UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

ACA CONNECTS – AMERICA'S COMMUNICATIONS ASSOCIATION;

CTIA – THE WIRELESS ASSOCIATION®;

NCTA – THE INTERNET & TELEVISION ASSOCIATION; and

USTELECOM – THE BROADBAND ASSOCIATION,

Plaintiffs,

v.

AARON FREY, in his official capacity as Attorney General of the State of Maine;

PHILIP L. BARTLETT II, in his official capacity as Chairman of the Maine Public Utilities Commission;

R. BRUCE WILLIAMSON, in his official capacity as Commissioner of the Maine Public Utilities Commission; and

RANDALL D. DAVIS, in his official capacity as Commissioner of the Maine Public Utilities Commission,

Defendants.

Civil Action No. _____

COMPLAINT FOR DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF

Plaintiffs ACA Connects – America's Communications Association, CTIA – The Wireless Association®, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association allege:

PRELIMINARY STATEMENT

1. Plaintiffs and their members, which include Internet Service Providers ("ISPs"), are committed to protecting their customers' privacy. Plaintiffs and their members have consistently supported reasonable laws and regulations that safeguard consumers' personal information uniformly across all consumer-facing companies, whether online or offline.

2. The Maine statute challenged here, L.D. 946 (June 6, 2019) ("the Statute"), which was enacted purportedly to advance the goal of consumer privacy, is not such a law. The Statute imposes unprecedented and unduly burdensome restrictions on ISPs', and only ISPs', protected speech. These include restrictions on how ISPs communicate with their own customers that are not remotely tailored to protecting consumer privacy. Indeed, by targeting ISPs alone, the Statute deliberately thwarts federal determinations about the proper way to protect consumer privacy — that is, with technology-neutral, uniform regulation.

3. The Statute violates the First Amendment because, among other things, it: (1) requires ISPs to secure "opt-in" consent from their customers before using information that is not sensitive in nature or even personally identifying; (2) imposes an opt-out consent obligation on using data that are by definition *not* customer personal information; (3) limits ISPs from advertising or marketing non-communications-related services to their customers; and (4) prohibits ISPs from offering price discounts, rewards in loyalty programs, or other cost-saving benefits in exchange for a customer's consent to use their personal information. The Statute thus excessively burdens ISPs' beneficial, pro-consumer speech about a wide variety of subjects, with no offsetting privacy-protection benefits. At the same time, it imposes no

restrictions at all on the use, disclosure, or sale of customer personal information, whether sensitive or not, by the many other entities in the Internet ecosystem or traditional brick-and-mortar retailers, thereby causing the Statute to diverge further from its stated purpose. To make matters worse, the Statute is shot through with irrational distinctions between closely related types of speech based on the content of the speech.

4. Protecting customer privacy is a laudable objective that ISPs support. But Maine has not shown — through evidence in the legislative record — that ISPs' privacy practices are causing any harm whatsoever to consumers, let alone harm that justifies unique restrictions on ISPs' communications. Nor has Maine shown that such unique restrictions are needed in light of federal privacy standards, which apply evenly across businesses of all types. Maine cannot discriminate against a subset of companies that collect and use consumer data by attempting to regulate just that subset and not others, especially given the absence of any legislative findings or other evidentiary support that would justify targeting ISPs alone. Maine's decision to impose unique burdens on ISPs' speech — while ignoring the online and offline businesses that have and use the very same information and for the same and similar purposes as ISPs — represents discrimination between similarly situated speakers that is impermissible under the First Amendment. *See Sorrell v. IMS Health Inc.*, 564 U.S. 552, 572 (2011); *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1238-39 (10th Cir. 1999).

5. This speaker-based discrimination, which renders the Statute inconsistent with its avowed goal of protecting consumers' privacy, is not the only reason the State cannot carry its burden under the First Amendment. Indeed, the Statute lacks any reasonable fit between its provisions and advancing consumer privacy — even as applied to ISPs. For example, the Statute restricts wide swaths of information that raise no plausible privacy concerns at all, including

information the Statute defines as *not* customer personal information. In addition, the Statute draws sharp, content-based distinctions between categories of speech that cannot be explained by any interest in protecting privacy — allowing, for example, ISPs to use consumer data for speech about their communications-related services but not about their *non*-communications-related services. The Statute also restricts valuable non-commercial speech such as location-based public service announcements and mandatory reports to the federal government.

6. The Statute's speech restrictions are also too vague to comply with due process because they force ISPs to guess at the boundaries of those restrictions. *Johnson v. United States*, 135 S. Ct. 2551, 2561 (2015). The Statute's amorphous, broad, and open-ended restrictions will therefore chill ISPs' protected First Amendment speech.

7. In addition to violating the First Amendment in multiple respects, the Statute is preempted by federal law because it directly conflicts with and deliberately thwarts federal determinations about the proper way to protect consumer privacy. Indeed, the Statute's express purpose was to contradict Congress's decision — embodied in a binding joint resolution signed by the President — to repeal and prohibit the federal adoption of an ISP-specific privacy regime in favor of privacy rules that apply uniformly to all companies holding consumers' personal information. The Statute also conflicts with the Federal Communications Commission's ("FCC") decision that a combination of disclosure, competition, and Federal Trade Commission ("FTC") oversight — not prescriptive ISP-specific rules — best balances the federal policies of promoting broadband and protecting consumer privacy. And it does so in a manner that makes it impossible for Plaintiffs' members to comply with mandatory federal reporting requirements and other disclosures required by law.

8. The Court should declare the Statute unconstitutional and enjoin its enforcement.

PARTIES

9. Plaintiff ACA Connects – America's Communications Association is a trade association representing nearly 800 small and medium-sized independent operators that provide video, broadband, and phone services. ACA Connects' members often operate in smaller markets and rural areas, where they provide communications services that are crucial to the economic prosperity of the communities they serve. ACA Connects' members include providers of broadband Internet access service in the State of Maine. ACA Connects maintains its principal place of business in Pittsburgh, PA.

10. Plaintiff CTIA represents the U.S. wireless communications industry and companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. Its members include providers of wireless broadband Internet access service to households, businesses, and governmental entities throughout the country, including to customers in the State of Maine. CTIA maintains its principal place of business in Washington, D.C.

