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,

Defendant.

Civil Action No. 1:20-cv-00055-LEW

PLAINTIFFS' MOTION FOR JUDGMENT ON THE PLEADINGS
WITH INCORPORATED MEMORANDUM OF LAW

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii

INTRODUCTION 1

BACKGROUND 3

LEGAL STANDARD 8

ARGUMENT 9

I. The Statute Violates the First Amendment (Count One) 10

A. The Statute Is Subject to and Fails Strict Scrutiny 11

B. In Any Event, the Statute Fails Intermediate Scrutiny 12

II. The Statute Is Void for Vagueness (Count Two) 16

III. Federal Law Preempts the Statute 17

A. The Statute Conflicts with Congress's Vacatur of the FCC's *ISP Privacy Order* (Count Three) 17

B. The Statute Conflicts with the *RIF Order* (Count Four) 19

C. The Statute Makes Compliance with Federal Disclosure Rules Impossible (Count Five) 19

CONCLUSION 20

TABLE OF AUTHORITIES

Page

CASES

Algonquin Gas Transmission, LLC v. Weymouth, 919 F.3d 54 (1st Cir. 2019) 20

Aponte-Torres v. Univ. of Puerto Rico, 445 F.3d 50 (1st Cir. 2006).....9

Arizona v. United States, 567 U.S. 387 (2012).....18

Ark. Elec. Co-op. Corp. v. Ark. Pub. Serv. Comm'n, 461 U.S. 375 (1983).....19

Cal. Democratic Party v. Jones, 530 U.S. 567 (2000) 12-13

Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.,
447 U.S. 557 (1980).....12, 13, 14

City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410 (1993) 15-16

City of New York v. FCC, 486 U.S. 57 (1988).....19

Coates v. City of Cincinnati, 402 U.S. 611 (1971) 17

Curran v. Cousins, 509 F.3d 36 (1st Cir. 2007) 9

Cutting v. City of Portland, 802 F.3d 79 (1st Cir. 2015) 15

Doran v. Salem Inn, Inc., 422 U.S. 922 (1975) 10

Edenfield v. Fane, 507 U.S. 761 (1993) 13

Fantasy Book Shop, Inc. v. City of Boston, 652 F.2d 1115 (1st Cir. 1981).....10

FCC v. Fox Television Stations, Inc., 567 U.S. 239 (2012).....17

Geier v. Am. Honda Motor Co., 529 U.S. 861 (2000).....19

Grayned v. City of Rockford, 408 U.S. 104 (1972) 16, 17

Greater New Orleans Broad. Ass'n, Inc. v. United States, 527 U.S. 173 (1999).....15

Johnson v. United States, 135 S. Ct. 2551 (2015) 16

Lorillard Tobacco Co. v. Reilly, 533 U.S. 525 (2001)..... 13-14

McLaughlin v. City of Lowell, 140 F. Supp. 3d 177 (D. Mass. 2015) 10

Mozilla Corp. v. FCC, 940 F.3d 1 (D.C. Cir. 2019).....19

Nat'l Fire Adjustment Co. v. Cioppa, 357 F. Supp. 3d 38 (D. Me. 2019) 10, 12

Nat'l Org. for Marriage v. McKee, 649 F.3d 35 (1st Cir. 2011) 16, 17

Nuclear Energy Inst., Inc. v. EPA, 373 F.3d 1251 (D.C. Cir. 2004) 18

Reed v. Town of Gilbert, 135 S. Ct. 2218 (2015).....11, 12

Rosenberger v. Rector & Visitors of Univ. of Va., 515 U.S. 819 (1995).....11

Rubin v. Coors Brewing Co., 514 U.S. 476 (1995) 15

Showtime Entm't, LLC v. Town of Mendon, 769 F.3d 61 (1st Cir. 2014) 15

Sorrell v. IMS Health Inc., 564 U.S. 552 (2011) 10, 11, 14

SPGGC, LLC v. Ayotte, 488 F.3d 525 (1st Cir. 2007).....18

Turner Broad. Sys., Inc. v. FCC:

512 U.S. 622 (1994).....11

520 U.S. 180 (1997).....13

U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) 10, 14

Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748 (1976).....12

Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014) 3

Wis. Right To Life, Inc. v. Barland, 751 F.3d 804 (7th Cir. 2014) 16

ADMINISTRATIVE DECISIONS

Declaratory Ruling, Report and Order, and Order, *Restoring Internet Freedom*, 33 FCC Rcd 311 (2018), *petitions for review denied in part*, *Mozilla Corp. v. FCC*, 940 F.3d 1 (D.C. Cir. 2019) 5, 19

Report and Order, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 31 FCC Rcd 13911 (2016) 4, 5, 6, 7, 15, 17, 18

Report and Order and Second Further Notice of Proposed Rulemaking, *Establishing the Digital Opportunity Data Collection; Modernizing the FCC Form 477 Data Program*, 34 FCC Rcd 7505 (2019).....20

CONSTITUTION, STATUTES, REGULATIONS, AND RULES

U.S. Const.:

Art. VI, cl. 2 (Supremacy Clause).....2, 18, 20

Amend. I 1, 2, 9, 10, 15

Communications Act of 1934, 47 U.S.C. § 151 *et seq.* 5, 19

47 U.S.C. § 222(c)(3).....13

Congressional Review Act, 5 U.S.C. § 801 *et seq.* 4, 17

5 U.S.C. § 801(b)(1) 18

Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017).....4, 5, 17, 18

Cal. Civ. Code:

