UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF MAINE

ACA CONNECTS – AMERICA'S COMMUNICATIONS ASSOCIATION, *et al.*, Plaintiffs, v. AARON M. FREY, in his Official Capacity as the Attorney General of the State of Maine, Defendant.	CIVIL ACTION NO.: 1:20-cv-00055-LEW

DEFENDANT'S OPPOSITION TO PLAINTIFFS' MOTION FOR JUDGMENT ON THE PLEADINGS

Defendant Aaron M. Frey submits this Opposition to Plaintiffs' Motion for Judgment on the Pleadings (ECF No. 25). Based on the few uncontested facts in Plaintiffs' Complaint, it would be premature—and misguided—for the Court to grant judgment to Plaintiffs.[1]

I. Maine's Privacy Law Passes First Amendment Scrutiny (Count I)

As Plaintiffs' Motion concedes, a court must decide a motion for judgment on the pleadings based only upon "*uncontested* and properly considered facts" (Mot. 8-9 (quoting *Aponte-Torres v. Univ of Puerto Rico*, 445 F.3d 50, 54-55 (1st Cir. 2006) (emphasis added)). Yet Plaintiffs' case for judgment on their First Amendment claims hinges upon allegations in the Complaint that Defendant denied in his Answer.[2] Plaintiff's argument is rooted, for example, in representations

[1] Defendant will forgo a summary of Plaintiffs' Complaint and Defendant's Answer—the only operative documents here—because those documents speak for themselves.

[2] While the Court's consideration of Plaintiffs' Motion is properly limited to the uncontested allegations in Plaintiffs' Complaint, Defendant has simultaneously filed a declaration from Dr. Jonathan R. Mayer—an academic in the field of data privacy—to underscore why the denials in Defendant's Answer were made in good faith (*see* ECF No. 29). The declaration also previews the issues that Defendant would explore in discovery, including the unique role of ISPs, the data ISPs can access, and the privacy interests at stake.

regarding how ISPs use consumer data, and assertions regarding so-called edge providers and their role "in the marketplace of targeted advertising" (Mot. 10-11), despite Defendant's corresponding denials (*compare* Compl. ¶¶ 23-29 *with* Answer ¶¶ 23-29). Plaintiffs even cite their conclusory contention—which Defendant also self-evidently denied—that Maine's Privacy Law (the "Law") burdens ISPs' protected speech (Mot. 10; *compare* Compl. ¶ 60 *with* Answer ¶ 60). These deficiencies alone are reason for the case to proceed to discovery.

That said, procedural defects aside, the merits of Plaintiffs' First Amendment likewise do not warrant judgment on the pleadings.

A. The Law Is, At Most, a Regulation on Commercial Speech that Satisfies the *Central Hudson* Standard

The Law—assuming it implicates the First Amendment at all—should at most be subject to intermediate scrutiny as a regulation of commercial speech, i.e., "expression related solely to the economic interests of the speaker and its audience." *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 561 (1980). As discovery will illustrate, ISPs gain access to customer information through the commercial transactions that define their businesses, and ISPs' use and disclosure of that information is, insofar as regulated by the Law, likewise distinctly commercial in nature. *See* Decl. of Dr. Jonathan R. Mayer ("Mayer Decl."), ECF No. 29 ¶¶ 6-7. The *Central Hudson* standard should accordingly guide the Court's consideration of Plaintiff's First Amendment claim. *See Friedman v. Rogers*, 440 U.S. 1, 10 n.9 (1979) ("By definition, commercial speech is linked inextricably to commercial activity...."); *c.f. Pharm. Care Mgm't Ass'n v. Rowe*, 429 F.3d 294, 309-310 (1st Cir. 2005) (per curiam) (applying commercial speech standard to provisions that were "on their face less related to 'economic interests'").

The First Amendment accords comparatively less protection to commercial speech than traditional protected speech. *See Central Hudson*, 447 U.S. at 561. Under *Central Hudson*,

regulation of commercial speech comports with the First Amendment so long as the government's interest is "substantial;" the regulation "'directly advances the governmental interest;'" and the restriction is "'not more extensive than is necessary to serve that interest.'" *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 554 (2001) (quoting *Central Hudson*, 447 U.S. at 566). Maine's sensible restrictions on the use and disclosure of customer personal information easily satisfy this standard.

1. The Law directly advances Maine's substantial interest in protecting consumer privacy.

When reviewing the constitutionality of a statute under the First Amendment, "courts must accord substantial deference to the predictive judgments" of the legislative branch. *Turner Broad. Sys. v. FCC*, 520 U.S. 180, 195 (1997) ("*Turner II*"); *see also Columbia Broad. Sys., Inc. v. Dem. Nat'l Cmte.*, 412 U.S. 94, 103 (1973) ("The judgment of the Legislative Branch cannot be ignored or undervalued simply because one [party] casts its claims under the umbrella of the First Amendment."). Accordingly, to pass constitutional muster, Defendant need only demonstrate that the Maine Legislature, "in formulating its judgments, … has drawn reasonable inferences based on substantial evidence." *Turner Broad. Sys. v. FCC*, 512 U.S. 622, 666 (1994) ("*Turner I*").

