UNITED STATES DISTRICT COURT

DISTRICT OF MAINE

ACA CONNECTS – AMERICA'S COMMUNICATIONS ASSOCIATION; CTIA – THE WIRELESS ASSOCIATION; NCTA – THE INTERNET & TELEVISION ASSOCIATION; and U.S. TELECOM – THE BROADBAND ASSOCIATION,	)	
Plaintiffs,	)	Case No. 1:20-cv-00055-LEW
v.	)	
AARON FREY, in his official capacity as Attorney General of the State of Maine,	)	
Defendant.	)	

ORDER ON CROSS MOTIONS FOR JUDGMENT ON THE PLEADINGS

Plaintiffs ACA Connects – America's Communications Association, CTIA – The Wireless Association, NCTA – The Internet & Television Association, and U.S. Telecom – The Broadband Association, several trade associations whose members include Internet Service Providers ("ISPs") in the State of Maine, have filed a Motion for Judgment on the Pleadings (ECF No. 25), asking for final judgment to be entered on all five counts of their Complaint. They seek declaratory and injunctive relief against an allegedly unconstitutional Maine state statute on the grounds that it violates the First and Fourteenth Amendments, is unconstitutionally void for vagueness, and is preempted by federal law. Defendant Aaron Frey filed a Cross Motion for Judgment on the Pleadings (ECF No. 30) seeking judgment on Plaintiffs' preemption claims. For the reasons that follow, I DENY Plaintiffs' Motion for Judgment on the Pleadings and GRANT Defendant's Cross Motion for Judgment on the Pleadings.

BACKGROUND

Because the record is as yet little-developed, I will only briefly recite the facts giving rise to this lawsuit, and these motions. On June 6, 2019, Maine enacted L.D. 946, an Act to Protect the Privacy of Online Customer Information (the "Privacy Statute"), a consumer privacy law that took effect on July 1, 2020. The statute prohibits Maine providers of broadband Internet access service from using, disclosing, selling or permitting access to customer's personal information unless the customer expressly consents to that use, disclosure, sale or access, subject to certain exceptions. 35-A M.R.S. §§ 9301(2), (3)(A). The statute further restricts the use of "information the provider collects pertaining to a customer that is not customer personal information," if a customer opts out. *Id.* § 9301(3)(C). Under the privacy regime ISPs cannot refuse to serve a customer, charge a customer a penalty or offer a customer a discount if the customer does not consent to the use of personal information. The provisions of the bill apply to providers operating within the State when providing broadband Internet access service to customers that are billed for service received in the State and are physically located in the State. Plaintiffs filed suit to prevent this law from going into effect, and now seek final judgment based only on the pleadings. The Defendant cross-moved for judgment on Plaintiffs' claims that the state law is preempted.

DISCUSSION

Rule 12(c) allows a party to move for judgment on the pleadings at any time "[a]fter the pleadings are closed—but early enough not to delay trial." Fed. R. Civ. P. 12(c). A motion for judgment on the pleadings pursuant to Rule 12(c) is "ordinarily accorded much the same treatment" as a Rule 12(b)(6) motion. *Aponte-Torres v. Univ. of P.R.*, 445 F.3d 50, 54 (1st Cir. 2006). To survive a motion for judgment on the pleadings, therefore, a plaintiff must plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Because a motion for judgment on the pleadings "calls for an assessment of the merits of the case at an embryonic stage," I "view the facts contained in the pleadings in the light most favorable to the nonmovant and draw all reasonable inferences" in their favor. *Pérez-Acevedo v. Rivero-Cubano*, 520 F.3d 26, 29 (1st Cir. 2008) (citation omitted).

On a Rule 12(c) motion, unlike a Rule 12(b) motion, I consider the pleadings as a whole, including the answer. *See Aponte-Torres*, 445 F.3d at 54-55. "Like Rule 12(b)(6), Rule 12(c) does not allow for any resolution of contested facts; rather, a court may enter judgment on the pleadings only if the uncontested and properly considered facts conclusively establish the movant's entitlement to a favorable judgment." *Id.* at 54. Therefore, because it is so early in the litigation, I will not consider any facts the parties dispute; for example, I will not credit any allegations in the complaint denied in the answer. *See Santiago v. Bloise*, 741 F. Supp. 2d 357, 360 (D. Mass. 2010).

