider must not, with respect to any consumer in the State of Montana (including but not limited to the State itself):
>
> 1. Block lawful content, applications, services, or nonharmful devices, subject to reasonable network management that is disclosed to the consumer;
>
> 2. Throttle, impair or degrade lawful internet traffic on the basis of internet content, application, or service, or use of a nonharmful

[28] Montana Executive Order No. 3-2018. http://governor.mt.gov/Portals/16/docs/2018EOs/EO-03-2018_Net%20Freedom.pdf?ver=2018-01-22-122048-023

device, subject to reasonable network management that is disclosed to the consumer;

3. Engage in paid prioritization; or

4. Unreasonably interfere with or unreasonably disadvantage:

a. End users' ability to select, access, and use broadband internet access service or the lawful internet content, applications, services, or devices of their choice; or

b. Edge providers' ability to make lawful content, applications, services, or devices available to end users."

The procurement approach can be effectively implemented by the executive branch because a Governor has authority over state contracts. This approach could also be enacted by state legislatures. However, there remain some legal questions about whether the second type of procurement approach will hold up in court, because it applies not just to the contracts with the state, but would encompass all of the ISPs customers in the state. The concern is that a court may interpret this as an impermissible attempt by the state to reinstate the federal law which will run into the same preemption issues that face more direct attempts to reinstate net neutrality rules.

Bills Filed in Massachusetts: Net Neutrality and ISP Privacy

Net Neutrality Legislation: There have been several bills filed in the Massachusetts legislature on net neutrality since the FCC vote in December of 2017. Although the different bills pursue a variety of enforcement mechanisms, they are generally organized around the three factors of the Washington State approach to net neutrality. As was above, there are significant legal uncertainties surrounding this approach. This is a novel area of the law and the courts will be the final arbiters of a state's authority to implement net neutrality within its borders.

Broadband Privacy Legislation: The state can be more confident in the ultimate success of implementing broadband privacy rules. As discussed above, the FCC under President Obama promulgated extensive rules relating to a customer's data that an ISP may collect while providing broadband service to customers. State legislatures also have an interest in protecting the privacy of those consumers when they go online. Below are summaries of Massachusetts bills filed in the 2017-18 legislative session relating to net neutrality and broadband privacy.

Net Neutrality

S.2336, *An Act Protecting Consumers by Prohibiting Blocking, Throttling, or Paid Prioritization in the Provision of Internet Service*

A person or entity engaged in the provision of the broadband internet access services in the Commonwealth of the Massachusetts shall not: block lawful content, applications, services, or non-harmful devices subject to reasonable network management; impair or degrade lawful internet traffic on the basis of internet content or service, or use of a non-harmful device subject to reasonable network management; or engage in paid prioritization. This legislation shall be enforced by the Attorney General and a consumer access fund shall be created to collect monies received and recovered by this office from lawsuits related to the Massachusetts Antitrust Act under within this legislation. This fund shall be administered by the Treasurer.

SD.2571. An Act to ensure a free and open internet in the Commonwealth.

The "Internet Freedom Act" would assert the Commonwealth's authority to require Internet service providers (ISPs) to treat all online traffic equally, and prohibit ISPs from blocking, manipulating, or otherwise discriminating against legal Web content. This bill would also require telecommunications companies who enter into state contracts to abide by net neutrality regulations, and would require ISPs to disclose information about the management, performance, and commercial practices of their Internet services to ensure that consumers can make informed choices. Violations of the Internet Freedom Act would be enforceable by the Attorney General under the Commonwealth's antitrust laws.

H.4222, *An Act Relative to Providing for Net Neutrality and Consumer Protection*

Establishes a Massachusetts Internet Service Provider Registry to require full disclosure of any actions by ISPs that do not adhere to net neutrality. ISPs are required to provide to all customers: access to any lawful internet content of their choice, the ability to attach or connect any lawful, non-harmful device to their end connection, and the ability to run any lawful application and use any lawful service of their choice. Furthermore, ISPs must provide customers with their disclosure of prioritization general policies and any agreement they have entered into with a content provider for prioritization of the content provider's internet traffic, written notification of policy changes that result in the prioritization of internet traffic, lists of charges for particular websites with time and date customer accessed the websites, and permit itemized bills. The Department of Telecommunications and Cable will enforce ISP compliance with these provisions and allow consumers to file a complaint with the Department against an ISP they believe is violating of the law.