Maine's Law is guided by the urgent need to safeguard the privacy of Internet consumers. *See, e.g.*, Legis. Rec. H-699 (2019) (Rep. Grohoski) ("[T]he stakes for establishing internet consumer privacy could not be higher than they are at this moment …."); *An Act to Protect the Privacy of Online Customer Information: Hearing on L.D. 946 Before the J. Standing Comm. on Energy, Utils. & Tech.*, 129th Legis. ("Committee Hearing") (2019) (testimony of Sen. Stacey Guerin) ("Guerin Test.") (expressing concern about ISP "access to some of our most personal information" which "could paint an intimate picture of a person[]"). This is far from a novel aim; the Supreme Court recognized a decade ago that privacy in the digital age is "integral to the person" and "essential to freedom," *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 580 (2011). There

thus can be no question, even absent discovery, that promoting privacy through reasonable regulation serves a "substantial" state interest, particularly given the lack of corresponding federal protections. *See, e.g., Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 766 (1976) (concluding that maintaining professional standards for pharmacists constitutes a substantial state interest); *Central Hudson*, 447 U.S. at 568-569 (same; conserving energy and promoting fair and efficient energy rates); *Rubin v. Coors Brewing Co.*, 514 U.S. 476, 485 (1995) (same; preventing alcohol "strength wars"); *see also* Mayer Decl. ¶ 17.

The Law advances this privacy interest in a straightforward manner, too. By requiring consent, the Law returns control to customers over whether and when their personal information is used and disclosed. *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 31 FCC Rcd 13911 (2016) ¶ 166 ("2016 Privacy Order") ("Respecting the choice of the individual is central to any privacy regime …."). That reasoning is apparent in both the legislative record, *see, e.g.*, Legis. Rec. H-699 (Rep. Grohoski) (describing how the Law protects consumers from "increasingly dangerous levels of unregulated corporate and government surveillance"), and the mountain of research that buttressed the FCC's 2016 Privacy Order, the inspiration for the Law, *see, e.g.*, Guerin Test. (describing bill as "fill[ing] the gap created by Congress" when it reversed the 2016 Privacy Order); *see also* Mayer Decl. ¶ 26.

2. The Law's restrictions on commercial speech are in reasonable proportion to the privacy interest they serve.

A restriction on commercial speech that advances a substantial state interest is constitutionally permissible under *Central Hudson* if it is in "reasonable proportion" to the State's substantial interest. *Edenfield v. Fane*, 507 U.S. 761, 767 (1993). The standard requires a "reasonable fit between the means and ends of the regulatory scheme"—i.e., that the statute is "narrowly tailored to achieve the desired objective." *Lorillard*, 533 U.S. at 556, 561. That fit need

not be "perfect," nor must it represent the "least restrictive means." *Bd. of Trustees of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 480 (1989).

The showing required to satisfy this standard is not extensive. Federal courts, in recognition of the large workload and limited resources of citizen legislatures, do not punish them for engaging in less exhaustive factfinding than the United States Congress. *See Gould v. Morgan*, 907 F.3d 659, 676 (2018) ("[A] court must grant the legislature flexibility to select among reasonable alternatives. It would be foolhardy—and wrong—to demand that the legislature support its policy choices with an impregnable wall of unanimous empirical studies."); *see also Fl. Bar v. Went For It, Inc.*, 515 U.S. 618, 628 (1995) ("[W]e have permitted litigants to justify speech restrictions by reference to studies and anecdotes pertaining to different locales altogether, or even … based solely on history, consensus, and simple common sense." (internal quotation marks omitted)).[3] That said, the Maine Legislature here considered a series of submissions from experts, industry advocates, and ordinary citizens, and based on that record it carefully designed the Law to advance customers' privacy interests without restricting "substantially more speech than is necessary to further the government's legitimate interests." *See Fox*, 492 U.S. at 478; *see also, e.g.*, Committee Hearing (testimony of Fletcher Kittredge, CEO of GWI) (describing Law's requirements as "not onerous" and the burden it imposes as "particularly small").

Specifically, the Law reasonably targets information procured by ISPs in their commercial relationship with customers by utilizing an opt-in provision to shield "customer personal information," and a less-restrictive opt-out provision to protect "information the provider collects pertaining to a customer that is not customer personal information." 35-A M.R.S. § 9301(3). This

[3] Nor, for that matter, is Defendant limited to the legislative record when defending the law. *See Turner II*, 520 U.S at 187 (assessing First Amendment challenge to statute based in part on tens of thousands of pages of discovery materials assembled on remand, including expert submissions, sworn declarations and testimony, and industry documents).