The list of uncontested facts in this case is not particularly long. Apart from admitting the identity of the parties, the jurisdiction of this Court, and the correctness of certain citations, Defendant denies the bulk of the allegations in Plaintiffs' Complaint. The factual record before me on these motions is therefore quite limited, confined mostly to the face of the Privacy Statute. The parties have not requested that I take judicial notice of any facts outside the Complaint, and I, therefore, consider their arguments only on this limited record.

A. PREEMPTION

The parties cross-move for judgment on the pleadings on Plaintiffs' preemption claims (Counts Three, Four, and Five[1]) and agree the record is ripe to decide the issue. The doctrine of preemption flows from the Supremacy Clause, which provides that "the Laws of the United States" (as well as treaties and the Constitution itself) "shall be the supreme Law of the Land … any Thing in the Constitution or Laws of any state to the Contrary notwithstanding." Art. VI, cl. 2. Consequently, Congress may preempt, *i.e.*, invalidate, a state law through federal legislation. It may do so not only by express language in a statute, but also by implication. *See Sprietsma v. Mercury Marine*, 537 U.S. 51, 64 (2002).

Plaintiffs allege the Privacy Statute impliedly conflicts with federal law, and is thus an unconstitutional exercise of the state's power. Conflict preemption exists where "compliance with both state and federal law is impossible," or where, as Plaintiffs argue here, "the state law stands as an obstacle to the accomplishment and execution of the full

[1] As Plaintiffs acknowledge in their Reply, Defendant's narrowing constructions moot Count Five, Plaintiffs' impossibility preemption claim. I will therefore dismiss that Count. *See* Reply at 2; Opposition at 20.

purposes and objectives of Congress." *Oneok, Inc. v. Learjet, Inc.*, 575 U.S. 373, 377 (2015) (internal citation omitted).

Plaintiffs believe Maine's Privacy Statute conflicts with two areas of federal law. In Count Three, Plaintiffs argue that the Statute conflicts with Congress's Joint Resolution to overturn the Federal Communications Commission's (FCC's) 2016 ISP Privacy Order pursuant to the Congressional Review Act. Plaintiffs contend the Statute "undermines the federal objectives that Congress sought to promote" through the Resolution." Complaint, ¶ 86. Count Four further alleges that the Statute conflicts with the FCC's Restoring Internet Freedom Order (RIF Order), in which the FCC determined that the best way to protect consumers' privacy interests is to pair mandatory privacy disclosures, RIF Order ¶ 223, with FTC enforcement of those disclosures, *id.* ¶ 244. Plaintiffs maintain "[t]he Statute conflicts with the FCC's determination about the best way to protect consumers' privacy interests" because the Statute "re-impos[es] the ISP Privacy Order's 'highly prescriptive privacy regulations for broadband Internet access service.'" Complaint ¶¶ 90-91 (quoting RIF Order ¶ 158).

In his Cross Motion for Judgment on the Pleadings, which incorporates the arguments presented in Defendant's Opposition to Plaintiffs' Motion for Judgment on the Pleadings (ECF No. 28), Defendant Frey counters that the Privacy Statute regulates a space Congress explicitly left open, and any conflict is a figment of Plaintiffs' imaginative pleading. (Opposition at 14-20.)

1. The ISP Privacy Order

In 2017, Congress passed and the President signed a Joint Resolution vacating the FCC's ISP Privacy Order pursuant to the Congressional Review Act (CRA). Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017) ("Joint Resolution"). Because the Joint Resolution passed through the bicameralism and presentment process, it carries the full force and preemptive effect of federal law. *See INS v. Chadha*, 462 U.S. 919, 951 (1983). However, this particular Joint Resolution has little effect. An expression of congressional disapproval under the CRA simply makes it "as though such rule had never taken effect," 5 U.S.C. § 801, returning to the status quo ante. Here, the Joint Resolution "disapproved" of the FCC's ISP Privacy Order, bringing back into force rules the ISP Privacy Order had itself repealed. *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Service, Order, 32 FCC Rcd 5442 (2017). This "disapproval" of an individual FCC order neither creates a broad federal policy nor speaks to what states might do in the ISP Privacy Order's absence. After the Joint Resolution, therefore, Maine had the same freedom to legislate to protect its citizens' privacy that it had before the ISP Privacy Order went into effect.