11. Plaintiff NCTA is the principal national trade association of the cable industry in the United States. NCTA's mission is to protect and advocate for the interests of the cable and telecommunications industry. Its members include cable operators offering fixed and wireless broadband Internet access services to households, businesses, and governmental entities throughout the country, including to customers in the State of Maine. NCTA maintains its principal place of business in Washington, D.C.

12. Plaintiff USTelecom is a non-profit association of telecommunications companies of all sizes working toward the common goal of providing accessible, thriving, and secure

broadband infrastructure in all corners of the United States. USTelecom's members provide fixed and wireless broadband Internet access service to millions of consumers and businesses across the country, including in the State of Maine. USTelecom maintains its headquarters in Washington, D.C.

13. Defendant Aaron Frey is the Attorney General of the State of Maine. His principal place of business is in Augusta, Maine, and he regularly transacts business within the State. Attorney General Frey is charged with enforcing Maine's civil law, including the Statute.

14. Defendant Philip L. Bartlett II is the Chairman, and Defendants R. Bruce Williamson and Randall D. Davis are Commissioners, of the Maine Public Utilities Commission, which has authority to enforce the Statute. Their principal place of business is in Hallowell, Maine, and they regularly transact business within the State. Chairman Bartlett is responsible for implementing the policies of the Commission as principal executive officer.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because the case arises under the First and Fourteenth Amendments and the Supremacy Clause of the United States Constitution.

16. 42 U.S.C. § 1983 provides a civil cause of action to any person who is deprived of rights guaranteed by the United States Constitution or federal law, by another person, under color of State law.

17. This Court may declare the legal rights and obligations of the parties in this action under 28 U.S.C. § 2201 because this action presents an actual controversy within the Court's jurisdiction.

18. Venue is proper in the District of Maine under 28 U.S.C. § 1391(b)(1) and (2), because Defendants have offices in, and therefore reside in, the District of Maine, and a substantial part of the events giving rise to Plaintiffs' claims occurred in the District of Maine.

19. Under Local Rule 3(b), this action should be assigned to the Bangor Division of this Court because a substantial part of the events giving rise to Plaintiffs' claims for relief occurred in Kennebec County.

20. ACA Connects, CTIA, NCTA, and USTelecom each have associational standing to bring this suit on behalf of their members because at least one member of each association will be directly, adversely, and imminently affected by the Statute and thus would have standing to sue in their own right. The interests that Plaintiffs seek to protect by way of this lawsuit are germane to each organization's purpose. Finally, neither the claims asserted nor the relief requested requires an individual member of ACA Connects, CTIA, NCTA, or USTelecom to participate in this suit.

FACTUAL BACKGROUND

Internet Service Providers And Consumer Data

21. ISPs provide consumers with access to the Internet. They deploy high-speed fixed and mobile links connecting their networks to consumers' homes and smartphones, and they operate the equipment and systems that in turn allow consumers to send and receive information from those networks across the Internet.

22. ISPs are just one segment of the broader Internet ecosystem. They provide consumers access to digital content, websites, and applications ("apps"), including those developed and operated by "edge providers," such as operators of streaming video services (*e.g.*, Netflix), search engines (*e.g.*, Google), social media (*e.g.*, Facebook), and online marketplaces (*e.g.*, Amazon), among countless others. Other businesses develop the software — including the

operating systems, web browsers, and other applications — that facilitate Internet activity on computers, tablets, smartphones, and other devices.

23. Each of these types of actors collects and uses consumer data for business, operational, marketing, and advertising purposes. Standard uses include providing products or services to customers, verifying customers' identities, processing payments, providing financing, and conducting research in order to improve existing products and services. Internet-based businesses are far from unique in this respect. Traditional brick-and-mortar businesses similarly collect and use customer information in the course of charging for products or services and administering customer loyalty or rewards programs. In addition to collecting data directly from customers, businesses also turn to so-called "data brokers" (*e.g.*, Experian) to purchase additional consumer data.

24. Online and offline businesses also use consumer information to develop and engage in effective and efficient communications with their customers. By analyzing this data, businesses — including ISPs, edge providers, and brick-and-mortar retailers — can better tailor their products, services, marketing, and advertising to meet consumer needs and satisfy their preferences.

25. This type of tailored marketing and advertising creates "enormous benefits" for businesses and consumers. Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* 50 (2014). It allows businesses to communicate with consumers more effectively and efficiently, and allows consumers to receive more relevant information and superior service. Because of these benefits, targeted marketing and advertising have become an important means of communication between Internet-based businesses and their customers. *See* eMarketer Editors, *US Digital Ad Spending Will Surpass Traditional in 2019* (Feb. 19, 2019)

(domestic spending on digital advertising is projected to account for more than half of all U.S. advertising spending).

26. Recent technological developments have limited ISPs' access to consumers' data when transmitted over their Internet connection. Widespread encryption is "pervasively limiting the ability of ISPs to see Internet activity." Peter Swire, et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* 25, Working Paper of The Institute for Information Security & Privacy at Georgia Tech (Feb. 29, 2016), https://b.gatech.edu/2Hn2ULi ("Swire Study"); *see also* Cam Cullen, *Global Internet Phenomena Preview: Encrypted Traffic Dominates the Internet*, Sandvine (2018) (estimating that 75 to 90 percent of Internet traffic is encrypted), https://bit.ly/2O8fzri. The widely adopted HTTPS encryption standard, for example, prevents ISPs from seeing both the full URL[1] and the content of websites their customers visit. *See* Swire Study at 26. To illustrate, if a customer conducts a Google search for "best bookstores in Portland," her ISP can "see" only that she contacted google.com; it *cannot* see what she asked Google to search for. For these and other reasons, "other companies often have access to more information and a wider range of user information than ISPs [and] ISPs have neither comprehensive nor unique access to information about users' online activity. Rather, the most commercially valuable information about online users, which can be used for targeted advertising and other purposes, is coming from other contexts." *Id.* at 3-4.

[1] A "URL" or Uniform Resource Locator is the text that represents information accessible over the Internet. For example, http://www.med.uscourts.gov is the URL for the Court's home page, while http://www.med.uscourts.gov/office-hours is the full URL that provides direct access to the page listing the clerk's office's telephone numbers and hours of operations.