H.4151, *An Act Protecting Consumers by Prohibiting Blocking, Throttling, or Paid Prioritization in the Provision of Internet Service*

The Department of the State Treasurer will create and oversee a consumer access account to collect receipts from lawsuits filed by the office of the Attorney General related to the administration and enforcement of the Massachusetts Antitrust Act provisions included in this legislation. A person engaged in the provision of broadband internet access service in the Commonwealth of Massachusetts may not: block lawful content, applications, services, or non-harmful devices subject to a reasonable network management; impair or degrade lawful internet traffic on the basis of internet content, application, or service, or use of a non-harmful device subject to reasonable network management; or engage in paid prioritization.

ISP Privacy Bills

S.2062, *An Act Relative to Internet Service Providers*

An internet service provider may not collect, use, disclose or permit third-party access to a customer's proprietary information without customer approval, with a few exceptions. Customer approval should be at the point of sale and when making a material change to a privacy policy, and shall be clear and conspicuous and not misleading. The request for customer approval shall disclose: the type of proprietary information the service provider is seeking to collect, use, disclose or permit third party access to and the purpose information will be used for and for whom it will be disclosed or granted access to. At no additional cost to the customer, the internet service provider shall make available a simple, easy-to-use mechanism for customers to grant, deny, or withdraw their opt-in approval at any time that shall be clear and conspicuous, and not misleading. This mechanism shall be available at all times on or through the internet service provider's website, by a toll-free telephone number when applicable, in the provider's application and any functional equivalent to the provider's homepage or application. A customer's change in permission will take effect immediately and remain in effect until the customer revokes or limits such grant, denial or withdrawal of approval. No financial incentive shall be offered by the internet service provider in exchange for a customer's opt-in approval and an itemized list of all proprietary information associated with a customer's account shall be provided to the customer within 30 days of a written and signed request by the customer. A customer may bring an action pursuant to section 9 of chapter 93A against an internet service provider to remedy violations of this chapter and an internet service provider shall not require binding arbitration of disputes that arise under this legislation. The Attorney General may also enforce the provisions of this new section under her existing authority in M.G.L. Chapter 93H.

S.2053, *An Act Ensuring Internet Security and Privacy*

No telecommunications or internet service provider that has entered into a franchise agreement, right-of-way- agreement, or other contract with the commonwealth of Massachusetts or a political subdivision, or that uses facilities that are subject to such agreements, even if it is not a party to the agreement, or otherwise operates in the commonwealth of Massachusetts may collect, use, disclose or otherwise disseminate, personal information from a customer resulting from the customer's use of the telecommunications or internet service provider without express written approval from the customer. No such telecommunication or internet service provider shall add an additional surcharge for customers that do not provide their express written approval, and said providers shall not refuse to provide services to a customer on the grounds that the customer has not approved collection, use, disclosure or other forms of dissemination of the customer's personal information.

H.3698, *An Act Relative to Internet Privacy*

An internet service provider may not collect, use, disclose, or permit access to sensitive customer proprietary information, with a few exceptions. Customer approval shall be solicited at the point of sale and when making changes to privacy policies, and shall be clear, conspicuous, not misleading, and in a language that is comprehensible. This solicitation must disclose the types of sensitive customer proprietary information the provider is seeking to collect, use, disclose or permit access to, the purpose the information shall be used for, and whom the provider intends to disclose or permit access to. The internet provider shall make available at no additional cost to the customer a simple, easy-to-use mechanism for customers to grant, deny, or withdraw opt-in approval at any time that is clear, conspicuous, in a comprehensive language, and is not misleading. This mechanism must be persistently available on or through the provider's website, toll-free telephone number, provider's application, homepage, and any equivalent application. The customer's grant, denial, or withdrawal of approval must be given effect promptly and remain in effect until the customer revokes or limits such grant, denial, or withdrawn approval.

H.3766, *An Act Prohibiting the Collection of Personal Information From a Consumer*

No telecommunications or internet service provider that has entered into a franchise agreement, right-of-way agreement, or other contract with the state of Massachusetts or a political subdivision, or that uses facilities that are subject to such agreements, even if it is not a party to the agreement, may collect personal information from a customer resulting from the customer's use of the telecommunications or internet service provider without express written approval from the customer.