approach is in lockstep with the FCC's determination in its 2016 Privacy Order of how best to strike the "right balance" when "giv[ing] customers control over the use and sharing of their information." 2016 Privacy Order ¶ 174; *see also* Mayer Decl. ¶¶ 19-26. The FCC reasoned that whether an opt-in is necessary should depend on the sensitivity of the information at issue, *id.* ¶ 365, and it therefore adopted that requirement for the use and disclosure of certain customer proprietary network information ("CPNI"), including "precise geo-location, health, financial, and children's information; Social Security numbers, content; and web browsing and application usage histories and their functional equivalents," *id.* ¶¶ 167, 365. As to other customer information, the FCC mandated that ISPs, "at a minimum, offer their customers the ability to opt out of [its] … use or sharing." *Id.* ¶ 172; *see also id.* ¶ 365.[4]

The Law here sets forth a similar, non-exhaustive list of information warranting the highest level of protection. 35-A M.R.S. §§ 1(C), 2. In so doing, the Law "reasonably balances burdens between carriers and their consumers" because "opt-out consent would be insufficient." 2016 Privacy Order ¶¶ 193-94. Further, while the Maine Legislature—like the FCC—concluded that other customer information derived from the ISP-customer relationship still warrants at least some protection, the necessity of which discovery will make clear, it determined that opt-out protection for that information was sufficient. *See id.* ¶¶ 198-200, 365. The Law thus regulates ISPs in a manner "not more extensive than is necessary" to advance its substantial privacy interests. *See Central Hudson*, 447 U.S. at 566; *cf. Lorillard*, 533 U.S. at 563 (recognizing that tailoring sometimes requires avoiding a "uniformly broad" sweep).

[4] *See also Implementation of the Telecommunications Act of 1996*: *Telecommunications Carriers' Use of Customer Proprietary Information and Other Customer Information*, 17 FCC Rcd 14860 (2002) ¶ 2 (adopting both opt-in and opt-out requirements).

Given these reasoned judgments, the administrative regulation at issue in *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), is an inapt comparator (*see* Mot. 14). First, as noted above, legislative conclusions are held to "a standard more deferential" than those of administrative agencies, the latter of which were at issue in *U.S. West*. *Turner II*, 520 U.S. at 195. Second, the *U.S. West* court noted that it was "difficult, if not impossible" to "conduct a full and proper narrow tailoring analysis" because there—unlike here—the regulation failed the "substantial interest" prong of the *Central Hudson* test. 182 F.3d at 1238. Third and finally, the Tenth Circuit faulted the FCC for failing to consider the possibility of using an opt-out regime, *id.* at 1238-39, whereas here, the Maine Legislature clearly studied the issue and decided, as the FCC did, that while an opt-in regime was necessary to protect consumer privacy in some circumstances, an opt-out regime would suffice in others.

Plaintiffs' contention that the Law sports "irrational distinctions" likewise rings hollow (Mot. 15). As explained below, the Maine Legislature chose to regulate ISPs because of the unique gatekeeping role they play. Further, Plaintiffs have failed to demonstrate how the Statute's narrow exceptions are illogical—they have not, for example, offered any support for their assertion that the statute permits the use of geolocation information in "certain types of emergency situations, but not others" (Mot. 15). Accordingly, the uncontested facts suggest only that the Law stands in "reasonable proportion" to Maine citizens' privacy interests. *Edenfield*, 507 U.S. at 767.

B. The Law Survives a Traditional First Amendment Analysis

Even if the Court disagrees with Defendant and concludes that the Law regulates non-commercial speech, it survives under traditional First Amendment review.

1. The Law is Subject to Intermediate Scrutiny as a Content-Neutral Regulation

Maine's Privacy Law is subject to intermediate scrutiny because it contains no impermissible speaker- or content-based distinctions. With respect to the former, while Plaintiffs contend that the Law unfairly regulates ISPs but not "edge providers" and other companies (*see* Mot. 11), discovery will demonstrate that ISPs occupy a distinct position in Internet commerce (*see* Mayer Decl. ¶¶ 18, 31-32). They "sit[] at a privileged place in the network, the bottleneck between the customer and the rest of the network …," 2016 Privacy Order ¶ 6, a unique vantage point to view the entirety of a customer's internet traffic in the context of that customer's real name, address, phone number, and billing history, *see, e.g.*, Legis. Rec. H-698 (Rep. Riley) (2019) ("We found out during the testimony on this that there were actual cases of ISPs giving real-time information to bounty hunters …."). Indeed, unlike their relationship with edge providers, customers *must* engage with an ISP *every time* they use the Internet. *See* Legis. Rec. H-699 (Rep. Grohoski) ("[Y]ou can choose not to use Google, Facebook, or other edge providers, … but in most places in Maine you cannot choose your ISP because there is only one provider."); Committee Hearing (testimony of Sen. Bellows) (describing ISPs as the "on-ramp to everything you do online and "conduit through which all information flows from you and to you."). ISPs accordingly sport precisely the sort of "'special characteristic[]" that warrants special regulation under *Turner I*, 512 U.S. at 660-61. *Cf.* 2016 Privacy Order ¶ 389 ("Were we to interpret *Sorrell* to [bar] sector-specific privacy laws … simply because they do not apply to all entities equally, it would stand to invalidate nearly every federal privacy law considering the sectoral nature of our federal privacy statutes.").