§ 1798.120.....8, 13, 14

§ 1798.125.....8

§ 1798.140(*o*), *as amended by* AB 874 (Oct. 11, 2019).....8

Minn. Stat.:

§ 325M.01(5) 8

§ 325M.02.....8

§ 325M.04(2) 8, 14

Me. L.D. 946 (2019) 1, 5

Me. Rev. Stat. tit. 35-A:

§ 9301(1)(A) 6, 11

§ 9301(1)(C).....6

§ 9301(1)(C)(1).....16, 20

§ 9301(1)(C)(2).....6, 14

§ 9301(2).....6, 7, 20

§ 9301(3)(A) 6, 20

§ 9301(3)(B)(2) 6

§ 9301(3)(C) 7, 13, 16, 17, 20

§ 9301(4) 7

§ 9301(4)(B) 7, 11

§ 9301(4)(C) 7, 20

§ 9301(4)(F) 7, 12

§ 9301(7) 8, 17

Nev. Rev. Stat.:

§ 205.498 8

§ 603A.320 8

Nev. SB 220 (2019) 8, 14

47 C.F.R.:

Pt. 1:

§ 1.7001(f) 7

Pt. 64 6

§ 64.2002(f)(2) 7

§ 64.2002(m) 13

§ 64.2004 ..... 6, 18

Fed. R. Civ. P.:

Rule 12(c) 1, 3, 8

Rule 26(a) 20

LEGISLATIVE MATERIALS

163 Cong. Rec.:

H2467 (Mar. 28, 2017) 4

H2490 (Mar. 28, 2017) 4

H2492 (Mar. 28, 2017) 4

H2495 (Mar. 28, 2017) 4

H2497 (Mar. 28, 2017) 4

S1900 (Mar. 22, 2017) 4

S1928 (Mar. 22, 2017) 4

Hearing on L.D. 946, An Act To Protect the Privacy of Online Customer Information (Apr. 24, 2019), https://bit.ly/3aMTmWZ 5-6, 18

ADMINISTRATIVE MATERIALS

Fed. Trade Comm'n:

Protecting Consumer Privacy in an Era of Rapid Change (Mar. 2012), https://bit.ly/2HodYI1 8

Statement from Acting FTC Chairman Maureen K. Ohlhausen on the FCC's Approval of the Restoring Internet Freedom Order (Dec. 14, 2017), https://bit.ly/2Ho4egW 5

OTHER MATERIALS

Internet Innovation Alliance, *Consumer Data Privacy Concerns* (July 2019), https://bit.ly/3bmV1SW 11

Progressive Policy Inst., *PPI Poll: Recent National Survey of Internet Users* (May 26, 2016), https://bit.ly/3bGusth 11

Plaintiffs ACA Connects – America's Communications Association, CTIA – The Wireless Association®, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association move for judgment on the pleadings under Rule 12(c).

INTRODUCTION

Plaintiffs' members include Internet Service Providers ("ISPs") that provide fixed and mobile broadband Internet access to consumers in Maine and across the country. Plaintiffs' members are only part of the Internet ecosystem: content providers, online retailers, social media companies, and search engines — collectively, "edge providers" — also collect and use consumers' personal information, as do scores of brick-and-mortar retailers and "offline" service providers. So too does an entire industry of data brokers that exclusively monetize consumers' personal information. Plaintiffs and their members are committed to protecting the privacy of their customers' personal information. Further, their privacy practices (like all other Internet companies') are subject to Federal Trade Commission ("FTC") oversight, and they have consistently supported reasonable laws and regulations that protect consumers' personal information uniformly across all of these businesses.

But Maine's L.D. 946 ("the Statute") is not such a law. The Statute's burdensome restrictions on ISPs — and only ISPs — offer no material protection for consumer privacy while burdening protected speech that is beneficial to consumers and disrupting existing federal privacy policies. For multiple reasons, this Court should declare the Statute unconstitutional.

First, the Statute violates the First Amendment. The unprecedented restrictions it imposes on ISPs' speech involving customer information are onerous, irrational, and unnecessary to advance any substantial privacy interest. For example, the Statute requires ISPs to secure "opt-in" consent from their customers before using information that is not sensitive or even personally identifying. And it imposes an "opt-out" consent obligation before ISPs can use

information that the Statute itself defines as *not* customer personal information. The Statute also draws unreasonable distinctions between closely related types of speech: It permits ISPs to advertise *communications-related* services to their customers while limiting how they advertise *non-communications-related* services to those same customers. Yet the Statute imposes no restrictions at all on *non*-ISPs' use, disclosure, or sale of consumer information. The Statute's restrictions are subject to strict scrutiny because they regulate speech based on its content and single out just one category of speaker — ISPs — and cannot pass such exacting scrutiny. But the Statute cannot pass muster under even intermediate scrutiny, because there is no substantial relationship between its restrictions and advancing consumer privacy. The Statute's speech restrictions are also so vague that they force ISPs to guess at the Statute's boundaries and chill protected speech in violation of the First Amendment.