27. In addition, consumers today increasingly access the Internet through multiple devices and, as a result, they typically use the services of more than one ISP. *See* Cisco, *Cisco Visual Networking Index (VNI), Complete Forecast Update, 2017–2022*, at 22 (Dec. 2018). In using several devices, many of which are mobile, consumers "constantly shift from one ISP to another, not just for home and work, but among many WiFi hotspots and other locations from which they connect to the Internet," providing ISPs mere "episodic glimpses" of a customer's Internet usage. Swire Study at 25.

28. These same developments have not affected the ability of edge providers and software developers to access Internet-usage information. *See* Swire Study at 11-14. To the contrary, edge providers are obtaining ever more comprehensive and detailed customer information by tracking customers across devices. *See id.* at 116-18.

29. Because of their greater access to comprehensive customer information, edge providers and software developers have become dominant players in the market for targeted advertising. Last year, nine of the top 10 largest digital ad sellers were projected to be edge providers or software developers, not ISPs. *See* Jasmine Enberg, *Global Digital Ad Spending 2019*, eMarketer (Mar. 2019), https://bit.ly/2FRu2lB.

30. The FTC's enforcement data reflects that ISPs are rarely the object of enforcement actions concerning consumer privacy. Of the 101 Internet privacy-related enforcement actions the FTC brought between 2008 and 2018, only one action involved an ISP.[2] U.S. Government Accountability Office, *Internet Privacy Report* 21 (Jan. 2019),

[2] This sole ISP was Level 3 Communications, LLC, which settled charges that it falsely claimed to participate in the international privacy framework called the U.S.-EU Safe Harbor. *See* FTC, Press Release, FTC Approves Final Orders Settling Charges of U.S.-EU Safe Harbor Violations Against 14 Companies, https://bit.ly/2OQIwGI.

https://bit.ly/2Hkx2XL. The others involved edge providers, software developers, and brick-and-mortar manufacturers also conducting business online, among others. *See id.* Moreover, several of the FTC's privacy-related enforcement actions involved product manufacturers or other brick-and-mortar businesses outside the Internet ecosystem, *see id.*, underscoring that consumer privacy interests are implicated by the actions of all consumer-facing businesses, not just those within the Internet ecosystem — and certainly not by ISPs alone.

Federal Internet Privacy Rules

31. The federal government has determined that consumer privacy is best protected through a technology-neutral, uniform, and nationwide approach applicable to all businesses and governed by a single regulator — the FTC — and not through a regime that addresses only ISPs.

32. The FTC has decades of experience bringing enforcement actions pursuant to uniform federal privacy standards that apply evenly to all businesses — including ISPs, edge providers, and brick-and-mortar retailers — nationwide. Indeed, in its traditional role "as the cop on the broadband beat," the FTC "has vigorously protected the privacy and security of consumer data." *Statement from Acting FTC Chairman Maureen K. Ohlhausen on the FCC's Approval of the Restoring Internet Freedom Order*, Federal Trade Commission (Dec. 14, 2017), https://bit.ly/2Ho4egW. That uniform, technology-neutral approach has long enjoyed broad support among consumers and the federal government. *See, e.g.*, Progressive Policy Institute, *Recent National Survey of Internet Users* (May 26, 2016), https://bit.ly/3bGusth (reporting that 94% of Internet users agreed that "[a]ll companies collecting data online should follow the same consumer privacy rules"); *Protecting Consumer Privacy in an Era of Rapid Change*, FTC, at 56 (Mar. 2012), https://bit.ly/2vsiT8m ("any privacy framework should be technology neutral"); Executive Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, White House

Report, at 36 (Feb. 2012), https://bit.ly/2vAlywv (recommending "a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency in the basis for FTC enforcement actions").

33. In 2016, the FCC departed from that uniform, technology-neutral approach to privacy regulation and sought to impose restrictions on what ISPs — and *only* ISPs — could do with "customer proprietary information." Report and Order, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 31 FCC Rcd. 13911 (2016) ("*ISP Privacy Order*").

34. Among other things, the *ISP Privacy Order* required ISPs to obtain "opt-in" consent to use, disclose, or permit access to "sensitive" customer proprietary information, and to permit customers to "opt out" of letting the ISP use, disclose, or permit access to "non-sensitive" customer proprietary information. *ISP Privacy Order* ¶ 9. But the *ISP Privacy Order* imposed no restrictions on the use of information that could not be "linked" to an individual (for example, aggregated or anonymized data). 47 C.F.R. § 64.2002(m) (2016). It permitted ISPs to use customer data to provide services and to make disclosures required by law. *See ISP Privacy Order* ¶ 9. And it allowed ISPs to offer discounts, benefits, or other incentives in exchange for customers' providing opt-in consent, as long as the ISP clearly described the offer's terms. *Id.* ¶¶ 298-303.

35. The *ISP Privacy Order* was short-lived. In 2017, Congress passed and the President signed a joint resolution under the Congressional Review Act, *see* 5 U.S.C. § 801(b)(1), repealing the *ISP Privacy Order* and stating that: "Congress disapproves the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 Fed. Reg. 87274

(December 2, 2016)), and such rule shall have no force or effect." Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017). The joint resolution not only vacated the *ISP Privacy Order*, but also precludes the FCC or any other federal agency from adopting "a new rule that is substantially the same" as the *ISP Privacy Order* unless "specifically authorized" by a subsequent act of Congress. 5 U.S.C. § 801(b)(2).

36. Members of Congress explained that the FCC's approach of targeting only ISPs would "arbitrarily treat ISPs differently from the rest of the internet, creating a false sense of privacy" among consumers. 163 Cong. Rec. at H2495 (Mar. 28, 2017) (statement of Rep. Lance). "[S]eparating edge providers from ISPs," one sponsor explained, "creates confusion for both consumers and business operations," and repeal of the *ISP Privacy Order* was therefore necessary to "reduce the confusion that has been created from this unnecessary regulation that has stifled competition and impeded innovation." *Id.* at H2497 (statement of Rep. Collins).

37. Another House sponsor observed that ignoring the rest of the industry by targeting only ISPs would do little to accomplish the FCC's stated objectives, in light of substantial evidence showing that "ISPs now have increasingly limited insight into our activities and information online." 163 Cong. Rec. at H2490 (statement of Rep. Blackburn). In contrast, "so-called edge providers, like search engines, social media, advertising, shopping, and other services online, often have greater visibility into personal consumer data." *Id.*

38. Members of Congress also emphasized the need for uniform enforcement of privacy practices across the Internet, in lieu of a patchwork of burdensome and inconsistent regulations. As one of the House sponsors explained, "[t]he FTC has served as our Nation's sole online privacy regulator for over 20 years" and having other "privacy cops on the beat will create confusion within the internet ecosystem and will end up harming consumers." 163 Cong. Rec. at

H2489 (statement of Rep. Blackburn). By repealing the *ISP Privacy Order*, Congress intended to "put[ ] all segments of the internet on equal footing and provide[ ] American consumers with a consistent set of privacy rules." *Id.* at H2495 (statement of Rep. Lance).