In this vein, Plaintiff's reliance on *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), is misplaced (*see* Mot. 11). The *Sorrell* Court faulted Vermont for banning pharmacies from selling prescriber information to only *some* third-party purchasers (pharmaceutical detailers), while not

restricting other potential third-party recipients (e.g. academic institutions) from procuring that same information. *Sorrell*, 564 at 564. Here, ISPs stand in the same position as the *Sorrell* pharmacies, but unlike in *Sorrell*, the Maine Legislature prohibits disclosure of information to *any* third parties, regardless of their identity or the purpose of the disclosure.

As to content-based restriction, the Law draws no distinctions based on message, recipient, or purpose. It contains only a narrow set of exceptions that ensures ISPs are still able to provide services; address emergencies; and comply with applicable law, *see* 35-A M.R.S. § 9301(4). Those exceptions are accordingly indicative of the Law's careful tailoring, rather than instances of impermissible content-based regulation. *See* 2016 Privacy Order ¶ 389 ("The fact that …our rules … apply to certain types of information and certain providers is a function of their tailoring, not indications that they are content-based.").[5] Indeed, this is not a case like *Sorrell*, wherein the Court rebuked Vermont for regulating prescriber information in a manner that favored one type of speech (academic research) to the detriment of another (marketing). 564 U.S. at 563-64. The Law's reasonable, limited exceptions do not render it content-based, but rather ensure the practical workability of the Law's content-neutral provisions.

2. The Law Survives Intermediate Scrutiny

"Content-neutral restrictions are subject to intermediate scrutiny, which demands that the law be 'narrowly tailored to serve a significant governmental interest.'" *Rideout v. Gardner*, 838 F.3d 65, 71-72 (1st Cir. 2016) (quoting *Ward v. Rock against Racism*, 491 U.S. 781, 791 (1989)). They "'need not be the least restrictive or least instructive means of' serving the government's interests." *Id.* at 72 (quoting *McCullen v. Coakley*, 573 U.S. 464, 486 (2014)).

[5] As noted above, Plaintiffs' contention that Maine's Privacy law prohibits unidentified "geographically specific public service announcements" lacks sufficient substantiation (*see* Mot. 12).

A "significant government interest" in the traditional speech context is equivalent to the "substantial governmental interest" described in *Central Hudson*. *Cf. Ward*, 491 U.S at 796-97 (using "significant governmental interest" interchangeably with "substantial interest"). Likewise, a statute is "narrowly tailored" where, as here, it "promotes a substantial government interest that would be achieved less effectively absent the regulation." *Turner I*, 512 U.S. at 662.

Accordingly, for the reasons identified above in the commercial speech context, Maine's Privacy Law survives traditional intermediate scrutiny analysis. The Maine Legislature's strong interest in protecting consumer privacy is sufficient to pass constitutional muster, and the Law strikes a permissible balance between competing interests by granting customers the ultimate authority to determine how their information is used outside the context of their economic transactions with ISPs. The Law relies on consent rather than an outright ban on speech to avoid infringing upon any "protected interest" in communication between ISPs and willing customers, *see Lorillard*, 533 U.S. at 564, and it places all potential third-party recipients of customer information on the same playing field to avert the "contrived choice" Vermont thrust upon doctors in *Sorrell*. 564 U.S. at 574.

3. Discovery will demonstrate that the Law would pass even strict scrutiny.

Plaintiffs' Motion fails to identify any content-specific restrictions on speech in the Law. Nevertheless, discovery will show that even under the strictest scrutiny, the Maine Legislature identified a "compelling state interest" in customer privacy and used the "least restrictive or least intrusive means" to advance that interest. *Rideout*, 838 F.3d at 71-72. Accordingly, if the Court believes there is any possibility that strict scrutiny should apply, Defendant should be permitted to engage in discovery to develop the record and illustrate the Law's necessity, the same necessity recognized by the FCC in 2016. *See* 2016 Privacy Order ¶¶ 1-3.

II. Plaintiffs' Facial Vagueness Claim is Meritless (Count II)

Plaintiffs' scattershot vagueness challenge is primarily an allegation of overbreadth. But the Supreme Court "has repeatedly warned that 'invalidation for First Amendment overbreadth is strong medicine that is not to be casually employed.'" *United States v. Sineneng-Smith*, 140 S.Ct. 1575, 1581 (2020) (quoting *United States v. Williams*, 553 U.S. 285, 293 (2008)). To overcome the "traditional rule" that litigants "may not challenge [a] statute on the ground that it may conceivably be applied unconstitutionally to others in situations not before the Court," *Los Angeles Police Dept. v. United Reporting Publ'g Corp.*, 528 U.S. 32, 38 (1999), facial vagueness challenges—whether alleging overbreadth or otherwise—must demonstrate a substantial risk of concrete harm, *National Endowment for Arts v. Finley*, 524 U.S. 569, 580 (1998); *see also Savage v. Gee*, 665 F.3d 732, 740 (6th Cir. 2012) ("While the doctrines of overbreadth and vagueness provide an exception to the traditional rules … '[a]llegations of a subjective chill are not an adequate substitute for a claim of specific present object harm or a threat of specific future harm.'" (quoting *Laird v. Tatum*, 408 U.S. 1, 13-14 (1972)).