Second, the Statute conflicts with federal law in multiple respects and is therefore preempted under the Supremacy Clause. Maine's decision to impose ISP-specific restrictions conflicts with Congress's decision to eliminate such restrictions in 2017. Indeed, the Maine Legislature enacted the Statute explicitly to override Congress's decision by adopting ISP-specific restrictions even more burdensome than those Congress rejected. The Statute also conflicts with the Federal Communications Commission's ("FCC") determination that a combination of disclosure, competition, and FTC oversight — not ISP-specific restrictions — best balances the federal policies of promoting broadband and protecting consumer privacy. And the Statute makes it impossible for Plaintiffs' members to comply with mandatory federal reporting requirements and other disclosures required by law.

Because Defendant's Answer confirms that the material facts supporting these allegations are undisputed, the Court should enter judgment in Plaintiffs' favor on the pleadings and declare

the Statute unconstitutional, thereby barring Defendant from enforcing it against Plaintiffs and their members. *See* Fed. R. Civ. P. 12(c).

BACKGROUND

Internet Service Providers and Consumer Data. ISPs provide consumers with access to the Internet. They deploy the high-speed links that connect the ISPs' networks to consumers' computers, smart devices, and smartphones, and they operate the equipment and systems that allow consumers to send and receive information from those networks across the Internet. *See* Compl. ¶¶ 21-22, ECF No. 1; *see also Verizon v. FCC*, 740 F.3d 623, 629 (D.C. Cir. 2014). In providing broadband Internet service, ISPs — like virtually all businesses — collect customer personal information, including in the course of verifying subscribers' identities, establishing service connections, processing payments, and providing financing. *See* Compl. ¶¶ 23-24.

But relative to many other businesses, ISPs have less access to the data that customers transmit over the Internet. Individuals increasingly send data over the Internet through encrypted channels, including through websites' widespread adoption of HTTPS. *See id.* ¶ 26. Encryption hides the content of transferred data; when data are encrypted, an ISP can "see" that a customer used its networks to retrieve or send data from or to a particular website (*e.g.*, google.com); but, unlike the edge provider that operates the website, the ISP cannot "see" the content of that communication or determine what actions the customer performed on that website (*e.g.*, the specific search on google.com). *See id.* Most individuals also use several networks managed by different ISPs daily, or even simultaneously, providing individual ISPs with at most snapshots of customer information. *See id.* ¶ 27.

These increasing technological limitations on ISPs' data access contrast sharply with the increasing ease of access enjoyed by other businesses, including those with which ISPs compete (such as in the advertising marketplace). In particular, edge providers and software developers

use their abilities to track customers across devices and to determine what actions customers performed using their services to develop comprehensive and detailed consumer profiles. *See id.* ¶ 28. As a consequence, they — not ISPs — are now the dominant players in the marketplace for targeted advertising. *See id.* ¶ 29.

Congress Affirms a Uniform Approach to Privacy. Both Congress and the FCC have recently acted to restore a uniform, nationwide approach to privacy, enforced by the FTC and applied consistently to ISPs, edge providers, and the many other businesses that collect consumer data — both online and offline. *See* Compl. ¶¶ 31-32. In 2017, Congress enacted and the President signed a Joint Resolution under the Congressional Review Act, 5 U.S.C. § 801 *et seq.*, vacating ISP-specific privacy rules that the FCC had adopted in 2016.[1] Congress did so because the *ISP Privacy Order* had "arbitrarily treat[ed] ISPs differently from the rest of the internet, creating a false sense of privacy." 163 Cong. Rec. H2467, H2495 (Mar. 28, 2017) (statement of Rep. Lance). As one congressional sponsor explained, ISP-only restrictions made no sense given that "ISPs now have increasingly limited insight into our activities and information online," unlike edge providers, which "often have greater visibility into personal consumer data." *Id.* at H2490 (statement of Rep. Blackburn). And "separating edge providers from ISPs" had created "confusion for both consumers and business operations," undermining public interest by impeding "competition" and "innovation." *Id.* at H2497 (statement of Rep. Collins).

Vacating the FCC's order "restor[ed] regulatory balance to the internet ecosystem" through "a single, uniform set of privacy rules." 163 Cong. Rec. S1900, S1928 (Mar. 22, 2017) (statement of Sen. Thune); *see also id.* at H2492 (Mar. 28, 2017) (statement of Rep. Walden)

[1] *See* Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017) (vacating Report and Order, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 31 FCC Rcd 13911 (2016) ("*ISP Privacy Order*")).

("What America needs is one standard, across-the-internet ecosystem, and the [FTC] is the best place for that standard."). The Joint Resolution thus reestablished the FTC in its traditional role "'as the cop on the broadband beat,'" in which role it "'has vigorously protected the privacy and security of consumer data.'" Compl. ¶ 32 (quoting FTC, *Statement from Acting FTC Chairman Maureen K. Ohlhausen on the FCC's Approval of the Restoring Internet Freedom Order* (Dec. 14, 2017), https://bit.ly/2Ho4egW).

After Congress's Joint Resolution, the FCC likewise concluded that it is not in the public interest to subject ISPs to a separate privacy regime. The FCC recognized that ISPs, edge providers, and other online and offline businesses should be subject to the same consumer privacy standards, which are enforced by the FTC — the only consumer protection agency with enforcement power that "operates on a national level across industries." *RIF Order*[2] ¶ 183. Accordingly, the FCC determined, pursuant to its delegated authority under the Communications Act of 1934, that promoting federal broadband policies and the public interest is best achieved through a transparency rule requiring, among other things, that an ISP make "[a] complete and accurate disclosure about the ISP's privacy practices." *Id.* ¶ 223; *see also id.* ¶ 232 (citing statutory authority for privacy practice disclosure rule). The disclosures that the transparency rule mandates are, in turn, enforceable by the FTC, as well as by state attorneys general acting consistently with federal law. *See id*. ¶ 244.