Plaintiffs' attempt to manufacture a conflict in this case is unavailing. The Supreme Court "has observed repeatedly that preemption is ordinarily not to be implied absent an 'actual conflict.'" *English v. General Elec. Co.*, 496 US 72, 90 (1990). In a typical example of an "actual conflict," the First Circuit recently found a local conservation commission's denial of a building permit was preempted where its federal counterpart approved a permit for the same project, considering the same evidence. *Algonquin Gas Transmission, LLC v. Weymouth, Massachusetts*, 919 F.3d 54, 65 (1st Cir. 2019) (finding

the local commission determination created "an effectively complete obstacle[] to FERC's ultimate determination that 'public convenience and necessity' 'require' that the Weymouth Compressor Station be built"). Plaintiffs fail to identify any similar obstacle Maine's Privacy Statute puts in the way of federal law.

In an attempt to create a conflict where none exists, Plaintiffs try to build a federal scheme using statements from lawmakers who voted for the Joint Resolution. They cite congressional testimony as evidence of this scheme, and argue that "Defendant fails to identify a single statement of congressional intent that undermines the widely shared view that Congress meant to prevent the imposition of ISP-only rules and to facilitate the creation of 'a single, uniform set of privacy rules.'" Plaintiffs' Reply at 14 (ECF No. 56) (citing, *e.g.*, 163 Cong. Rec. S1900, S1928 (Mar. 22, 2017) (Sen. Thune)). But unelected federal judges do not, or should not in any case, read Congressional tea leaves when deciding whether federal action preempts state law. Instead, we "interpret[] a statute [or in this case, a Joint Resolution] in accord with the ordinary public meaning of its terms at the time of its enactment." *Bostock v. Clayton Cty., Georgia*, No. 17-1618, __ U.S. __, __ (June 15, 2020) (slip op., at 4). Anything more than that is anti-democratic vanity run amuck; a judicial astrologist's attempt to divine the legislative heavens with an armillary sphere and palm readings. The words of a law are not the beginning of a riddle as to its meaning. Congressional debates and public statements are produced in bulk, but they do not reveal the hidden meaning of a law. "After all, *only the words on the page constitute the law adopted by Congress and approved by the President.*" *Id.* (emphasis added).

The words on this page read only that "Congress disapproves the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 Fed. Reg. 87274 (December 2, 2016) [the ISP Privacy Order], and such rule shall have no force or effect." Joint Resolution, Pub. L. No. 115-22, 131 Stat 88 (Apr. 3, 2017). Congress's nullification of the ISP Privacy Order, therefore, creates no overarching federal policy, and enacts no scheme with which the Maine Privacy Statute can conflict.

Finally, Plaintiffs' argument flies in the face of a strong presumption against implied federal preemption of state law. That presumption is strongest "in fields of traditional state regulation," and it applies whether preemption is alleged to be explicit, implied, or a result of conflict. *New York State Conference of Blue Cross & Blue Shield Plans v. Travelers Ins. Co.*, 514 U.S. 645, 655 (1995). Privacy regulation is just such a field. *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."). To drive the point home, the law Plaintiffs cite as justification for preemption itself conceived of joint state and federal regulation. *See* 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."); 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]"). Maine's

Privacy Statute is an exercise of state regulatory authority anticipated by federal law, which Congress's Joint Resolution does not foreclose. I, therefore, find Maine's statute is not preempted and will grant Defendant's Cross Motion for Judgment on the Pleadings on Count Three.

2. FCC's RIF Order

Plaintiffs also argue, in Count Four, that Maine's Privacy Statute is preempted by the federal policy expressed in the FCC's RIF Order, in which the FCC "determined that the best way to protect consumers' privacy interests 'without imposing costly burdens on ISPs' is to pair mandatory privacy disclosures, RIF Order ¶ 223, with FTC enforcement of those disclosures, *id*. ¶ 244." Complaint, ¶ 90. In the RIF 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 the FCC's regulatory ambit. *Mozilla Corp. v. Fed. Commc'ns Comm'n*, 940 F.3d 1, 78 (D.C. Cir. 2019). The upshot is that the RIF Order is not an instance of affirmative deregulation, but rather a decision by the FCC that it lacked authority to regulate in the first place and 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. As described in further detail above, 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.