Here, Plaintiffs have failed to justify the Court's consideration of whether the Law is unconstitutionally vague on its face. They have made no showing of harm beyond asserting, without substantiation, that there will be a chilling effect of unspecified substance and scope. This deficiency alone is sufficient to deny Plaintiffs judgment on their facial vagueness challenge. *See Los Angeles Police Dep't.*, 528 U.S. at 40-41 (dismissing claims that did "not fit within the case law allowing courts to entertain facial challenges").

That said, even if the Court were to reach vagueness, the Law is not constitutionally infirm because it provides to ISPs the "fair warning" that Due Process demands. *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). The ever-changing nature of the broadband ecosystem renders

precise statutory regulation particularly difficult. *See, e.g.*, 2016 Privacy Order ¶ 109 ("[A] list of identifiers that must be removed from data … would … rapidly become obsolete in the evolving broadband context."). The Supreme Court's recognition that "perfect clarity and precise guidance have never been required even of regulations that restrict expressive activity," *Ward*, 491 U.S. at 794, therefore rings particularly true in the Internet privacy context. Indeed, the Law's flexibility is not a fault, but a necessary feature to ensure it is nimble enough to remain relevant, promote fairness, and—above all—protect customer privacy as technology evolves. *Cf. In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 287 (3d Cir. 2016) (recognizing that Congress, by permitting updates to its definition of "personal information," "built flexibility" into the Children's Online Privacy Protection Act "to keep pace with evolving technology"); 2016 Privacy Order ¶ 281 (noting "overall approach" is to "adopt rules that incorporate flexibility to account for changing circumstances").

To this end, the Law identifies categories of data warranting different levels of protection, consistent with the FCC's past regulatory approach. Both the FCC and Maine's Legislature set forth a list of customer information subject to the opt-in requirement, including customers' social security numbers, financial information, and health information; information pertaining to the customer's children; browsing history; application usage history; and communication content. *Compare* 35-A M.R.S. § 9301(1)(C) *with* 2016 Privacy Order ¶ 177. Both lists are also non-exhaustive: the FCC's opt-in requirement applied "at a minimum" to listed categories of information "and [their] functional equivalents." 2016 Privacy Order ¶ 177.[6] These similarities underscore the reasonability—and understandability—of the Law's structure and terminology.

[6] Plaintiffs cite to *Johnson v. United States*, 135 S. Ct. 2551, 2561 (2015), seeming to imply that because the Law contains an illustrative list of examples alongside a "residual clause," it must be unconstitutionally vague (Mot. 16). But *Johnson* involved a vague residual clause in a *criminal* statute, and rather than strike the statute down, the Supreme Court deemed it severable. *Id.* at 2563. If necessary, the Court could do the same here. *See* 1 M.R.S. § 71(8).

The Law's reference to "information that "pertain[s] to a customer … that is not customer personal information" also reflects the 2016 Privacy Order. *See* 35 M.R.S. § 9301(3)(C). The FCC required, "at a minimum," that ISPs permit customers to opt-out of sharing "non-sensitive customer PI," without further defining the term. 2016 Privacy Order ¶ 167. Though the Law does not utilize the same terminology, it similarly requires that customers be permitted to opt-out of the use and disclosure of information that falls outside the scope of § 9301(1)(C), but nonetheless still warrants some protection.

Plaintiffs' claim that the geographic scope of the Law is also vague is a red herring. The Law, on its face, applies to (a) ISPs operating within the State, when (b) they are providing service to customers that are physically located in the state, and physically billed for those services within the State. *See* 35 M.R.S. § 9301(7). The statute accordingly does not depend upon any "wholly subjective judgments" that would raise constitutional alarm. *Williams*, 553 U.S. at 306.

In short, vagueness can only void a statute when "its prohibitions are not clearly defined." *Grayned*, 408 U.S. at 108. Here, like the FCC's 2016 Privacy Order, the Law sufficiently describes both the information it protects, and under what circumstances that protection applies. Plaintiffs do not claim to lack any grasp of the Law's regulatory scope, and instead appear to conflate vagueness with their distaste for the Law. But disagreement with duly enacted regulations does not gain constitutional dimension simply because the regulated industry objects to their contours.

The caselaw Plaintiffs cite is no more helpful to their cause. In *Grayned*, the Supreme Court examined a far more ambiguous ordinance that prohibited "willfully mak[ing] or assist[ing] in the making of any noise or diversion which disturbs or tends to disturb the peace or good order of such school session." 408 U.S. at 107-08. The Court nevertheless upheld the ordinance, despite its lack of "meticulous specificity," because of its "flexibility and reasonable breadth." *Id.* at 110. Further,

although the Court abrogated a local ordinance in *Coates v. City of Cincinnati*, 402 U.S. 611, 615 (1971), for prohibiting "annoying" conduct, this Law contains no such broad, subjective prohibitions, and instead relies on commonly understood industry terms and practices.