39. The FCC subsequently reaffirmed that it does not serve the public interest to subject ISPs to a separate and different privacy regime than other businesses. Instead, the FCC found that ISPs, no different from edge providers or other online and offline businesses, should fall under the jurisdiction of the FTC, which is the only consumer protection agency with enforcement power that "operates on a national level across industries." Declaratory Ruling, Report and Order, and Order, *Restoring Internet Freedom*, 33 FCC Rcd 311, ¶ 183 (2018) ("*RIF Order*"), *petitions for review denied in pertinent part*, *Mozilla Corp. v. FCC*, 940 F.3d 1 (D.C. Cir. 2019). The FCC concluded that "[r]estoring FTC jurisdiction over ISPs will enable the FTC to apply its extensive privacy and data security expertise to provide the uniform online privacy protections [across the Internet ecosystem] that consumers expect and deserve." *Id.* ¶ 181. This reflects the practical reality that the Internet necessarily operates across state lines and throughout myriad industries.

40. As a complement to restoring jurisdiction over ISPs' privacy and data security practices to the FTC, the FCC concluded that ISPs should comply with a narrow Transparency Rule requiring them to make "[a] complete and accurate disclosure about the ISP's privacy practices," including "whether any network management practices entail inspection of network traffic, and whether traffic [information] is stored, provided to third parties, or used by the ISP for non-network management purposes." *RIF Order* ¶ 223. The FCC determined that these privacy-related disclosures "inform the [FCC], consumers, entrepreneurs, and other small businesses about the parameters of the service, without imposing costly burdens on ISPs." *Id.*

To the extent an ISP acts inconsistently with its stated policies, the FCC determined, the FTC can protect consumer interests by "tak[ing] [enforcement] action against deceptive ISP conduct." *Id.* ¶ 244.

41. The FCC determined that a combination of requiring disclosure of ISP privacy practices, together with consumer protection enforcement by the FTC, better comported with those goals than "complex and highly prescriptive privacy regulations for broadband Internet access service." *RIF Order* ¶ 158.

42. Separately, the FCC requires ISPs to submit data about their subscribers, including the number of active customers the ISP currently serves within each specified geographic area, to the agency on Form 477. *See* 47 C.F.R. § 1.7001. To comply with this reporting requirement, ISPs must use information they have collected that pertains to their customers, including the number of customers per location based on residential address, geolocation information, and telephone number. Failing to file Form 477 subjects an ISP to "enforcement action pursuant to the Act and any other applicable law." *Id.* § 1.7001(f).

Maine Enacts L.D. 946

43. On June 6, 2019, Maine enacted L.D. 946 — an ISP-only privacy law and "the nation's strictest" information privacy statute to date. Casey Leins, *Maine Passes Nation's Strictest Internet Privacy Protection Law*, U.S. News (June 7, 2019), https://bit.ly/2mgQAFt. The Statute takes effect on July 1, 2020. L.D. 946, § 2.

44. The sponsors of L.D. 946 expressly intended to reinstate the rules from the *ISP Privacy Order* that Congress had repealed. As one of the bill's co-sponsors explained: "In April 2017, the U.S. Congress voted to reverse new privacy protections from the [FCC] that would have required [ISPs] to seek customers' permission before sharing their personal information"; "[s]oon after," the Maine House responded by introducing legislation to "fill the gap created by

the Congress." Hearing on LD 946, An Act To Protect the Privacy of Online Consumer Information (Apr. 24, 2019) (Testimony of Sen. Guerin).

45. The Statute applies *solely* to ISPs — "providers" of "broadband Internet access service," defined as "mass-market retail service[s]," including fixed and mobile Internet access that "provides the capability to transmit data to and receive data from all or substantially all Internet endpoints." Me. Rev. Stat. tit. 35-A, § 9301(1)(A), (D). It leaves wholly unregulated the vast majority of entities — online and offline — that collect and use the same customer personal information and for the same or similar purposes as ISPs.

46. The Statute requires "express, affirmative consent" — that is, opt-in consent — for any use, disclosure, sale, or access to "customer personal information." Me. Rev. Stat. tit. 35-A, § 9301(2), (3)(A).

47. The Statute broadly defines "customer personal information" to include both (1) "[p]ersonally identifying information about a customer, including but not limited to the customer's name, billing information, social security number, billing address and demographic data," and (2) "[i]nformation from a customer's use of broadband." Me. Rev. Stat. tit. 35-A § 9301(1)(C)(1), (2). Although the Statute lists certain categories of information falling within each prong, it makes clear that these are simply non-exclusive examples of "customer personal information." *Id.* The Statute thus demands opt-in consent for a vast swath of information *regardless* of sensitivity — including technical information such as an IP address used to connect a customer to the Internet — a demand that even the *ISP Privacy Order* did not impose. Indeed, the Statute's opt-in consent requirement apparently restricts even the use of information that is not "[p]ersonally identifying information" at all, including anonymized or aggregated data, if that

information is data derived "from a customer's use of broadband Internet access service." *Id.* § 9301(1)(C)(2).

48. The Statute also prohibits ISPs from offering customers discounts, rewards in loyalty programs, marketing offers for other products and services, or other cost-saving benefits in exchange for their agreement to opt in. Me. Rev. Stat. tit. 35-A § 9301(3)(B)(2).

49. The Statute's opt-in regime is subject to limited exceptions. *See, e.g.*, Me. Rev. Stat. tit. 35-A, § 9301(2) ("A provider may not use, disclose, sell or permit access to customer personal information, except as provided" by specified Maine and federal laws); *id.* § 9301(4) (listing other exceptions). For example, the Statute permits an ISP to "advertise or market the provider's *communications*-related services to the customer" without securing opt-in consent, *id.* § 9301(4)(B) (emphasis added), but prohibits ISPs from advertising or marketing *non*-communications related services to its customers, absent opt-in consent. Similarly, the Statute rightly allows ISPs to provide "geolocation information concerning the customer" to public safety officials in certain emergencies, *id.* § 9301(4)(F), but prohibits them from using this same information to make location-based public service announcements even at the behest of State or local authorities, absent opt-in consent.