Legislative Proposal – Summary

Bill Overview:

The proposed legislation would protect consumers from blocking, throttling, or paid prioritization in the provision of internet service; would require internet service providers to be transparent about their network management practices through the creation of the Massachusetts Internet Service Provider Registry; and would promote net neutrality through government contract requirements and IP-to-IP interconnectivity agreements. Finally, this bill would protect consumers' privacy by prohibiting internet service providers from collecting, using or disseminating consumers' personal data without their consent.

Section-by-Section Summary:

SECTION 1: Clarifies the Department of Telecommunications and Cable's authority over interconnection agreements for IP enabled service between ISPs who have customers in Massachusetts.[29] Requires ISPs to disclose to the Department when they are having a dispute about interconnection that results in degradation of service to customers. The Department will try to resolve the dispute within 30 days, after which it will notify the public of the dispute. Requires net neutrality clauses in order for final interconnection agreements to be approved by the Department.

SECTION 2: The Department of Telecommunications and Cable is entirely funded by an assessment upon cable television, telephone and telegraph companies.30 This section would allow the Commissioner to also make an assessment against each internet service provider under the jurisdictional control of the Department. This expansion will allow the Department to cover the new costs associate with the Department's new role in the ISP sector.

SECTION 3: Clarifies the Department of Telecommunications and Cable's authority over interconnection agreements for wireless service between ISPs who have customers in Massachusetts. Requires ISPs to disclose to the Department when they are having a dispute about interconnection that results in degradation of service to customers. The Department will try to resolve the dispute within 30 days, after which it will notify the public of the dispute. Requires net neutrality clauses in order for final interconnection agreements to be approved by the Department.

---

[29] It is currently an open legal question about whether DTC can regulate the IP-to-IP interconnection agreements. DTC definitely has the authority to regulate interconnection agreements between telephone companies under 47 U.S.C. § 252(e)(2)(ii) and disapprove of such agreements if they violate the "public interest."

[30] M.G.L. Chapter 25C Section 7.

SECTION 4: This section contains an outright ban on ISPs engaging in the practices that violate the three net neutrality principles (blocking, throttling or paid prioritization) by making such practices per se violations of Chapter 93A.

SECTION 5: Massachusetts Internet Service Provider Registry

ISPs are required to make the same net neutrality disclosures to the Massachusetts Department of Telecommunications and Cable that they already have to make to the FCC. The Department may conduct verification tests and will have strong enforcement powers to make sure that the ISPs are making truthful disclosures.

The Department shall develop standards for what it means to be a "net neutral" ISP and determine whether each ISP complies with the criteria set forth by the Department. If an ISP is voluntarily in compliance with the Department's standards for net neutrality, the ISP may display the "Massachusetts Net Neutrality Seal" on its marketing materials. Anyone who uses the "Massachusetts Net Neutrality Seal," while not in compliance with the standards set forth by the Department, shall be liable under Chapter 93A for a deceptive business practice.

The Department shall develop regulations to rank all internet service providers on the quality of their net neutrality practices based on the disclosures and verification tests in this section. The Department will score each ISP against its criteria to determine a net neutrality score for each internet service provider. ISPs must display the Department's score at the point of sale, in an initial customer contract and annually thereafter.

SECTION 6: The Department of Telecommunications and Cable shall have jurisdiction, general supervision, regulation and control over an internet service provider's compliance with the requirements of the Massachusetts Internet Service Provider Registry. Any internet service provider who fails to comply with any requirement may be fined not more than one thousand dollars per violation, per day, by the Department.

SECTION 7: Government entities must consider the network management practices of all ISPs before entering into a contract for broadband internet service. ISPs submitting a bid or proposal to provide broadband internet service must provide all DTC-required disclosures to the government body, which must consult with the Department of Telecommunication and Cable about the ISPs network management practices. Preference shall be given to internet service providers who are compliant with the Department's standards for the "Massachusetts Net Neutrality Seal."