If there remains any doubt, discovery will fill the gap. With a fully developed record, Defendant will demonstrate that "customer personal information" is a familiar concept in the industry; that the Law creates no unconstitutional grey area; and that ISPs will have no trouble understanding the Law's prohibitions. *See* 2016 Privacy Order ¶¶ 177-191.

III. Maine's Privacy Law Does Not Conflict with Federal Law (Counts III-V)

Consistent with bedrock federalist principles, the Supreme Court has long recognized a presumption against federal preemption of state law. *N.Y.S. Conf. of Blue Cross & Blue Shield Plans v. Travelers Ins. Co.*, 514 U.S. 645, 654 (1995); *see also Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947). That presumption is strongest "in fields of traditional state regulation," and it applies regardless of whether preemption is alleged to be explicit, implied, or a result of conflict between state and federal law. *Travelers Ins.*, 514 U.S. at 655; *see also Philip Morris v. Harshbarger*, 122 F.3d 58, 68 (1st Cir. 1997). Privacy regulation is no exception. *See, e.g., Medtronic v. Lohr*, 518 U.S. 470, 475 (1996) ("[T]he States traditionally have had great latitude under their police powers to legislate as to the protection of the lives, limbs, health, comfort, and quiet of all persons."); *Katz v. United States*, 389 U.S. 347, 350-51 (1967) ("[T]he protection of a person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States."). The Law is therefore entitled to the strongest presumption against preemption, one that can only be overcome by a "clear and manifest" preemptive purpose. *Rice*, 331 U.S. at 230; *see also Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996); *Harshbarger*, 122 F.3d at 68.

The federal government shares responsibility for protecting consumer privacy with the States. The Communications Act itself contemplated "dual federal-state authority and cooperation." *Mozilla Corp. v. FCC*, 940 F.3d 1, 81 (D.C. Cir. 2019); *see also* 47 U.S.C. § 253(b) ("Nothing in this section shall affect the ability of a State to impose … requirements necessary to … protect the public safety and welfare, … and safeguard the rights of consumers."); 2016 Privacy Order ¶ 324 (emphasizing "the important role states play in upholding the pillars of privacy and protecting consumer information"); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Information and Other Customer Information IP-Enabled Services*, 22 FCC Rcd 6927 (2007) ¶ 60 (FCC "should allow states to also create rules for protecting" customer personal information).[7] Indeed, it remains just as "imperative" today that "the states maintain broad authority for privacy regulation and enforcement," including through laws "more restrictive than those adopted by the Commission." 2016 Privacy Order ¶¶ 324, 327 (citation omitted).

Plaintiffs nonetheless maintain that Maine is preempted from protecting the privacy rights of its citizens as they use the Internet. Specifically, Plaintiffs claim that the Law conflicts with (1) Congress's reversal of the FCC's 2016 Privacy Order under the Congressional Review Act ("CRA"), *see* Joint Resolution, Pub. L. No. 115-22, 131 Stat 88 (Apr. 3, 2017); (2) a 2018 FCC Order, *see* Declaratory Ruling, Report and Order, *Restoring Internet Freedom*, FCC 17-166, 333 FCC Rcd. 311 (2018) ("RIF Order"); and (3) federal disclosure rules, namely the FCC's Form 477 and Federal Rule of Civil Procedure 26(a). Plaintiffs are mistaken: It is not impossible for ISPs to comply with both the Law and the cited federal authorities, nor does the Law "stand[] as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."

[7] Available at https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0317/DOC-343949A1.pdf.

California v. ARC Am. Corp., 490 U.S. 93, 101 (1989). The Law is accordingly not preempted. *See Geier v. Am. Honda Motor Co., Inc.*, 529 U.S. 861, 885 (2000) ("[A] court should not find pre-emption too readily in the absence of clear evidence of a conflict.").

Beginning with Congress's reversal of the FCC's 2016 Privacy Order, Defendant is unaware of any circumstance—nor have Plaintiffs cited any—where a court has found that a disapproval resolution adopted under the CRA preempts state law. This is for good reason: Preemption turns on Congressional intent asserted through statutory text, and CRA disapproval resolutions contain almost no text at all. *See* 5 U.S.C. § 802(a). Here, for example, the Joint Resolution only expressed Congress's "disapprov[al] [of] the rule submitted by the Federal Communications Commission," and provided that "such rule shall have no force or effect." 131 Stat. 88. While the Joint Resolution thus prevents the FCC from taking contrary action, any broader preemptive Congressional intent is untethered from a statutory vehicle for its expression. *Puerto Rico Dep't of Consumer Affairs v. Isla Petroleum Corp.*, 485 U.S. 495, 503 (1988) ("There is no federal pre-emption *in vacuo*, without a constitutional text or a federal statute to assert it."); *see also Kansas v. Garcia*, 140 S. Ct. 791, 801 (2020) (same; noting that the "conflict with state law must stem from either the Constitution itself or a valid statute enacted by Congress").[8]

It is also not possible to discern Congress's intent in passing the Joint Resolution. There are a variety of potential rationales for reversing an agency rule, reasons which may differ—and even conflict—among individual legislators. *See* 142 CONG Rec. S3683 (Statement for the

[8] CRA disapproval resolutions are thus not an exercise of Congressional power under the Supremacy Clause, but rather an assertion of the separation of powers. *See* 142 CONG. REC. S3686 (1996) (Joint Statement) (noting CRA corrects circumstance where federal agencies are given "too much latitude in implementing and interpreting Congressional enactments"); *see also* Bernard Bell, Notice & Comment, *A Preemptive Grin Without the Statutory Cat?: Congressional Review Act Disapproval & State Legislative Initiatives (Part II)*, Yale J. Reg. (Mar. 10, 2020), available at https://www.yalejreg.com/nc/a-preemptive-grin-without-the-statutory-cat-congressional-review-act-disapproval-resolutions-state-legislative-initiatives-part-ii/.