50. Although the Statute permits ISPs to use customer personal information to comply with Maine's laws governing production of specific content and information in court proceedings or Section 2703 of the federal Stored Communications Act, Me. Rev. Stat. tit. 35-A, § 9301(2), it does not include an exception for compliance with other state or federal laws, such as the FCC's Form 477 reporting requirement.

51. While "customer personal information" is defined extremely broadly, the Statute restricts even the use of "information the provider collects pertaining to a customer that is *not*

customer personal information," if the customer opts out of that use. Me. Rev. Stat. tit. 35-A, § 9301(3)(C) (emphasis added). The Statute does not attempt to clarify what types of data, if any, "pertain[] to a customer" but do not qualify as "customer personal information" subject to the opt-in regime.

52. The Statute's opt-out regime for information that is not customer personal information is not subject to any exceptions. *See* Me. Rev. Stat. tit. 35-A, § 9301(4) (exceptions limited to the use of "customer personal information").

53. The Statute purports to have a limited geographic scope, applying "to providers operating within the State when providing broadband Internet access service to customers that are physically located and billed for service received in the State." Me. Rev. Stat. tit. 35-A, § 9301(7). But it is unclear whether and to what extent the Statute applies when non-Maine residents use their mobile broadband Internet access services during the time they visit Maine.

54. These provisions render the Statute an extreme outlier, even compared to other state privacy laws. In general, other state privacy laws provide opt-out rights for most consumer data and reserve opt-in consent for a narrow subset of *sensitive* personal information. *See, e.g.*, Cal. Civ. Code § 1798.120 (2019); Nev. SB 220 § 2 (2019); Minn. Stat. § 325M.04(2) (2003); *see also* FTC Privacy Framework, https://bit.ly/2HodYI1 at 58-60 (affirmative opt-in consent should be obtained with respect to sensitive data, such as financial, health, or children's information, Social Security numbers, and precise, individualized geolocation data). In addition, other state privacy laws apply only to information that is linked (or reasonably could be linked) to a particular individual, and none imposes restrictions on anonymized or aggregated data. *See, e.g.*, Cal. Civ. Code § 1798.140(o), *as amended by* AB 874 (Oct. 11, 2019); Nev. Stat. Rev. § 603A.320 (2019); Minn. Stat. § 325M.01(5). Finally, other state privacy laws do not

arbitrarily limit the business's ability to communicate with its own customers, or forbid the business from offering discounts or other incentives in exchange for consent. *See* Cal. Civ. Code §§ 1798.120; 1798.125; Minn. Stat. § 325M.02; Nev. Rev. Stat. § 205.498 (1999); Nev. SB 220, §§ 1.6, 2.

55. The Statute also imposes far more burdensome restrictions than even the repealed *ISP Privacy Order*. For example, the *ISP Privacy Order* distinguished between sensitive and non-sensitive customer information, requiring opt-in consent for the former and opt-out consent for the latter. It did not purport to regulate in any manner aggregated or anonymized data that poses no threat to consumer privacy. *See ISP Privacy Order* ¶ 61 ("Our rules allow providers to use and disclose customer data without approval if the data is properly de-identified."). It expressly permitted discounts and other cost-saving incentives in exchange for consent as long as these offers are clearly explained to consumers. *See id.* ¶ 294 ("We also adopt heightened disclosure and affirmative consent requirements for [ISPs] that offer customers financial incentives, such as lower monthly rates, in exchange for the right to use the customers' confidential information."). And it contained critical exceptions that the Statute omits, including an exception permitting the use of customer information whenever "otherwise required or authorized by law" and to "protect the [ISP's] rights or property." 47 C.F.R. § 64.2004(a)(3), (6) (2016).

CLAIMS FOR RELIEF

Count One:
The Statute Violates The First Amendment

56. Plaintiffs incorporate all preceding paragraphs by reference.

57. The First Amendment to the U.S. Constitution, applicable to the States through the Fourteenth Amendment, provides that "Congress shall make no law . . . abridging the freedom of speech." U.S. Const. amend. I.

58. ISPs use customer information internally and to engage in a wide variety of beneficial, pro-consumer speech. For example, by using customer information, ISPs are able to communicate with their customers effectively and efficiently, to engage in competitive marketing and advertising, to facilitate geographically targeted public service announcements, and to comply with mandatory federal reporting requirements.

59. The Statute burdens ISPs' protected speech by restricting how they use information for those purposes. *See Sorrell*, 564 U.S. at 570 ("[T]he creation and dissemination of information are speech within the meaning of the First Amendment."); *see also id.* at 557 ("Speech in aid of . . . marketing . . . is a form of expression protected by the Free Speech Clause of the First Amendment."); *U.S. West*, 182 F.3d at 1232 (prohibition on "using [customer information] to target customers" constitutes speech restriction).

60. The Statute restricts not only protected commercial speech — communications that do "no more than propose a commercial transaction," *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 776 (1976) — but also non-commercial speech, including the use of information for non-advertising purposes, such as location-based public service announcements and mandatory reports to the government.

61. The Statute is subject to strict scrutiny because "on its face and in its practical operation" the law "imposes a burden based on the content of speech and the identity of the speaker." *Sorrell*, 564 U.S. at 567; *see also Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2230 (2015). Strict scrutiny applies "regardless of the government's benign motive, content-neutral

justification, or lack of 'animus toward the ideas contained' in the regulated speech." *Reed*, 135 S. Ct. at 2228.

62. The Statute imposes speaker-based restraints because it is "aimed at" and burdens just one category of speaker — ISPs and ISPs alone. *Sorrell*, 564 U.S. at 567. But it leaves other speakers (including edge providers, data brokers, and offline retailers) free to use the same or even greater quantities of customer personal information, regardless of how sensitive it may be, for any purpose whatsoever. The Statute thus "has the effect of preventing [ISPs] — and only [ISPs] — from communicating . . . in an effective and informative manner." *Id.* at 564. "[G]overnment regulation may not favor one speaker over another." *Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 828 (1995).