Not only is the FCC's abdication of authority in favor of the FTC of dubious preemptive effect, but Plaintiffs also have failed to identify any conflict between the FCC's proclamation that the FTC is the proper federal regulator of ISPs, RIF Order ¶¶ 140-41, and Maine's decision to impose privacy protections at the state level. The idea that the FCC's relinquishment of authority over ISPs creates a federal scheme prohibiting state privacy regulation of ISPs blinks reality. Because there is no tension between Maine's Privacy Statute and any of the affirmative rules promulgated by the FCC in the RIF Order, I likewise find Plaintiffs have failed to show how the FCC's RIF Order preempts state action, and therefore grant Defendant's Motion for Partial Judgment on the Pleadings for Counts Four.

B. FIRST AMENDMENT CLAIM

Having decided that federal law does not preempt Maine's Privacy Statute, I will consider Plaintiffs' shoot-the-moon argument that the few uncontested facts in the record entitle them to final judgment on Count One, the claim that the Privacy Statute is a facially unconstitutional violation of the First and Fourteenth Amendments. Like Harold with a purple crayon, Plaintiffs have drawn themselves a steep mountain to climb by filing for judgment on the pleadings. As is frequently the case, much hinges on which First Amendment standard applies. Plaintiffs argue that Maine's ISP-specific regulation is both speaker- and content-based, so should be reviewed with strict scrutiny. Plaintiffs' Motion at 11 (citing *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011)). Defendant points me to the more familiar intermediate scrutiny standard typically applied to commercial speech, articulated in *Central Hudson Gas & Electric Corporation v. Public Service Commission*

of New York, 447 U.S. 557, 561 (1980). Defendant's Opposition at 2. For the reasons that follow, I find Maine's Privacy Statute is subject to intermediate scrutiny.

The Privacy Statute restricts ISPs' ability to use, disclose, sell, and provide access to customers' personal information. Though this is not speech in the political-rally-in-the-town-square sense, the Supreme Court has held that "creation and dissemination of information [is] speech within the meaning of the First Amendment," and found "[t]here is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes." *Sorrell*, 564 U.S. at 570. I, therefore, proceed from the presumption that Plaintiffs' marketing of customer data, like the prescriber-identifying data in *Sorrell*, is sheltered by the First Amendment. But not all speech deserves the same level of protection. "Commercial speech, or 'expression related solely to the economic interests of the speaker and its audience,' is ordinarily accorded less First Amendment protection than are other forms of constitutionally guaranteed expression." *Rocket Learning, Inc. v. Rivera-Sanchez*, 715 F.3d 1, 13 (1st Cir. 2013) (quoting *Cent. 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 *Cent. Hudson*, 447 U.S. at 566).

Plaintiffs suggest that the Supreme Court altered the *Central Hudson* analysis when it decided *Sorrell*, applying "heightened scrutiny" to a New Hampshire commercial speech regulation, and striking that regulation down. Plaintiffs believe *Sorrell* supplants *Central*

Hudson, auguring a new regime of strict scrutiny for any speaker- or content-based speech regulation, commercial or otherwise. Plaintiffs are mistaken. *Sorrell* holds that "heightened scrutiny" applies when regulations discriminate on the basis of the speaker or the content. But *what level* of "heightened" scrutiny is, in turn, determined by the type of speech being regulated. *Sorrell* 564 U.S. at 571 (noting the possibility for "a special commercial speech inquiry" or "a stricter form of judicial scrutiny," *i.e.* strict scrutiny). The First Circuit has yet to weigh in, but every other Circuit to consider the question has affirmed that *Central Hudson* is still good law following *Sorrell*, and that intermediate scrutiny ought to govern the constitutional review of commercial speech regulations.[2] Because I find Maine's Privacy Statute regulates commercial speech, I will analyze its constitutionality under *Central Hudson*.

At this preliminary stage, Plaintiffs have not done enough to show, on the face of the pleadings, an entitlement to judgment as a matter of law on their claim that Maine's Privacy Statute is a facially unconstitutional violation of the First Amendment. They make two arguments that Maine's law does not pass *Central Hudson* muster. First, Plaintiffs believe that Maine cannot show it has a substantial interest in regulating the specific "aspect" of privacy at issue "in the circumstances of this case." Motion at 12 (quoting *Cal.*