SECTIONS 8-11: Broadband Privacy

Clearly defines Internet Service Provider (ISP) and Customer Proprietary Information (customer data); requires ISPs to notify customers in the event of a data breach and to comply with other requirements in the event of a data breach; requires ISPs to seek the customer's express permission (opt-in) to use, collect, disclose or allow access to a customer's data for purposes such as selling that data to third parties; clearly delineates when an ISP may use data without customer approval, including data collected for the basic functions of operating the internet service, and data requested by emergency personnel in response to an emergency; prohibits ISPs from offering financial incentives or imposing penalties to entice customers to grant permission, or denying service based on a customer's refusal to grant permission.

Authorizes consumers to request that ISPs provide them with a list of any data collected by the ISP regarding that consumer within 30 days of a written and signed request from the consumer; authorizes the Attorney General to bring an action against a non-compliant ISP; allows the Department of Telecommunications and Cable to promulgate regulations and enforce the privacy requirements; allows consumers whose information is misused a private right of action if their information was misused; prohibits ISPs from requiring that disputes be resolved through binding arbitration; provides statutory and punitive damages for misuse of consumer information.

SECTION 12: Updates the Municipal Light Plant law, which was last amended in 1996, to clarify that a municipality may build and run its own internet networks. Under the 1996 amendment, municipalities already have the ability to build and run their own "telecommunications systems" for the benefit of the town and its residents. This change will merely make clear that "telecommunications systems" do in fact include the internet.

SECTION 13: The Department of Telecommunications and Cable shall promulgate regulations to effectuate the Massachusetts Internet Service Provider Registry within 60 days of the effective date of this act. The Department shall begin enforcement of such regulations on January 1, 2019.

SECTION 14: Internet service providers shall seek opt-in approval from existing customers under Section 11 of this act not later than 30 days after the effective date of this act.

Appendix I: State Net Neutrality Legislation

"Block lawful content, applications, services or non-harmful devices, subject to reasonable network management	WA MA NE NY CA HI AK CT IL ID
"Impair or degrade lawful internet traffic on the basis of internet content, application or service, or use of a non-harmful device, subject to reasonable network management"	WA MA NE NY CA HI AK IL ID
"Engage in paid prioritization"	WA MA NE NY CA HI CT IL ID
"Interfere with end user's ability to use content, applications, services, or devices of choice"	NE CA HI AK CT IL ID
"Set up an Internet Consumer Access fund to ensure the free flow of internet equitably - from money received by the AG in pertinent lawsuits"	MA NE CA
"Require registration and regular extensive reporting from all Internet Service Providers ("ISPs") to ensure compliance"	NE CA MT
"Exempt ISPs in the case of necessary public interest or if it is unreasonable to their preservation of business"	MA NE MT
"Mandate state agencies and municipalities to only contract with internet service providers that adhere to the principles of net neutrality via well-defined contracts"	NY CA RI
"Make violations unfair and deceptive business practices"	CA WA
"Fine ISPs who violate net neutrality"	NE
"Establish statewide consumer protection rules, easily accessible to the public, including the ability to freely test their internet speed with the ability to submit the results to the commission"	CA
"Establish the ability to modify eligible carrier status, which is necessary for federal funding, to ensure compliance with net neutrality"	CA

Appendix II: Legislative Proposal – Bill Text

SECTION 1: Section 6A of said chapter 25C, as so appearing, is hereby amended by inserting in paragraph (e) the following words:-

(1) The department shall review any interconnection agreement for IP enabled service adopted by negotiation or arbitration which effects Massachusetts customers pursuant to 47 U.S.C. \s 252(e)(2). The department shall not approve of any agreement which does not contain a contract term prohibiting each party from:

(i) Blocking lawful content, applications, services, or nonharmful devices, subject to reasonable network management;

(ii) Impairing or degrading lawful internet traffic on the basis of internet content, application, or service, or use of a nonharmful device, subject to reasonable network management; or

(iii) Engaging in paid prioritization.

(2) IP enabled service providers who are engaged in a contract negotiation regarding interconnection must disclose to the department if that negotiation has resulted in degraded service to customers in Massachusetts for more than a 24 hour period. The department shall attempt to mediate or arbitrate the dispute to avoid harm to customers. If the dispute cannot be resolved by voluntary means within 30 days, the department shall publish on its website a notice regarding the scope of the dispute and its effect on consumers in Massachusetts. Any IP enabled service providers involved in the dispute

must also notify, in writing, all affected customers about the cause of the degradation of the service if the dispute cannot be resolved within 30 days from the date the degradation notice was filed with the department.