63. Moreover, the Statute is shot through with content-based distinctions. For example, ISPs need not obtain customer consent to use customer personal information for the purpose of marketing "communications-related services to the customer." Me. Rev. Stat. tit. 35-A, § 9301(4)(B). But ISPs must obtain opt-in consent to use the same information to market *non*-communications-related services to the same customer. Similarly, it permits the use of geolocation information for certain emergency calls, but prohibits use of that same data for geographically specific public service announcements in closely related situations. *Id.* § 9301(4)(F).

64. The Statute cannot survive strict scrutiny because Maine cannot "prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest." *Reed*, 135 S. Ct. at 2231; *see also National Fire Adjustment Co. v. Cioppa*, 357 F. Supp. 3d 38, 44 (D. Me. 2019) ("Content-based regulations are presumptively violative of expressive rights and will stand only where the regulation is narrowly tailored to serve a compelling state interest.").

65. The Statute does not adopt "the least restrictive means among available, effective alternatives" to protect Internet privacy. *Rideout v. Gardner*, 838 F.3d 65, 71 (1st Cir. 2016). It prohibits ISPs from using non-sensitive customer personal information absent opt-in consent, rather than a less restrictive opt-out alternative. Maine's failure to employ this "obvious and substantially less restrictive alternative, an opt-out strategy, indicates that it did not narrowly tailor" the Statute. *U.S. West*, 182 F.3d at 1238-39.

66. Although the Statute is subject to strict scrutiny, it cannot survive even intermediate scrutiny.

67. To satisfy intermediate scrutiny, the State must establish a substantial interest in regulating privacy, not merely "in the abstract," but "in the circumstances of this case." *California Democratic Party v. Jones*, 530 U.S. 567, 584 (2000) (emphasis omitted). The State also must show that the Statute "directly advances" the substantial government interest and "is not more extensive than is necessary to serve that interest." *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y.*, 447 U.S. 557, 566 (1980). The State's burden is a heavy one: It "is not satisfied by mere speculation or conjecture; rather, a [State] seeking to sustain a restriction on commercial speech must demonstrate that *the harms it recites are real* and that its restriction will in fact alleviate them to *a material degree*." *Edenfield v. Fane*, 507 U.S. 761, 770-71 (1993) (emphasis added); *see also Rubin v. Coors Brewing Co.*, 514 U.S. 476, 490 (1995) ("anecdotal evidence and educated guesses" are not enough).

68. Maine cannot carry this burden. The State made no attempt to show that ISPs' practices have harmed consumer privacy. Indeed, the Legislature did not make any findings *at all*, let alone that ISPs — which have taken affirmative steps to protect consumers' privacy and data security — pose a special threat to consumer privacy relative to the many other

organizations doing businesses in Maine that use this data without restriction to the same or greater extent. Nor did the Legislature make findings that its ISP-specific rules are necessary in light of existing, uniform technology-neutral federal privacy rules. Without any evidence in the legislative record, Maine cannot show that its "recited harms" "are real" rather than "merely conjectural" in this context. *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 664 (1994); *Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180, 211 (1997) ("[T]he question is whether the legislative conclusion was reasonable and supported by substantial evidence *in the record before Congress*.") (emphasis added).

69. In addition, the Statute's restrictions are both overinclusive and underinclusive, not "narrowly drawn" to protect consumer privacy. *Central Hudson*, 447 U.S. at 565.

70. The Statute restricts speech well beyond what is plausibly necessary to "protect customer privacy" and, therefore, is fatally overinclusive. *U.S. West*, 182 F.3d at 1238-39. On its face, the Statute "regulate[s] speech that poses no danger" to privacy, *Central Hudson*, 447 U.S. at 565, including the use of information "that is *not* customer personal information," Me. Rev. Stat. tit. 35-A, § 9301(3)(C) (emphasis added), or that is anonymized and thus does not *identify* any individuals, let alone harm their privacy, *id.* § 9301(1)(C)(2). And it imposes an overly restrictive opt-in regime for non-sensitive customer personal information, and even for certain information that is not personally identifying, where an opt-out alternative was available. *See U.S. West*, 182 F.3d at 1238-39 (holding that a privacy law was unconstitutional where the government failed to "adequately show that an opt-out strategy would not sufficiently protect customer privacy").

71. The Statute also applies to ISPs alone, notwithstanding that myriad other businesses use the same, and even more, customer personal information as ISPs. It is, therefore,

fatally underinclusive. The Supreme Court has repeatedly invalidated laws that similarly "select among speakers conveying virtually identical messages" in ways that bear no "meaningful relationship to the particular [State interest] asserted." *Greater New Orleans Broad. Ass'n, Inc. v. United States*, 527 U.S. 173, 193-94 (1999) (law restricted casino advertising by private casinos but not tribal or government casinos); *Rubin*, 514 U.S. at 488 (law restricted alcohol content on beer labels but not on wine and spirit labels); *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 428 (1993) (city could not ban "newsracks dispensing 'commercial handbills'" while permitting newsracks dispensing newspapers).

72. Finally, the Statute draws irrational distinctions that cannot be explained as an attempt to protect consumer privacy. For example, as explained above, it allows communications about certain kinds of ISPs' services, but not others, and permits ISPs to provide consumers' geolocation information in certain types of emergency situations, but not others. And although the Statute does not require ISPs to obtain opt-in approval to comply with a court order or specified Maine and federal laws, it does require ISPs to do so before using customer personal information to comply with other federal or state laws or civil discovery obligations because, unlike the *ISP Privacy Order* and other privacy laws, the Statute does not contain an exception for using information "[a]s otherwise required or authorized by law." 47 C.F.R. § 64.2004(a)(6) (2016).

73. Thus, even assuming the State could satisfy the threshold requirement of identifying a real privacy harm linked to ISPs (which, as explained above, it cannot), the Statute is nevertheless invalid because it "provides only ineffective and remote support" for addressing that allegedly substantial interest. *El Dia, Inc. v. Puerto Rico Dep't of Consumer Affairs*, 413 F.3d 110, 115 (1st Cir. 2005). The law "is so pierced by exemptions and inconsistencies that the

[State] cannot hope to exonerate it." *Greater New Orleans Broad.*, 527 U.S. at 190; *see also Rubin*, 514 U.S. at 489 (statute's "exemptions and inconsistencies . . . ensure[ ] that the labeling ban will fail to achieve [its] end").