The Statute. On June 6, 2019, Maine enacted L.D. 946, which takes effect on July 1, 2020. The Statute was intended to "fill the gap created by Congress" when it vacated the *ISP Privacy Order*. Hearing on L.D. 946, An Act To Protect the Privacy of Online Customer

[2] Declaratory Ruling, Report and Order, and Order, *Restoring Internet Freedom*, 33 FCC Rcd 311 (2018) ("*RIF Order*"), *petitions for review denied in pertinent part*, *Mozilla Corp. v. FCC*, 940 F.3d 1 (D.C. Cir. 2019) (per curiam).

Information (Apr. 24, 2019) ("L.D. 946 Hearing") (testimony of Sen. Guerin). Like the ISP-specific regime that Congress rejected, the Statute applies only to ISPs that offer "mass-market retail service[s]" that "provide[ ] the capability to transmit data to and receive data from all or substantially all Internet endpoints." *Compare* Me. Rev. Stat. tit. 35-A, § 9301(1)(A) (defining "Broadband Internet access service"), *with ISP Privacy Order* ¶ 40 n.69 (same). But the onerous restrictions that the Statute imposes on ISPs go well beyond those the *ISP Privacy Order* imposed.

To begin with, the Statute requires "express, affirmative consent" — that is, opt-in consent — for *any* "use" of "customer personal information." Me. Rev. Stat. tit. 35-A, § 9301(2), (3)(A). The Statute demands this opt-in consent for a vast swath of information *regardless* of sensitivity. It 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) *non*-personally-identifying information — including anonymized or aggregated data — gleaned from customers' "use of broadband Internet access service." *Id.* § 9301(1)(C).[3] And the Statute forbids ISPs from offering customers *any* benefits — such as discounts, rewards in loyalty programs, and the like — in exchange for their agreement to opt in. *See id.* § 9301(3)(B)(2). By contrast, the *ISP Privacy Order* had distinguished between "sensitive" and "non-sensitive" personal information and limited the requirement of opt-in consent to the former category. *See* 47 C.F.R. § 64.2004.[4] And the *ISP Privacy Order* expressly permitted ISPs to offer discounts and other benefits in exchange for consent. *See ISP Privacy Order* ¶ 294.

[3] This latter category includes, but is "not limited to," nine enumerated categories of information, such as the not personally identifying "media access control address[es]" assigned to interconnected devices. Me. Rev. Stat. tit. 35-A, § 9301(1)(C)(2).

[4] The cited provisions in Part 64 of Title 47 of the Code of Federal Regulations are set forth in Appendix A of the *ISP Privacy Order* at 31 FCC Rcd at 14,080-84.

The Statute's opt-in consent regime is subject to limited and arbitrary 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 use customer personal information 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 it prohibits the same ISP from using the same information to advertise or market the provider's *non*-communications-related services to 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 it prohibits ISPs from using the same information to make location-based public service announcements — even at the behest of state or local authorities — absent opt-in consent. And, while ISPs can disclose customer personal information to comply with a handful of specifically enumerated laws or "a lawful court order," *id.* § 9301(2), (4)(C), they cannot do so to comply with other laws, such as the FCC's mandatory reporting requirements, *see* 47 C.F.R. § 1.7001(f), or civil discovery obligations under the Federal Rules of Civil Procedure.

Further, the Statute restricts the use of "information the provider collects pertaining to a customer that is *not* customer personal information," if a customer opts out. Me. Rev. Stat. tit. 35-A, § 9301(3)(C) (emphasis added). But the Statute leaves the scope of this category undefined. And the Statute provides no exceptions to the restrictions applicable to this undefined category of information. In that respect, too, the Statute goes beyond the vacated *ISP Privacy Order*, which did not impose either opt-in or opt-out consent requirements for the use of information that was not traceable to any particular customer. *See* 47 C.F.R. § 64.2002(f)(2), (m) (defining "customer

proprietary information" as "information that is linked or reasonably linkable to an individual or device").

The Statute applies to ISPs "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 while they are visiting Maine.

The Statute is an outlier among state consumer privacy laws, both because it targets only ISPs and because other state laws distinguish between sensitive and non-sensitive consumer information, requiring opt-in consent only for a narrow subset of information deemed sensitive. *See*, *e.g.*, Cal. Civ. Code § 1798.120; Nev. SB 220, § 2 (2019); Minn. Stat. § 325M.04(2); *see also* FTC, *Protecting Consumer Privacy in an Era of Rapid Change* 58-60 (Mar. 2012), https://bit.ly/2HodYI1. Other state privacy laws recognize that de-identified and aggregated data do not implicate privacy concerns and thus restrict only individually identifiable information. *See*, *e.g.*, Cal. Civ. Code § 1798.140(*o*), *as amended by* AB 874 (Oct. 11, 2019); Nev. Rev. Stat. § 603A.320; Minn. Stat. § 325M.01(5). Finally, other privacy laws do not preclude businesses from offering discounts or other incentives in exchange for customer consent. *See* Cal. Civ. Code §§ 1798.120, 1798.125; Minn. Stat. § 325M.02; Nev. Rev. Stat. § 205.498; Nev. SB 220, §§ 1.6, 2 (2019).