SECTION 2: Section 7 of chapter 25C, as so appearing, is hereby amended by inserting after the first sentence, in line 7, the following sentence:-

"The commissioner may also make an assessment against each internet service provider which is required to make disclosures as part of the Massachusetts Internet Service Provider Registry under Section 10 of this chapter."

SECTION 3: Section 8 of said chapter 25C, as so appearing, is hereby amended by inserting after the paragraph (b) the following paragraph:-

(c) The department shall review any interconnection agreement for wireless service adopted by negotiation or arbitration which effects Massachusetts customers pursuant to 47 U.S.C. \s 252(e)(2). The department shall not approve of any agreement which does not contain a contract term prohibiting each party from:

(1) Blocking lawful content, applications, services, or nonharmful devices, subject to reasonable network management;

(2) Impairing or degrading lawful internet traffic on the basis of internet content, application, or service, or use of a nonharmful device, subject to reasonable network management; or

(3) Engaging in paid prioritization.

(d) Wireless service providers who are engaged in a contract negotiation regarding interconnection must disclose to the department if that negotiation has resulted in degraded service to customers in Massachusetts for more than a 24 hour period. The department shall attempt to mediate or arbitrate the dispute to avoid harm to customers. If the dispute cannot be resolved by voluntary means within 30 days, the department shall publish on its website a notice regarding the scope of the dispute and its effect on consumers in Massachusetts. Any wireless service provider involved in the dispute must also notify, in writing, all affected customers about the cause of the degradation of the service if the dispute cannot be resolved within 30 days from the date the degradation notice was filed with the department.

SECTION 4: Chapter 25C of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by adding the following section:—

Section 9. Protecting consumers from blocking, throttling, or paid prioritization in the provision of internet service

(a) The following words as used in this section shall have the following meanings, unless the context clearly requires otherwise:

"Broadband internet access service" a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up internet access service or any service that the federal communications commission finds to be providing a functional equivalent thereof that is used to evade the protections set forth in this section.

"Paid prioritization" the management of a broadband provider's network to favor, either directly or indirectly, certain traffic over other traffic. Paid prioritization may include the use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management, either:

(1) In exchange for consideration (monetary or otherwise) from a third party; or

(2) to benefit an affiliated entity.

“Reasonable network management" a practice that has a primarily technical network management justification but does not include other business practices. A network management practice is reasonable if it is primarily used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband internet access service.

(b) A person or entity engaged in the provision of broadband internet access service in Commonwealth shall not:

(1) Block lawful content, applications, services, or nonharmful devices, subject to reasonable network management;

(2) Impair or degrade lawful internet traffic on the basis of internet content, application, or service, or use of a nonharmful device, subject to reasonable network management; or

(3) Engage in paid prioritization.

(c) The Department of Telecommunications and Cable may waive the prohibition on paid prioritization in subsection (b)(3) of this section only if the petitioner demonstrates that the practice would serve a legitimate and significant public interest and would not harm the open nature of the internet in the Commonwealth.

(d) It shall be an unfair or deceptive act or practice and a violation of chapter 93A to violate any provision of this chapter and the attorney general of the commonwealth or any other person may bring an action pursuant to chapter 93A.

SECTION 5: Chapter 25C of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by adding the following section:—

Section 10: Massachusetts Internet Service Provider Registry

(a) The following words as used in this chapter shall have the following meanings, unless the context clearly requires otherwise:

"Broadband internet access service" or “BIAS” a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up internet access service or any service that the federal communications commission finds to be providing a functional equivalent thereof that is used to evade the protections set forth in this section.

“Internet service provider” or “BIAS provider”, a person who provides BIAS to customers in the commonwealth.

(b) There is established in the department the "Massachusetts Internet Service Provider Registry" for the purpose of making internet service quality and network management practices readily available to customers within the commonwealth.

(c) The department shall promulgate regulations that require all internet service providers to affirmatively disclose the following network management and security information to the department:

(i) Blocking. Any practice, other than reasonable network management elsewhere disclosed, that blocks or otherwise prevents end user access to lawful content, applications, service, or non-harmful devices, including a description of what is blocked.