Count Two:
The Statute Is Void For Vagueness

74. Plaintiffs incorporate all preceding paragraphs by reference.

75. "It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined." *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). A statute contravenes that principle if "a person of average intelligence would be forced to guess at its meaning and modes of application." *National Org. for Marriage v. McKee*, 649 F.3d 34, 65 (1st Cir. 2011) (quotation marks omitted).

76. The vagueness doctrine "requires a 'greater degree of specificity' in cases involving First Amendment rights." *National Org. for Marriage*, 649 F.3d at 65 (quoting *Buckley v. Valeo*, 424 U.S. 1, 77 (1976)).

77. The Statute defines "[p]ersonally identifying information" to include both obviously identifying information — *e.g.*, a consumer's "name," "billing address," and "social security number" — and information that is not, on its own, personally identifying at all, including "billing information" and "demographic data" (*e.g.*, age, marital status, income). Me. Rev. Stat. tit. 35-A, § 9301(1)(C)(1). Because "[p]ersonally identifying information" is further defined to "includ[e] but not [be] limited," *id.*, to this "confusing list of examples," the Statute is unlawfully vague, *Johnson*, 135 S. Ct. at 2561. It leaves persons of "average intelligence . . . to guess" about the scope of the Statute's restrictions. *National Org. for Marriage*, 649 F.3d at 65.

78. The Statute also does not define at all the category of information "pertaining to a customer that is not customer personal information" and that is subject to the Statute's opt-out

requirement. Me. Rev. Stat. tit. 35-A, § 9301(3)(C). ISPs are therefore left to guess at when information that is not within the Statute's definition of customer personal information nonetheless "pertain[s] to a customer."

79. The full reach of the Statute's geographic scope is equally vague. While it clearly applies to Maine residents who purchase broadband Internet access service for use in Maine and who use that service while physically located in Maine, *see* Me. Rev. Stat. tit. 35-A, § 9301(7), no clear "standard of conduct" makes it "possible to know" whether the Statute extends to non-Maine residents who use their mobile broadband Internet access services while they temporarily visit Maine, *International Harvester Co. of Am. v. Kentucky*, 234 U.S. 216, 221-22 (1914).

80. These ambiguities deprive ISPs of "fair warning" as to what the Statute prohibits, "chilling the exercise of [their] First Amendment rights" as they aim for compliance. *National Org. for Marriage*, 649 F.3d at 62. The Statute therefore is void for vagueness.

Count Three:
The Statute Conflicts With And Is Preempted By
Congress's Joint Resolution Under The Congressional Review Act

81. Plaintiffs incorporate all preceding paragraphs by reference.

82. "[T]he Supremacy Clause nullifies state laws that interfere with, or are contrary to federal laws," *Bower v. Egyptair Airlines Co.*, 731 F.3d 85, 92 (1st Cir. 2013) (quotation marks omitted), including where a state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress," *Crosby v. National Foreign Trade Council*, 530 U.S. 363, 373 (2000).

83. The Congressional Review Act provides that a final agency rule "shall not take effect" if Congress enacts and the President signs a joint resolution disapproving of the rule. 5 U.S.C. § 801(b)(1). It also prohibits federal adoption of "substantially the same" rule absent

express congressional authorization. 5 U.S.C. § 801(b)(2). Like all resolutions "enacted in accordance with [the Constitution's] bicameralism and presentment requirements," joint resolutions under the Congressional Review Act carry the full force and effect of federal law. *Nuclear Energy Inst., Inc. v. EPA*, 373 F.3d 1251, 1309 (D.C. Cir. 2004).

84. In April 2017, Congress repealed the *ISP Privacy Order* under the Congressional Review Act. *See* Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017). The Joint Resolution reflects Congress's judgment that imposing privacy rules only on ISPs and not any other actor in the Internet ecosystem would undermine the public interest by creating a false sense of privacy, sowing confusion for both consumers and businesses, stifling competition, and impeding innovation in the Internet marketplace. Congress also made clear that a uniform, technology-neutral approach, rather than a patchwork of burdensome regulation, was necessary to give consumers consistent privacy protection. As members of Congress explained, the Joint Resolution advanced the goal of "restoring regulatory balance to the internet ecosystem" by establishing "a single, uniform set of privacy rules" administered by the FTC. 163 Cong. Rec. at S1928 (statement of Sen. Thune); *see also* 163 Cong. Rec. at H2495 (statement of Rep. Lance) (Congress sought to "provide[ ] American consumers with a consistent set of privacy rules").

85. The Statute was expressly intended to undo this act of Congress by reinstating privacy regulations only on ISPs and not any other companies. As noted above, one of the Statute's co-sponsors indicated that the Statute was intended to "fill the gap created by the Congress." Hearing on LD 946, An Act To Protect the Privacy of Online Consumer Information (Apr. 24, 2019) (Testimony of Sen. Guerin). Specifically, the Statute imposes many of the rules in the *ISP Privacy Order* that Congress vacated, but without the FCC's exceptions for non-sensitive information, 47 C.F.R. § 64.2004(b) (2016) (subjecting this information to a less

burdensome opt-out regime), non-identifying information, *ISP Privacy Order* ¶¶ 106, 110 (explaining that de-identified or aggregated data not "linkable" to any individual is not subject to any consent regime), or using information "[a]s otherwise required or authorized by law," 47 C.F.R. § 64.2004(a)(6) (2016).

86. As a result, the Statute conflicts with the Joint Resolution's repeal of the *ISP Privacy Order* and undermines the federal objectives that Congress sought to promote through this repeal. And it does so to an even greater extent than the FCC's Congressionally disapproved rule by not only reinstating the *ISP Privacy Order* at the state level but also by making it even more burdensome and disruptive.

87. The Joint Resolution prohibiting the federal adoption of privacy rules applicable only to ISPs and not any other companies applies *a fortiori* to a patchwork of state laws that seek to do the same — or, in the case of the Statute, more. And because it is binding federal law, it preempts such state laws that "frustrate the purposes of the federal scheme," including the Statute. *SPGGC, LLC v. Ayotte*, 488 F.3d 525, 531 (1st Cir. 2007).

Count Four:
The Statute Conflicts With And Is Preempted By
The FCC's *RIF Order*

88. Plaintiffs incorporate all preceding paragraphs by reference.

89. Regulations adopted by a federal agency acting within the scope of its congressionally delegated authority preempt "any state or local law that conflicts with such regulations or frustrates the purposes thereof." *City of New York v. FCC*, 486 U.S. 57, 64 (1988).