LEGAL STANDARD

"After the pleadings are closed — but early enough not to delay trial — a party may move for judgment on the pleadings." Fed. R. Civ. P. 12(c). The Court is to apply to "the pleadings as a whole" substantially the same standard it applies to a complaint when considering a motion to dismiss for failure to state a claim: the Court should grant the motion "if the uncontested and

properly considered facts conclusively establish the movant's entitlement to a favorable judgment." *Aponte-Torres v. Univ. of Puerto Rico*, 445 F.3d 50, 54-55 (1st Cir. 2006); *see also Curran v. Cousins*, 509 F.3d 36, 43 (1st Cir. 2007) (affirming disposition of constitutional claims on cross-motions for judgment on the pleadings).

ARGUMENT

This case is not about whether consumers' privacy should be protected. Plaintiffs' members are committed to protecting consumers' personal information under the same FTC-enforced consumer privacy standards that apply to all other companies. Rather, this case is about whether Maine's outlier ISP-only privacy regime — which disturbs those evenly applied federal standards — contravenes constitutional limits on Maine's regulatory authority. It does, for multiple reasons.

First, the Statute violates the First Amendment. It excessively burdens ISPs' beneficial, pro-consumer speech about a wide variety of subjects, with no offsetting privacy-protection benefits. It also restricts the speech of ISPs — and only ISPs — without regulating the many other businesses (online and offline) that have and use the same or even more customer information, thereby further preventing the Statute from advancing its stated purpose. For both reasons, the Statute unconstitutionally restricts ISPs' speech, whether this Court applies strict or intermediate scrutiny. *Second*, the Statute's restrictions are so vague that they unconstitutionally chill protected speech. *Third*, the Statute conflicts with federal law and policy goals in multiple respects and is therefore preempted. It conflicts with Congress's rejection of an ISP-specific regime, the FCC's rejection of proscriptive restrictions in favor of a disclosure standard plus uniform FTC enforcement, and federal law requiring certain data disclosures.

These conclusions follow inexorably from the statutory language and the undisputed facts. *See generally* Answer, ECF No. 23. The Court should therefore enter judgment on the

pleadings and declare that the Statute is unconstitutional, barring Defendant from enforcing it. *See, e.g., Fantasy Book Shop, Inc. v. City of Boston*, 652 F.2d 1115, 1126 (1st Cir. 1981) (recognizing, in a First Amendment case, that, "in a suit challenging the constitutionality of an act," declaratory relief "offers an alternative remedy" to an injunction and "does not require a showing" of the same elements as an injunction); *McLaughlin v. City of Lowell*, 140 F. Supp. 3d 177, 197 n.16 (D. Mass. 2015) (declaratory judgment in First Amendment case appropriate alternative to permanent injunctive relief); *see also Doran v. Salem Inn, Inc.*, 422 U.S. 922, 931 (1975) ("At the conclusion of a successful federal challenge to a state statute or local ordinance, a district court can generally protect the interests of a federal plaintiff by entering a declaratory judgment, and therefore the stronger injunctive medicine will be unnecessary.").

I. The Statute Violates the First Amendment (Count One)

ISPs use consumer information to communicate with their customers, to market and advertise their products, and to facilitate geographically targeted public service announcements. *See* Compl. ¶¶ 23-25. These communications are "speech within the meaning of the First Amendment." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011); *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, Inc. v. FCC*, 182 F.3d 1224, 1232 (10th Cir. 1999) (prohibition on "using [customer information] to target customers" restricts speech). And because this speech "is protected under the First Amendment," ISPs "are entitled to engage in" that speech "without unduly burdensome interference by the government." *Nat'l Fire Adjustment Co. v. Cioppa*, 357 F. Supp. 3d 38, 43 (D. Me. 2019). Yet the Statute burdens ISPs' protected speech — both commercial (*e.g.*, advertisements) and non-commercial (*e.g.*, public service announcements), *see* Compl. ¶ 60 — in ways that violate the First Amendment, whether this Court subjects the Statute to strict or intermediate scrutiny.

A. The Statute Is Subject to and Fails Strict Scrutiny

Two features of the Statute subject it to strict scrutiny. *First*, its restrictions are speaker based: the Statute "has the effect of preventing [ISPs] — and only [ISPs] — from communicating . . . in an effective and informative manner." *Sorrell*, 564 U.S. at 564; *see also Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 828 (1995) ("[G]overnment regulation may not favor one speaker over another."). The Statute makes no attempt to regulate edge providers, data brokers, or offline companies. *See* Me. Rev. Stat. tit. 35-A, § 9301(1)(A). No "special characteristics" of ISPs justify that distinction. *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 661 (1994). In fact, recent technological developments give edge providers and software developers equal or greater access to consumers' personal information. *See* Compl. ¶¶ 26-28. As a result, it is those companies — not ISPs — that are the dominant players in the marketplace of targeted advertising. *See id.* ¶ 29. And it is those companies, along with brick-and-mortar companies conducting business online and offline, that have been the overwhelming focus of FTC enforcement actions. *See id.* ¶ 30. Consistent with these technological realities, a survey of Internet users found that more than 94 percent of respondents agreed that "[a]ll companies collecting data online should follow the same consumer privacy rules."[5]

Second, the Statute's restrictions are content based: they attempt to "defin[e] regulated speech by particular subject matter." *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2227 (2015). 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

[5] Progressive Policy Inst., *PPI Poll: Recent National Survey of Internet Users* 2 (May 26, 2016), https://bit.ly/3bGusth; *see* Internet Innovation Alliance, *Consumer Data Privacy Concerns* (July 2019), https://bit.ly/3bmV1SW.

non-communications-related services to the same customer. Similarly, the Statute permits the use of geolocation information for certain emergency calls, but prohibits use of that same information for geographically specific public service announcements in closely related situations. *Id.* § 9301(4)(F). These facially content-based restrictions trigger strict scrutiny "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.