[2] *See, e.g. Retail Digital Network, LLC v. Prieto*, 861 F.3d 839, 845–46 (9th Cir. 2017); *see also Vugo, Inc. v. City of New York*, 931 F.3d 42, 49 (2d Cir. 2019), cert. denied sub nom. *Vugo, Inc. v. New York, NY*, No. 19-792, 2020 WL 1978946 (U.S. Apr. 27, 2020); *1-800-411-Pain Referral Service, LLC v. Otto*, 744 F.3d 1045, 1055 (8th Cir. 2014) (the "upshot" of *Sorrell* is that "when a court determines commercial speech restrictions are content- or speaker-based, it should then assess their constitutionality under *Central Hudson*"); *In re Brunetti*, 877 F.3d 1330, 1350 (Fed. Cir. 2017) ("[P]urely commercial speech [is] reviewed according to the intermediate scrutiny framework established in Central Hudson."); *Flying Dog Brewery, LLLP v. Michigan Liquor Control Comm'n*, 597 F. App'x 342, 365 (6th Cir. 2015) ("[A]lthough Sorrell stated that 'heightened judicial scrutiny' applied, it reaffirmed the use of the *Central Hudson* test.").

Democratic Party v. Jones, 530 U.S. 567, 584 (2000)). Second, they stress that "the Statute's restrictions are 'more extensive than is necessary to serve' privacy interests because they restrict 'speech that poses no danger' to privacy." *Id.* at 13 (quoting *Cent. Hudson*, 447 U.S. at 565-66).

Although the parties dispute whether Maine possesses sufficient interest to regulate ISPs in this way, Plaintiffs' Motion for Judgment on the Pleadings fails because it boils down to this: there is no record on which to evaluate the relative strength of the parties' arguments, much less one that convincingly entitles Plaintiffs to final judgment under *Central Hudson*.

For example, for the state to show its interest is "substantial" to satisfy *Central Hudson*, it must demonstrate that (1) "the harms it recites are real," and (2) "that its restriction will in fact alleviate them to a material degree." *Edenfield v. Fane*, 507 U.S. 761, 771 (1993). The Supreme Court has "permitted litigants to justify speech restrictions by reference to studies and anecdotes," which might come before me on a summary judgment record. *Lorillard*, 533 U.S. at 555. Though Plaintiffs allege that Maine "made no attempt to show that ISPs' practices have harmed consumer privacy," and that "the Legislature [did not] make findings that its ISP-specific rules are necessary in light of existing, uniform technology-neutral federal privacy rules," Complaint ¶ 68, Defendant denies these allegations in full. Answer ¶ 68. Without more, I have no information properly in front of me—when considering a motion for judgment *on the pleadings*—to assess whether Maine has a substantial interest in regulating privacy as it does. Because I do not resolve factual disputes at this stage, and make all inferences in favor of the

nonmoving party, the Defendant may well be able to prove it has a "substantial interest" in protecting privacy as it has, and for that reason I will not award Plaintiffs final judgment on the basis of their first argument.

Plaintiffs' argument that the Privacy Statute is not well-tailored to its purpose fares no better. Under *Central Hudson*, the Defendant must "affirmatively establish" a reasonable fit between the regulation and its goal. *Bd. of Trustees of State Univ. of New York v. Fox*, 492 U.S. 469, 480 (1989). This inquiry does not require "that there be no conceivable alternative" to the government's approach, or that the government's regulation be the least restrictive means of advancing its asserted interests. *Id*. at 478. In addition, the Defendant is afforded "considerable leeway in determining the appropriate means to further a legitimate government interest." *Clear Channel Outdoor, Inc. v. City of New York*, 594 F.3d 94, 105 (2d Cir. 2010) (internal alterations and quotation marks omitted); as an unelected federal judge, I am "loath to second-guess the [g]overnment's judgment to that effect." *Fox*, 492 U.S. at 478. All this is to say that the Defendant has plenty of room to show—through discovery—that its privacy statute does not overshoot the mark. At this stage, the only evidence of "fit" I have before me are Plaintiffs' allegations that the Privacy Statute is "both overinclusive and underinclusive," Complaint ¶¶ 69, 70, and Defendant's corresponding denials, Answer ¶¶ 69, 70. As noted above, this is not enough to award Plaintiffs final judgment on the pleadings, and I will deny their motion on this basis as well.