90. Acting pursuant to congressionally delegated authority in the *RIF Order*, the FCC determined that the best way to protect consumers' privacy interests "without imposing costly burdens on ISPs" is to pair mandatory privacy disclosures, *RIF Order* ¶ 223, with FTC enforcement of those disclosures, *id.* ¶ 244. That approach applied the FTC's technology-neutral

privacy framework to ISPs and non-ISPs alike, instead of imposing restrictions only on ISPs and not any other companies regarding the use of consumer data. *Id.* ¶¶ 181-183, 244-245.

91. The Statute conflicts with the FCC's determination about the best way to protect consumers' privacy interests by re-imposing the *ISP Privacy Order*'s "highly prescriptive privacy regulations for broadband Internet access service." *RIF Order* ¶ 158.

92. Because the Statute conflicts with and frustrates the federal goals articulated in the *RIF Order* of encouraging competition and innovation, while avoiding patchwork, burdensome, and ISP-specific privacy regulations, it is preempted. *See City of New York*, 486 U.S. at 64.

Count Five:
The Statute Conflicts With And Is Preempted By
Federal Law Requiring Disclosure Of Information

93. Plaintiffs incorporate all preceding paragraphs by reference.

94. Federal law mandates that ISPs disclose certain consumer information that the Statute subjects to individual customer consent, making compliance with both "impossible" and thus rendering the Statute void. *Algonquin Gas Transmission, LLC v. Weymouth*, 919 F.3d 54, 63 (1st Cir. 2019) (upholding finding that conflict preemption prohibits application of local ordinance contrary to application of federal permitting law).

95. For example, ISPs cannot comply with FCC Form 477 — which requires that ISPs report "the total number of connections in each census tract [*e.g.*, subdivision of a county] in which they provide service," Report and Order, *Establishing the Digital Opportunity Data Collection Modernizing the FCC Form 477 Data Program*, 34 FCC Rcd 7505, ¶ 7 (2019) — without using "billing address[es]," Me. Rev. Stat. tit. 35-A, § 9301(1)(C)(1), to prepare the information they are required to disclose and then using and disclosing to the FCC location-based and demographic "information the provider collects pertaining to a customer that is not

customer personal information," *id.* § 9301(3)(C). But the Statute prohibits the use of billing addresses unless a customer opts in, and prohibits the use or disclosure of information pertaining to a customer if the consumer opts out. *Id.* § 9301(3)(A), (C). And its exceptions for specifically enumerated federal laws, *id.* § 9301(2), (4)(C), omit mandatory Form 477 disclosures, *see* 47 C.F.R. § 1.7001(f) (mandating Form 477 disclosures).

96. Moreover, the Statute permits ISPs to disclose information to "comply with a lawful court order," *id.* § 9301(4)(C), but it makes no exception for mandatory disclosures required by the Federal Rules of Civil Procedure for civil discovery, *see* Fed. R. Civ. P. 26(a), and it lacks the broader exception contained in the *ISP Privacy Order* for uses or disclosures "otherwise required or authorized by law." 47 C.F.R. § 64.2004(a)(6) (2016); *see McCoy v. Mass. Inst. of Tech.*, 950 F.2d 13, 21 (1st Cir. 1991) (explaining that the Federal Rules of Civil Procedure "have the same force and effect as federal statutory law").

97. The Statute violates the Supremacy Clause because it allows consumers to dictate (by opting out or declining to opt in) when ISPs can use or disclose information that they must rely on to comply with federal law, rendering "compliance with both" state and the foregoing federal laws "impossible." *Algonquin Gas*, 919 F.3d at 63 (quoting *Oneok, Inc. v. Learjet, Inc.*, 135 S. Ct. 1591, 1595 (2015)).

PRAYER FOR RELIEF

An actual controversy has arisen between the parties entitling Plaintiffs to legal, declaratory, and injunctive relief.

WHEREFORE, Plaintiffs demand judgment against Defendants as follows:

A. A declaration, pursuant to 28 U.S.C. § 2201, that the Statute violates the First Amendment to the United States Constitution;

B. A declaration, pursuant to 28 U.S.C. § 2201, that the Statute violates the Due Process Clause of the Fourteenth Amendment to the United States Constitution;

C. A declaration, pursuant to 28 U.S.C. § 2201, that the Statute violates the Supremacy Clause of the United States Constitution;

D. An injunction prohibiting Defendants in their official capacities — as well as Defendants' officers, agents, employees, and all persons acting in concert with them who receive actual notice of the injunction — from enforcing or threatening to enforce the Statute and any implementing regulations, thereby depriving Plaintiffs of their rights under the First and Fourteenth Amendments to the Constitution of the United States. *See* 42 U.S.C. § 1983;

E. All costs, attorneys' fees, and expenses that Plaintiffs reasonably incur, *see* 42 U.S.C. § 1988; and

F. Such other relief as this Court deems just and proper.

Dated: February 14, 2020

Respectfully submitted,

By /s/ Joshua A. Randlett

Joshua A. Randlett
RUDMAN WINCHELL
84 Harlow Street
P.O. Box 1401
Bangor, ME 04402
Email: jrandlett@rudmanwinchell.com
Attorneys for all Plaintiffs

Helgi C. Walker*
Jacob T. Spencer*
Nick Harper*
Sarah Akhtar*
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
Email: hwalker@gibsondunn.com

Sarah E. Erickson-Muschko*
GIBSON, DUNN & CRUTCHER LLP
1801 California Street, Suite 4200
Denver, CO 80202
Email: SEricksonmuschko@gibsondunn.com

Attorneys for Plaintiff
NCTA – The Internet & Television Association

Scott H. Angstreich*
Collin R. White*
Alex A. Parkinson*
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, PLLC
1615 M St. NW, Suite 400
Washington, D.C. 20036
Email: sangstreich@kellogghansen.com

Attorneys for Plaintiffs
CTIA – The Wireless Association® and USTelecom – The Broadband Association

Jeffrey A. Lamken*
MOLOLAMKEN LLP
The Watergate, Suite 600
600 New Hampshire Ave., NW
Washington, DC 20037
Email: jlamken@mololamken.com

Attorney for Plaintiff
ACA Connects – America's Communications Association

* *pro hac vice* certification pending