.

Record by Senators Nickles, Reid, and Stevens ("Joint Statement")) (1996) (CRA enables Congress to "find a rule to be too burdensome, excessive, inappropriate or duplicative"). That divergence in viewpoint is evident in the legislative record here. While one lawmaker thought the FCC overstepped its jurisdiction, *see* 163 CONG. REC. H2489 (2017) (Rep. Blackburn); others preferred case-by-case action to comprehensive regulation, *id.* at H2497 (Rep. Capuano); *id.* at S1928 (Sen. Thune); and yet another—the resolution's co-sponsor—preferred comprehensive Congressional privacy legislation, *see id.* at H2493 (Rep. Flores). In fact, some lawmakers affirmatively suggested they had no intent of pre-empting state law. *See id.* at H2497 (Rep. Collins) (noting that ISPs would remain subject to "the many other existing Federal and State privacy rules"); *id.* at S1925 (Sen. Flake) (same); *id.* at S1928 (Sen. Thune) (same). It is therefore unreasonable to claim, as Plaintiffs do, that the Joint Resolution constitutes a Congressional "judgment" against broadband-specific state privacy legislation, never mind a "federal scheme" with preemptive effect (Mot. 18). *See SPGGC, LLC v. Ayotte*, 488 F.3d 525, 531 (1st Cir. 2007).

Plaintiffs' reliance on the RIF Order fares no better. In that order, the FCC reinterpreted broadband Internet as an information service covered by Title I of the Communications Act, rather than as a telecommunications service covered by Title II, RIF Order ¶ 2, thereby placing it outside of the FCC's express regulatory authority, *see Mozilla*, 940 F.3d at 78. The upshot is that the RIF Order is not an instance of affirmative deregulation, but rather a decision by the FCC that (a) it lacked authority to regulate in the first place, and (b) it would defer to the FTC's enforcement of existing antitrust and consumer protection laws. RIF Order ¶ 181 ("By reinstating the information service classification …, we return jurisdiction to regulate broadband privacy … to the Federal Trade Commission."); *see also id.* ¶¶ 2, 140-54, 160-61, 182-83.[9]

[9] The cases Plaintiffs cite do not suggest otherwise. *Arkansas Electric* provides that "a federal decision to forgo regulation in a given area *may* imply an authoritative federal determination that … would have … pre-emptive force."

As the D.C. Circuit made clear when it rejected the FCC's ill-fated attempt to explicitly preempt state privacy laws, *see* RIF Order ¶¶ 194-204, preemption cannot be a "mere byproduct of self-made agency policy," but rather must be achieved through power delegated by Congress. *Mozilla*, 940 F.3d at 78; *see also id.* at 83 ("No matter how desirous of protecting their policy judgments, agency officials cannot invest themselves with power that Congress has not conferred."); *accord Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986) ("[A] federal agency may pre-empt state law only when and if it is acting within the scope of its congressionally delegated authority."). Here, the FCC decided that it has no such power. Accordingly, no matter how often the FCC stated its support for a "light touch" regulatory framework in the RIF Order, the FCC could not simultaneously decide that it lacked Title II regulatory authority over ISPs, but also dictate that no State could exercise similar authority pursuant to its own police powers.

The Law is thus in harmony with the FCC's reclassification of broadband Internet. *See Mozilla*, 940 F.3d at 85. There is no conflict between the FCC's proclamation that the FTC is the proper federal regulator of ISPs, RIF Order ¶¶ 140-41; *see also* 15 U.S.C. § 45, and Maine's decision to regulate at the state level. Further, as to the sole affirmative rules promulgated by the FCC in the RIF Order—transparency rules adopted pursuant to a separate, unrelated section of the Communications Act, RIF Order ¶¶ 215; *see also Mozilla*, 940 F.3d at 18—Plaintiffs have made no attempt to explain how the Law makes it impossible to comply with those transparency rules, nor is Defendant aware of any such tension.

Ark. Elec. Co-op. Corp. v. Arkansas. Pub. Serv. Comm'n, 461 U.S. 375, 384 (1983). This is simply a case, like *Ark. Electric*, where there is no such preemptive effect. *Id.* Likewise, in *Geier*, the Court determined that an affirmative Department of Transportation regulation, together with its authorizing statute, preempted a conflicting state common-law tort action. *See Geier*, 529 U.S. at 864-65. And, on the pages Plaintiffs cite, the Court simply reaffirms the preemptive effect of agency action absent formal preemptive intent. *See id.* at 883-84.