C. Void for Vagueness

In Count Two, Plaintiffs argue the Privacy Statute is unconstitutionally vague for two reasons: an unclear geographic scope and a nebulous definition of "customer personal

information" in 35-A M.R.S. § 9301(1)(C), which further obscures the definition of "information pertaining to a customer that is not customer personal information" in § 9301(3)(C). They allege that, because "[t]hese ambiguities deprive ISPs of 'fair warning' as to what the Statute prohibits, 'chilling the exercise of [their] First Amendment rights' as they aim for compliance," the Privacy Statute is void for vagueness. Complaint ¶ 80 (citing *Nat'l Org. for Marriage v. McKee*, 649 F.3d 34, 62 (1st Cir. 2011)). Instead of reading the language and interpreting its meaning, however, Plaintiffs simply throw up their hands and cry foul. Plaintiffs argue the law's vagueness chills their First Amendment protected expression as they "develop their products and services," but fail to substantiate any real danger of a chill. Should the Plaintiffs demonstrate a concrete chill related to a significant aspect of their speech activity, they may be entitled to relief. However, that showing is not established on the pleadings and, thus, I will deny their motion for judgment on Count Two.

1. Legal Standard

"It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined." *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972). And even though a law may be constitutional under the First Amendment it may still be vulnerable to a facial vagueness challenge under the Due Process Clause. *Whiting v. Town of Westerly*, 942 F.2d 18, 22 (1st Cir. 1991). "For such a facial challenge to succeed, however, the complainant must demonstrate that the law is impermissibly vague in all of its applications." *Id.*; *see also Donovan v. City of Haverhill*, 311 F.3d 74, 77 (1st Cir. 2002) ("To prevail in a facial challenge to an ordinance that does not regulate

constitutionally protected conduct, plaintiffs must surmount a dauntingly high hurdle." (citing *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498-99 (1982)).

To comport with due process, a law must draw boundaries "'[1] with sufficient definiteness that ordinary people can understand what conduct is prohibited and [2] in a manner that does not encourage arbitrary and discriminatory enforcement.' The void-for-vagueness doctrine embraces these requirements." *Skilling v. United States*, 561 U.S. 358, 402–403 (2010) (internal citation omitted). But as the First Circuit has noted, "words are rough-hewn tools, not surgically precise instruments," which inevitably means "some degree of inexactitude is acceptable in statutory language." *URI Student Senate v. Town Of Narragansett*, 631 F.3d 1, 13–14 (1st Cir. 2011) (citing *Grayned*, 408 U.S. at 110 (acknowledging that one "can never expect mathematical certainty from our language")). Consistent with this reality, "the fact that a statute requires some interpretation does not perforce render it unconstitutionally vague." *IMS Health Inc. v. Ayotte*, 550 F.3d 42, 61 (1st Cir. 2008). "[R]easonable breadth" in statutory language does not require that a law be invalidated on vagueness grounds. *See Grayned*, 408 U.S. at 110.

Context matters when evaluating a plaintiff's facial void-for-vagueness challenge. For example, the Supreme Court has applied a "less strict vagueness test" to commercial regulation "because its subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action." *Vill. of Hoffman Estates*, 455 U.S. at 498. And vagueness review is less exacting still where the law at issue carries no criminal penalties. As the

First Circuit has noted, "vagueness concerns are more pressing when there are sanctions (such as expulsion) attached to violations of a challenged regulation." *Ridley v. Massachusetts Bay Transp. Auth.*, 390 F.3d 65, 95–96 (1st Cir. 2004); *see also Reno v. ACLU*, 521 U.S. 844, 871–72 (1997) (the vagueness inquiry is most rigorous in a criminal context, where there is a high risk speech will be chilled). Because Plaintiffs' members are businesses accustomed to regulation, and the Privacy Statute does not appear to carry any criminal penalty, the vagueness review is less searching in this case.

2. Geographic Scope

I begin with the Privacy Statute's geographic scope. Plaintiffs complain that the Statute provides "no clear 'standard of conduct'" to judge whether the Statute "extends to non-Maine residents who use their mobile broadband Internet services during the time they visit Maine." Motion at 17 (citing *Coates v. City of Cincinnati*, 402, U.S. 611, 614 (1972). But neither *Coates* nor the vagueness doctrine more generally supports Plaintiffs' claim. In *Coates*, the Court found a statute that criminalized "annoying" conduct was vague because its terms were open to subjective interpretation and arbitrary enforcement. *Coates*, 402 U.S. at 614 ("Conduct that annoys some people does not annoy others."). The Privacy Statute, by contrast, applies to a clearly-defined set of businesses when providing services to a clearly-defined set of customers; the law regulates ISPs operating in Maine serving customers that are physically located in Maine, and physically billed for those services in Maine. 35-A M.R.S. § 9301(7). This language gives the Plaintiffs fair warning of the customer accounts subject to regulation without leaving any wiggle room for arbitrary enforcement or confusion. Because I find the language sufficiently clear, I will deny

Plaintiffs' Motion to invalidate the Privacy Statute as unconstitutionally vague due to its geographic scope.