Because the Statute's speech restrictions are facially speaker and content based, they are "presumptively violative of expressive rights and will stand only where the regulation is narrowly tailored to serve a compelling state interest." *Cioppa*, 357 F. Supp. 3d at 44; *see also Reed*, 135 S. Ct. at 2231. Here, the Statute cannot satisfy that standard because, as discussed below, it fails even to satisfy the less rigorous test applicable to commercial speech restrictions.[6]

B. In Any Event, the Statute Fails Intermediate Scrutiny

Even if the Statute were subject to intermediate scrutiny, Maine must establish that the Statute "directly advances" a "substantial" government interest and "is not more extensive than is necessary to serve that interest." *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 566 (1980). Maine cannot do so for multiple independent reasons.

First, although consumer privacy is a "highly significant value[ ]" "in the abstract," Maine has not shown — and cannot show — that it has a substantial interest in regulating the specific "*aspect*" of privacy at issue "*in the circumstances of this case*." *Cal. Democratic Party*

[6] The Statute restricts not only commercial speech — communications that do "no more than propose a commercial transaction," *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 762 (1976) (citation omitted) — 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. Because the Statute fails intermediate scrutiny, Plaintiffs are entitled to judgment regardless of whether the Statute is limited to commercial speech.

v. Jones, 530 U.S. 567, 584 (2000). Maine cannot satisfy its burden "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) (emphases added).

Yet Maine made no attempt to show that ISPs' practices have harmed consumer privacy. The Legislature made *no* findings at all. The Legislature did not find that ISPs threaten privacy "harms" that "are real" or unique relative to edge providers, data brokers, and other businesses with equal or greater access to customers' information. *Id.* It did not find that an ISP-specific opt-in regime applicable to substantial amounts of non-sensitive information "will in fact alleviate" any such unique harm "to a material degree." *Id.* Nor did it find that the Statute's ISP-specific rules are necessary in light of existing, technology-neutral federal privacy standards. Without any legislative record evidence, Maine's unwarranted and discriminatory restrictions on ISPs' speech cannot stand. *See 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.").

Second, the Statute's restrictions are "more extensive than is necessary to serve" privacy interests because they restrict "speech that poses no danger" to privacy. *Cent. Hudson*, 447 U.S. at 565-66. For example, the Statute limits the use of information that Maine itself recognizes "is *not* customer personal information." Me. Rev. Stat. tit. 35-A, § 9301(3)(C) (emphasis added). It also restricts the use of de-identified or aggregated information, which Congress, the FCC, and other States have recognized should be exempted from privacy regulation. *See* 47 U.S.C. § 222(c)(3); 47 C.F.R. § 64.2002(m); Cal. Civ. Code § 1798.120. "[T]he range of communications restricted" by the Statute is therefore "unduly broad." *Lorillard Tobacco Co. v. Reilly*, 533 U.S.

525, 563 (2001); *see also Sorrell*, 564 U.S. at 574 ("Rules that burden protected expression may not be sustained when the options provided by the State are too narrow to advance legitimate interests or too broad to protect speech.").

Further, the Statute's imposition of an opt-in regime even for non-sensitive information ignores an obvious and available "narrower restriction[]" — an opt-out regime. *Cent. Hudson*, 447 U.S. at 565. The Statute's opt-in regime extends to information that often is publicly available (such as a customer's billing address), as well as *all* "[i]nformation from a customer's use of broadband Internet access service" irrespective of its sensitivity (such as a customer's IP address). Me. Rev. Stat. tit. 35-A, § 9301(1)(C)(2). As federal courts, the FCC, the FTC, and even several other States with their own consumer privacy laws have recognized,[7] subjecting that broad category of information to opt-in, rather than opt-out, consent is unnecessary to achieve any legitimate privacy goal. *See U.S. West*, 182 F.3d at 1238-39.

In that respect, the Statute is similar to the regime held unconstitutional in *U.S. West*. There, the Tenth Circuit struck down an FCC opt-in regime for telephone companies' use of customers' information, recognizing that an opt-out rule would protect privacy interests without unduly restricting harmless uses of "customer personal information" to facilitate routine business practices, including targeted marketing. *See id.* As the Tenth Circuit explained, "mere[] speculat[ion] that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so," "hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires." *Id.* at 1239.

[7] *See, e.g.*, Cal. Civ. Code § 1798.120; Nev. SB 220, § 2 (2019); Minn. Stat. § 325M.04(2).

Similarly, the FCC found in its *ISP Privacy Order* that, for most information, an opt-in regime burdened speech more than necessary to protect consumer privacy because "customers expect their providers to use their non-sensitive information to market improved services, lower-priced service offerings, promotional discounts for new services, and other offers of value." *ISP Privacy Order* ¶¶ 383, 385-386. Because Maine "did not try — or adequately explain why it did not try — [this] other, less speech restrictive means of addressing the [privacy] concerns it identified," the Statute fails intermediate scrutiny. *Cutting v. City of Portland*, 802 F.3d 79, 91 (1st Cir. 2015).