(ii) Throttling. Any practice, other than reasonable network management elsewhere disclosed, that degrades or impairs access to lawful Internet traffic on the basis of content, application, service, user, or use of a non-harmful device, including a description of what is throttled.

(iii) Affiliated Prioritization. Any practice that directly or indirectly favors some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, or resource reservation, to benefit an affiliate, including identification of the affiliate.

(iv) Paid Prioritization. Any practice that directly or indirectly favors some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, or resource reservation, in exchange for consideration, monetary or otherwise.

(v) Congestion Management. Descriptions of congestion management practices, if any. These descriptions should include the types of traffic subject to the practices; the purposes served by the practices; the practices' effects on end users' experience; criteria used in practices, such as indicators of congestion that trigger a practice, including any usage limits triggering the practice, and the typical frequency of congestion; usage limits and the consequences of exceeding them; and references to engineering standards, where appropriate.

(vi) Application-Specific Behavior. Whether and why the ISP blocks or rate-controls specific protocols or protocol ports, modifies protocol fields in ways not prescribed by the protocol standard, or otherwise inhibits or favors certain applications or classes of applications.

(vii) Device Attachment Rules. Any restrictions on the types of devices and any approval procedures for devices to connect to the network.

(viii) Security. Any practices used to ensure end-user security or security of the network, including types of triggering conditions that cause a mechanism to be invoked (but excluding information that could reasonably be used to circumvent network security).

(d) The department shall conduct verification tests, on its own or through a third-party, to determine the accuracy of the disclosures made by each internet service provider under subsection (c).

(e) The department shall compile the information disclosed by all of the internet service providers within the commonwealth pursuant to this section and from the

department's own verification tests, conducted pursuant to this section, into an "Internet Service Provider Registry." The department shall organize the registry in a format that is conducive to review and comparison by customers and prospective customers of internet service.

(f) The department shall establish minimum standards for a “Massachusetts Net Neutrality Seal” which will set an expectation of equal access to an open and neutral internet. The department shall publicly disclose the criteria by which it will measure the network management practices of each internet service provider. The department shall determine whether each internet service provider complies with the criteria set forth by the department. If an internet service provider is voluntarily in compliance with the department’s standards for net neutrality, the internet service provider may display the “Massachusetts Net Neutrality Seal” on its marketing materials. Anyone who uses the “Massachusetts Net Neutrality Seal,” while not in compliance with the standards set forth by the department, shall be liable under Chapter 93A for a deceptive business practice.

(g) The department shall develop regulations to rank all internet service providers on the quality of their net neutrality practices based on the disclosures and verification tests in this section. The department will score each internet service provider against its criteria to determine a net neutrality score for each internet service provider.

(h) The department shall make available electronically on its internet website in English and Spanish the information contained in the registry, including net neutrality scores in one comparison chart for fixed line internet service providers and one comparison chart for wireless internet service providers, and shall provide the information

to customers and prospective customers upon request by means of a toll-free telephone service operated by the department.

(i) Each internet service provider that conducts business in the commonwealth must display its net neutrality score to all customers at the point of sale. The internet service provider must also provide the website and phone number for the "Massachusetts Internet Service Provider Registry" for consumers to learn more about what the score means. Each internet service provider that conducts business in the commonwealth shall also disclose its net neutrality score to all customers in the commonwealth upon entering into an agreement for service and annually thereafter.

SECTION 6: Chapter 25C of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by adding the following section:—

Section 11: (a) Notwithstanding any provision of chapter 25C or any other general or special law to the contrary, the department shall have jurisdiction, general supervision, regulation and control over an internet service provider's compliance with section 10.

(b) Any internet service provider who fails to comply with any requirement of section 10 of this chapter may be fined not more than one thousand dollars per violation, per day, by the department.

(c) The department shall have the right to institute, or to intervene as a party in, any action in any court of competent jurisdiction seeking injunctive or other relief to compel compliance with any provision of section 10 or any rule, regulation or order

adopted thereunder, or to restrain or otherwise prevent or prohibit any illegal or unauthorized conduct in connection therewith.

(d) The department or its employees may visit the places of business and other premises and examine the records and facilities of all internet service providers to ascertain if all rules and regulations and orders of the department have been complied with. The department shall also have the power to issue subpoenas to compel the attendance of witnesses and the production of documents, papers, books, records, and other evidence before it in any matter over which it has jurisdiction, control or supervision. The department shall have the power to administer oaths and affirmations to persons whose testimony is required.