3. Customer Personal Information

Plaintiffs next argue that the Privacy Statute's definition of "customer personal information" in the opt-in section of the statute is unclear, making the subsequent definition of "information … pertaining to customers but not customer personal information" in the opt-out section impossible to parse. They believe these inexact terms render the Statute unconstitutionally vague because they will not know where opt-in information ends and opt-out information begins. The Defendant counters that the Legislature relied explicitly on the FCC's repealed *ISP Privacy Order*, copying its distinction between opt-in and opt-out categories almost verbatim. Since the *ISP Privacy Order* went through notice and comment rulemaking and went into place in 2016, Defendant believes Plaintiffs are well aware of the line Maine draws between opt-in and opt-out.

"In prohibiting overly vague laws, the [vagueness] doctrine seeks to ensure that persons of ordinary intelligence have 'fair warning' of what a law prohibits, …and, in cases where the "statute 'abut(s) upon sensitive areas of basic First Amendment freedoms,' avoid chilling the exercise of First Amendment rights." *McKee*, 649 F.3d at 62 (citing *Grayned*, 408 U.S. at 108-09). The Maine statute very nearly copies a federal regulation familiar to the Plaintiffs, and, so far as can be assessed from the pleadings, provides sufficient clarity to give notice of what will fall into the bucket of "customer personal information." The FCC's *ISP Privacy Order* defined the information subject to opt-in approval in its scheme as "sensitive customer PI." *See ISP Privacy Order*, 31 FCC Rcd at 14080, App. A,

§ 64.2002(f), (n). Maine's Privacy Statute tracks that definition almost exactly, except that it adds a few categories of information to be covered by its opt-in protection. 35-A M.R.S. § 9301(1)(C) (adding "name, billing information…billing address, [and] demographic information" to its list of information covered by the opt-in requirement). What Maine adds to the *ISP Privacy Order*'s opt-in category is identified with seemingly straight forward terms that should prove easy to apply. Because the "customer personal information" in the Privacy Statute's opt-in section mirrors language familiar to Plaintiffs, and makes a few precise additions, I am not persuaded that Plaintiffs' pleadings resolve the matter. By logical extension, I cannot resolve on the pleadings the related concern over what information is "not customer personal information."[3]

Finally, Plaintiffs' Motion simply fails to clarify how an ill-defined opt-in and opt-out regime would inhibit any protected First Amendment activity; for example, how it might chill them from preparing particular marketing materials for sale to customers. And, they have not begun to bear their burden to show the statute would be unconstitutional in "all of its applications," as they must for a facial challenge. *See URI Student Senate*, 631 F.3d at 13.

[3] I accept the limiting construction offered by the state that it refers to the same category expressed in the ISP Privacy Order. *Vill. of Hoffman Estates*, 455 U.S. at 495, n.5 ("In evaluating a facial challenge to a state law, a federal court must, of course, consider any limiting construction that a state court or enforcement agency has proffered."). I further note that Maine's addition of "including, but not limited to" in the opt-in categories it copies from the ISP Privacy Order does not render those definitions unconstitutionally vague. Though such language appears broad at first blush, these additions are limited by the phrases they modify: "[p]ersonally identifying information," § (1)(C)(1), and "[i]nformation from a customer's use of broadband Internet access service," § (1)(C)(2). Because these phrases are spelled out by the representative categories copied from the ISP Privacy Order, a list of categories well-known to these Plaintiffs, I do not find these "including but not limited to" additions push the Privacy Statute into unconstitutionally vague territory. Should the law be enforced outside the bounds of the statutory language it might give rise to an as-applied challenge, but such language does not make the Privacy Statute unconstitutionally vague on its face.

For these reasons, I will deny Plaintiffs' Motion for Judgment on the Pleadings as to Count II.

CONCLUSION

For the foregoing reasons, Plaintiffs' Motion for Judgment on the Pleadings (ECF No. 25) is DENIED, and Defendant's Cross Motion for Judgment on the Pleadings (ECF No. 30) is GRANTED. Counts Three, Four, and Five are DISMISSED.

SO ORDERED.

Dated this 7th day of July, 2020.

/s/ Lance E. Walker
UNITED STATES DISTRICT JUDGE