Third, the Statute is riddled with irrational distinctions that undermine its ostensible purpose of protecting consumer privacy. It applies only to ISPs, even though myriad other businesses collect, use, and sell consumer information to an equal and often greater extent. Any privacy risks thus "flow in equal measure from" these "other businesses, which nonetheless are left untouched by" the Statute. *Showtime Entm't, LLC v. Town of Mendon*, 769 F.3d 61, 73 (1st Cir. 2014). Moreover, the Statute allows ISPs to use customer information for communications about certain kinds of services, but not others, and it permits ISPs to provide consumers' geolocation information in certain types of emergency situations, but not others. Because the Statute is "so pierced by" these "exemptions and inconsistencies," it cannot coherently protect Maine's asserted privacy interest and therefore cannot be squared with the First Amendment. *Greater New Orleans Broad. Ass'n, Inc. v. United States*, 527 U.S. 173, 190 (1999) (invalidating a law restricting "advertising about privately operated commercial casino gambling" but not "for tribal casino gambling"); *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 488 (1995) (invalidating law that 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).

II. The Statute Is Void for Vagueness (Count Two)

The Statute also violates the Constitution for the independent reason that the outer limits of its restrictions on ISPs' speech "are not clearly defined," rendering it "void for vagueness." *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972) (vagueness doctrine applies to speech restrictions that "are not clearly defined"); *Wis. Right To Life, Inc. v. Barland*, 751 F.3d 804, 835 (7th Cir. 2014) (striking down vague speech restriction and recognizing that "[v]ague or overbroad speech regulations carry an unacceptable risk that speakers will self-censor, so the First Amendment requires more vigorous judicial scrutiny").

Vagueness pervades the Statute's provisions. The Statute's burdensome opt-in restriction, for example, applies to "[p]ersonally identifying information." Me. Rev. Stat. tit. 35-A, § 9301(1)(C)(1). But the Statute defines that term 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). *Id.* Because "[p]ersonally identifying information" is further defined to "includ[e] but not [be] limited to" (Me. Rev. Stat. tit. 35-A, § 9301(1)(C)(1)) this "confusing list of examples," the Statute is unlawfully vague. *Johnson v. United States*, 135 S. Ct. 2551, 2561 (2015). It leaves persons of "average intelligence . . . to guess" about the scope of its opt-in restriction, chilling lawful speech. *Nat'l Org. for Marriage v. McKee*, 649 F.3d 35, 65 (1st Cir. 2011).

The Statute also does not define *at all* the category of information subject to its opt-out requirement: information that "pertain[s] to a customer" but "that is not customer personal information." Me. Rev. Stat. tit. 35-A, § 9301(3)(C). ISPs are therefore left to guess when

information outside the Statute's vague and broad definition of "customer personal information" nonetheless "pertain[s] to a customer" and requires opt-out consent. *Id.* That the Statute so vaguely draws the line it uses to identify the speech (if any) that is unregulated by the Statute "raises special First Amendment concerns," which the Statute nowhere remedies. *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 254-55 (2012) (citation omitted).

Equally unclear is the Statute's geographic scope. 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, for example, whether the Statute extends to non-Maine residents who use their mobile broadband Internet services during the time they visit Maine, *Coates v. City of Cincinnati*, 402 U.S. 611, 614 (1971).

These ambiguities deprive Plaintiffs' members of "fair warning" as to what the Statute prohibits and what it permits, thereby "chilling the exercise of [their] First Amendment rights" as they develop their products and services while attempting to comply with the Statute. *Nat'l Org. for Marriage*, 649 F.3d at 62. As the Supreme Court has recognized, "[u]ncertain meanings inevitably lead" affected speakers "to steer far wider of the unlawful zone than if the boundaries of the forbidden areas were clearly marked." *Grayned*, 408 U.S. at 109 (alteration and citation omitted). Because this intrusion "upon sensitive areas of basic First Amendment freedoms" will chill and deter protected speech, the Statute is unconstitutional. *Id.* (citation omitted).

III. Federal Law Preempts the Statute

A. The Statute Conflicts with Congress's Vacatur of the FCC's *ISP Privacy Order* (Count Three)

In 2017, Congress passed and the President signed a Joint Resolution vacating the *ISP Privacy Order* pursuant to the Congressional Review Act. *See* Joint Resolution, Pub. L. No.

115-22, 131 Stat. 88 (2017).[8] As a result, the *ISP Privacy Order* did "not take effect," and federal agencies may not adopt "substantially the same" rule without express congressional authorization. 5 U.S.C. § 801(b). Congress vacated the *ISP Privacy Order* because it targeted ISPs and only ISPs, thereby harming the public interest by causing consumer confusion, undermining federal broadband policy, and interfering with the uniform enforcement of consumer privacy standards by the FTC. *See supra* pp. 4-5.

Maine Legislators made no secret that the Statute was designed to "frustrate the purposes of the federal scheme" by undoing Congress's judgment that an ISP-specific privacy regime is not in the public interest. *SPGGC, LLC v. Ayotte*, 488 F.3d 525, 530-31 (1st Cir. 2007); *see* L.D. 946 Hearing (testimony of Sen. Guerin) (noting purpose to "fill the gap created by Congress"). And the Statute imposes ISP-specific restrictions even more onerous than those Congress vacated. For example, the Statute adopts a blanket opt-in requirement for *all* customer personal information, without regard to its sensitivity, while the *ISP Privacy Order* had at least limited the requirement of opt-in consent to "sensitive" personal information. 47 C.F.R. § 64.2004.