(e) Subject to section 4 of chapter 25C, the commissioner of the department shall have all the powers and duties under this chapter including, but not limited to: presiding at hearings; maintaining or intervening in an action; hearing appeals and issuing enforcement orders; enforcement powers; and all other authority to carry out the duties and responsibilities of section 10.

(g) Nothing in this section shall be construed to affect or modify the authority of the attorney general to apply and enforce chapter 93A and other consumer protection laws of general applicability.

SECTION 7: Chapter 30B of the General Laws is hereby amended by inserting after section 23 the following section:-

Section 24: Net Neutrality and Internet Service Providers Entering into State Contracts

a) A person that submits a bid or proposal to, or otherwise proposes to enter into or renew, a contract with a governmental body with respect to the provision of internet service shall provide the contracting authority with copies of all disclosures required in Section10 of chapter 25C.

b) A governmental body shall consult with the Department of Telecommunication and Cable about the network management practices of each internet service provider under consideration for the award of a contract. The internet service provider's network management practices shall be a factor in the government body's decision about awarding the broadband internet service contract. Preference shall be given to internet service providers who are compliant with the Department's standards for the "Massachusetts Net Neutrality Seal."

SECTION 8. Section 1 of chapter 93H of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by inserting after the definition of "Breach of security" the following 3 definitions:-

"Broadband internet access service" or "BIAS", a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up internet access service; provided, that "broadband internet access service" shall also include any service

that the Federal Communications Commission finds to be providing a functional equivalent of the service described in this definition.

"Customer", a current or former subscriber to an internet service in the commonwealth or an applicant for an internet service in the commonwealth.

"Customer's proprietary information", the customer's information which is protected under this chapter, including the following 3 types of information collected by telecommunications carriers through the provision of broadband or other telecommunications services that are not mutually exclusive: (i) individually identifiable customer proprietary network information, CPNI, as defined in 47 U.S.C. 222 (h)(1), including, but not limited to, website browsing history and application usage; (ii) personal information as defined in Section 1 of this chapter; and (iii) content of communications.

SECTION 9. Said section 1 of said chapter 93H, as so appearing, is hereby further amended by inserting after the definition of "Encrypted" the following definition:-

"Internet service provider" or "BIAS provider", a person who provides BIAS to customers in the commonwealth.

SECTION 10. Said section 1 of said chapter 93H, as so appearing, is hereby further amended by inserting after the definition of "Notice" the following definition:-

"Opt-in approval", a method for obtaining customer consent to collect, use, disclose or permit third-party access to customer proprietary information; provided, however, that the approval method shall require that the internet service provider obtain from the customer affirmative, expressed consent allowing the requested collection, usage,

disclosure or access to the customer's proprietary information after the customer is provided appropriate notification of the internet service provider's request as required by this chapter.

SECTION 11. Said chapter 93H is hereby further amended by inserting after section 6 the following 3 sections:-

Section 7. (a) An internet service provider shall be subject to all the data security regulations and data breach reporting requirements of this chapter.

(b) An internet service provider may not collect, use, disclose or permit third-party access to a customer's proprietary information except as described in subsection (c) or with the opt-in approval of a customer under subsection (d).

(c) An internet service provider may collect, use, disclose or permit third-party access to a customer's proprietary information without customer approval for the following purposes: (i) to provide internet service from which such information is derived or to provide services necessary to or used in the provision of such internet service; (ii) to initiate, render, bill or collect payment for internet service; (iii) to protect the rights or property of the internet service provider or to protect users of the internet service and other internet service providers from fraudulent, abusive or unlawful use of the service; (iv) to provide any inbound marketing, referral or administrative services to the customer for the duration of a real-time interaction, if such interaction was initiated by the customer; (v) to provide first-party marketing to customers about improved service offerings within the scope of service to which they already subscribe; (vi) to provide location information or other customer proprietary information to: (1) a public safety answering point, emergency

medical service provider or emergency dispatch provider, public safety, fire service, law enforcement official or hospital emergency or trauma care facility, in order to respond to the customer's request for emergency services; or (2) providers of information or database management services solely to assist in the delivery of emergency services in response to an emergency; or (vi) as otherwise required or authorized by law.