Plaintiffs' third bid at conflict preemption—that it somehow prevents compliance with federal disclosure rules—misses the mark, too. Plaintiffs cite two sources of potential conflict: FCC's Form 477 and initial disclosures required by Federal Rule of Civil Procedure 26(a). The Law is not a barrier to compliance with either.

Form 477 requires that ISPs identify, among other aspects of their service, the number of customers they serve in each census tract (Mot. 19-20). In other words, Form 477 does not require the reporting of customer-specific information, but rather seeks aggregate, deidentified information—information which is not protected by the Law. Indeed, aggregate, deidentified information, i.e., information about a group of customers that does not identify who those customers are, is neither customer personal information under § 9301(1)(C)), nor information pertaining to a customer under § 9301(3)(C). And while such information may be fashioned from customer personal information, the aggregation and deidentification of customer personal information is not a "use" of customer personal information under § 9301(2).[10] Quite the opposite: Stripping information of aspects warranting protection prior to its use or disclosure fulfills the statute's fundamental purpose and serves the public interest.

That said, even if Form 477 *did* require the disclosure of customer personal information, the Law still does not stand in the way. In recognition of the impossibility of predicting every potential future federal requirement for the provision of broadband Internet, § 9301(4)(A) of the statute provides that customer personal information may be used and disclosed "[f]or the purpose of providing the service from which such information is derived or for the services necessary to

[10] Defendant's interpretation of the Law is entitled to substantial deference. *See March v. Mills* 867 F.3d 46, 60 n.11 (1st Cir. 2017) (acknowledging duty to defer to Maine Attorney General's authoritative construction of state statute); *see also Forsyth City, Ga. v. Nationalist Movement*, 505 U.S. 123, 131 (1992) ("In evaluating respondent's facial challenge, we must consider the [government's] authoritative constructions of the ordinance, including its own implementation and interpretation of it.").

the provision of such service." Given the FCC requires entities that wish to provide broadband Internet to complete Form 477, *see* 47 U.S.C. §§ 502-03 (authorizing imposition of fines for failure to adhere to FCC rules), the use and disclosure of customer personal information fits neatly within § 9301(4)(A) and therefore does not run afoul of the Law.

As to the initial disclosure requirements of Federal Rule of Civil Procedure 26(a), Defendant is unaware of any hypothetical situation in which an ISP would be required to release customer personal information absent authorization by the customer in question. But even if such a hypothetical situation arose, and an ISP somehow found itself having to reveal the name, address, and/or telephone number of a customer because that customer had discoverable information, *see* Fed. R. Civ. P. 26(a)(1)(A)(i), there would still be no conflict between state and federal law. To comply with the Law, an ISP need only act pursuant to a court order. 35-A M.R.S. § 9301(4)(C). In nearly all civil cases litigated in the in the District of Maine, the court enters a scheduling order directing that disclosures set forth in Rule 26(a) be made by a date certain. *See* D. Me. Local Rule 16.2.[11] It is therefore not at all impossible—and, in fact, quite uncomplicated—to comply with both Rule 26(a)'s initial disclosure requirements and the Law. *See Fidelity Fed. Sav. & Loan Ass'n v. de la Cuesta*, 458 U.S. 141, 153 (1982) (requiring that compliance with federal and state law be a "physical impossibility" for preemption).

Conclusion

Maine's Privacy Law withstands First Amendment scrutiny, survives any attack for facial vagueness, and does not conflict with federal law or policy. Defendant respectfully requests that the Court deny Plaintiffs' Motion for Judgment on the Pleadings.

[11] An ISP could also, in an abundance of caution, affirmatively seek a court order to permit disclosures not otherwise permitted under the Law.

DATED: May 27, 2020

Respectfully submitted,

AARON M. FREY
Attorney General

/s/ Jason Anton
Jason Anton
Assistant Attorney General
jason.anton@maine.gov

Christopher C. Taub
Deputy Attorney General

Paul Suitter
Assistant Attorney General

Six State House Station
Augusta, Maine 04333-0006
Tel. (207) 626-8800
Fax (207) 287-3145

CERTIFICATE OF SERVICE

I hereby certify that on this, the 27th day of May, 2020, I electronically filed the above document with the Clerk of Court using the CM/ECF system, which will send notification of such filing to each of the following:

SCOTT H. ANGSTREICH
sangstreich@kellogghansen.com

SARAH E. ERICKSON-MUSCHKO
sericksonmuschko@gibsondunn.com

DENIS NICHOLAS HARPER
nharper@gibsondunn.com

JEFFREY A. LAMKEN
jlamken@mololamken.com

ALEX ATTICUS PARKINSON
aparkinson@kellogghansen.com

JOSHUA A. RANDLETT
jrandlett@rudmanwinchell.com

JACOB T. SPENCER
jspencer@gibsondunn.com

HELGI C. WALKER
hwalker@gibsondunn.com

COLLIN R. WHITE
cwhite@kellogghansen.com

SARAH AKHTAR
sakhtar@gibsondunn.com

/s/ Jason Anton