The Joint Resolution vacating the *ISP Privacy Order* also prohibited adoption of a "substantially" similar federal rule without express congressional authorization. 5 U.S.C. § 801(b)(1). That applies *a fortiori* to preempt, as a matter of conflict preemption, ISP-only state laws that similarly "frustrate the purposes of the federal scheme," including the Statute. *SPGGC*, 488 F.3d at 530-31; *cf. Arizona v. United States*, 567 U.S. 387, 406 (2012) (finding conflict preempted state laws contrary to the "instruction . . . draw[n] from the text, structure, and history of" a statute).

[8] Like any other enactment passed through the bicameralism and presentment process, the Joint Resolution is a federal law, *see Nuclear Energy Inst., Inc. v. EPA*, 373 F.3d 1251, 1309 (D.C. Cir. 2004) (per curiam), and therefore carries the full force and effect of the Supremacy Clause.

B. The Statute Conflicts with the *RIF Order* (Count Four)

The FCC has determined that the best way to balance consumer privacy interests and the promotion of broadband innovation, competition, and deployment is to pair mandatory privacy disclosures, *see RIF Order* ¶ 223, with FTC enforcement of ISPs' compliance with those disclosures, *id.* ¶ 244 — not to mandate ISP-specific restrictions on the use of consumer data. That assessment carries the full preemptive force of federal law. *See Ark. Elec. Co-op. Corp. v. Ark. Pub. Serv. Comm'n*, 461 U.S. 375, 384 (1983) (agency "decision to forgo regulation" carries "as much pre-emptive force as a decision *to* regulate"); *see also City of New York v. FCC*, 486 U.S. 57, 64 (1988) (statutorily authorized regulations preempt contrary state law).[9]

The Statute's burdensome ISP-specific regime thus conflicts with the FCC's determination that requiring transparency around ISPs' privacy practices — combined with uniform enforcement by the FTC — best achieves the purposes of the Communications Act and "avoid[s] tilting the playing field against ISPs and causing economic distortions" in the marketplace. *RIF Order* ¶ 140. Because the Statute stands as an obstacle to the achievement of that federal determination, it is preempted. *See, e.g., Geier v. Am. Honda Motor Co.*, 529 U.S. 861, 883-84 (2000) (federal agency determination that statutory objectives were best achieved through a balance of regulation preempted state law that struck a different balance).

C. The Statute Makes Compliance with Federal Disclosure Rules Impossible (Count Five)

Federal law mandates that ISPs disclose certain customer information. For example, FCC Form 477 requires ISPs to report "the total number of connections in each census tract [*e.g.*,

[9] Nothing in *Mozilla Corp.* is to the contrary. The D.C. Circuit vacated only "the portion of the [*RIF Order*] that expressly preempts" "a broader array of state and local laws than traditional conflict preemption principles would allow," 940 F.3d at 74; it thrice declined "to make a conflict-preemption assessment," *id.* at 82; *accord id.* at 85-86, leaving open whether any specific state law impermissibly conflicts with the *RIF Order*.

subdivision of a county] in which they provide service." Report and Order and Second Further Notice of Proposed Rulemaking, *Establishing the Digital Opportunity Data Collection; Modernizing the FCC Form 477 Data Program*, 34 FCC Rcd 7505, ¶ 7 (2019). ISPs cannot do so without using customer "billing address[es]," Me. Rev. Stat. tit. 35-A, § 9301(1)(C)(1), 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 customer opts out. *Id.* § 9301(3)(A), (C). And, while the Statute provides an exception for compliance with specifically enumerated federal laws, *see id.* § 9301(2), it makes no exception for compliance with mandatory Form 477 reporting requirements.

Similarly, the Statute permits ISPs to use or disclose information to "comply with a lawful court order," *id.* § 9301(4)(C), but it makes no exception for mandatory disclosures pursuant to civil discovery, *see* Fed. R. Civ. P. 26(a). 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 and thus renders "compliance with both" state and the foregoing federal laws "impossible," the Statute violates the Supremacy Clause. *Algonquin Gas Transmission, LLC v. Weymouth*, 919 F.3d 54, 63 (1st Cir. 2019) (citation omitted).

CONCLUSION

For the foregoing reasons, the Court should grant judgment on the pleadings in Plaintiffs' favor and declare the Statute unconstitutional, thereby barring Defendant from enforcing it.

Dated: April 6, 2020

Respectfully submitted,

By /s/ Joshua A. Randlett

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

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

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, P.L.L.C.
1615 M Street, N.W., 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., N.W.
Washington, D.C. 20037
Email: jlamken@mololamken.com

Attorney for Plaintiff
ACA Connects – America's Communications Association

* admitted *pro hac vice*

CERTIFICATE OF SERVICE

I hereby certify that, on this date, I electronically filed the foregoing document entitled *Plaintiffs' Motion for Judgment on the Pleadings with Incorporated Memorandum of Law* via the Court's CM/ECF system, which will serve a copy of same upon all counsel of record.

Dated: April 6, 2020

/s/ Joshua A. Randlett
Joshua A. Randlett, Esq.