(d) Except as otherwise provided in this section, an internet service provider shall obtain opt-in approval from a customer to: (i) collect, use, disclose or permit third-party access to a customer's proprietary information for any purpose not authorized under subsection (c); or (ii) when making a material, retroactive change that would result in a use, disclosure or permission of third-party access to the customer's proprietary information previously collected by the internet service provider for which the customer did not previously grant approval for such use, disclosure or permission of access.

(e) An internet service provider shall, at a minimum, solicit customer opt-in approval pursuant to subsection (d), as applicable, at the point of sale and when making a material change to a privacy policy. The request for customer approval shall be clear and conspicuous and shall not be misleading. The request for customer approval shall disclose: (i) the type of proprietary information that the internet service provider is seeking customer approval to collect, use, disclose or permit third-party access to; (ii) the purpose for which the customer's proprietary information will be used; and (iii) the type of entity that the internet service provider intends to disclose or grant access to the customer's proprietary information. The request for customer approval shall be translated into a

language other than English if the internet service provider transacts business with the customer in that other language.

(f) An internet service provider shall make available a simple, easy-to-use mechanism for customers to grant, deny or withdraw opt-in approval at any time. The mechanism to grant, deny or withdraw opt-in approval shall be clear and conspicuous, and shall not be misleading and shall be made available at no additional cost to the customer. Such mechanism shall be available at all times (i) on or through the internet service provider's website, (ii) in the internet service provider's application, if it provides an application for account management purposes, and (iii) any functional equivalent to the internet service provider's homepage or application. If an internet service provider does not have a website, the internet service provider shall provide a mechanism by another means that is available at all times including, but not limited to, a toll-free telephone number. The customer's grant, denial or withdrawal of approval shall take effect immediately and remain in effect until the customer revokes or limits such grant, denial or withdrawal of approval.

(g) An internet service provider shall not add a surcharge for service to customers that do not provide opt-in approval and shall not refuse to provide services to a customer on the grounds that the customer refused to give opt-in approval. An internet service provider shall not offer a financial incentive in exchange for a customer's opt-in approval.

(h) An internet service provider shall provide a customer with an itemized list of all of the proprietary information associated with that customer's account within 30 days of a written and signed request by the customer.

Section 8. Notwithstanding sections 6A and section 8 of chapter 25C, the department of telecommunications and cable shall have the authority to promulgate regulations and enforce section 7 of this chapter under its powers to monitor and enforce the "Massachusetts Internet Service Provider Registry" under Section 11 of Chapter 25C.

Section 9. Civil Liability

(a) Statutory Damages. Any person who negligently or willfully fails to comply with any requirement imposed under this chapter shall be liable to any person whose personal information or customer proprietary information was involved in such violation for the following statutory damages. These statutory damages shall be indexed to inflation starting in the year that this act is enacted.

(i) Each person whose personal information or customer proprietary information has been misused under this chapter shall be entitled to a minimum statutory damage of $1000, per person; and

(ii) Each person whose personal information or customer proprietary information has been misused under this chapter shall be entitled to $5000, per person, or actual damages, whichever is greater, if the person can prove that their identity has been stolen or some other specific harm has resulted.

(b) Punitive Damages. Any person who willfully fails to comply with any requirement imposed under this chapter shall be liable to any person whose personal information or customer proprietary information was involved in such violation for such punitive damages as the court may allow. Any calculation of punitive damages shall take into account the size of the defendant's business and its annual profits.

(c) Attorney's Fees. In the case of any successful action to enforce any liability under this section, the plaintiff shall be entitled to the costs of the action together with reasonable attorney's fees as determined by the court.

Section 10. An internet service provider shall not require binding arbitration of disputes that arise under this chapter.

SECTION 12: The first sentence of section 47E of chapter 164 of the General Laws, as appearing in the 2016 Official Edition, is hereby amended by inserting, in line 6, after the word "system" the following words:-

", including, but not limited to, internet access including wireless internet access,"

SECTION 13: The department shall promulgate regulations to effectuate Sections 5 and 6 of this act with 60 days of the effective date of this act. The department shall begin enforcement of such regulations on January 1, 2019.

SECTION 14: Internet service providers shall seek opt-in approval from existing customers under Section 11 of this act not later than 30 days after the effective date of this act.