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 the Attorney General of Maine;

Defendant.

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

BRIEF OF PUBLIC KNOWLEDGE AS *AMICUS CURIAE* SUPPORTING DEFENDANT

TABLE OF CONTENTS

INTRODUCTION

In June of 2019, Maine passed a law prohibiting broadband internet service providers (hereafter "ISPs") from using, disclosing, selling, or permitting access to customer personal information unless the customer expressly consents, or a lawful exception applies. This law does not infringe on ISPs' First Amendment rights and is not preempted by any federal laws.

INTERESTS OF AMICUS

Public Knowledge (PK) is a 501(c)(3) non-profit organization that advocates for technology policy that serves the public interest. PK advocates before Congress, the courts, the Federal Communications Commission, and other governmental entities. Public Knowledge works to uphold and protect consumers' rights, including the right to privacy.

ARGUMENT

I. MAINE'S ISP PRIVACY LAW DOES NOT RAISE FIRST AMENDMENT CONCERNS.

The Plaintiff ISPs argue that Maine's ISP privacy protection law, 35-A M.R.S. § 9301, violates their First Amendment right to use the information broadband subscribers have no choice but to expose to ISPs in order to use broadband. Plaintiffs' argument fails for many reasons. First, it is important to recognize Maine's ISP privacy law is part of a longstanding and continuing tradition of complementary state and federal laws that prohibit communications networks, whether paper or electronic, from disclosing any information relating to the acts of communication.[1] As discussed below, this common law duty was recognized – and often augmented by statute – because individuals wishing to send messages have no choice but to

[1] *See* Daniel J. Solove, "A Brief History of Information Privacy Law" in PROSKAUER ON PRIVACY, §3.1 PLI (2006), https://scholarship.law.gwu.edu/faculty_publications/923/

expose their information to the messenger.[2] Complainants' position unfairly permits the intermediary to exploit information to which they would otherwise not be given access, permitting unjust enrichment, and threatening both personal privacy and commerce.

When Congress, or a state, acts to modernize and protect a long recognized common law right, it raises no question of "viewpoint discrimination" triggering strict scrutiny. *See, e.g. Eichenberg v. ESPN*, 876 F.3d 979, 983-84 (9th Cir. 2017) (Video Privacy Protection Act rooted in common law privacy); *Braitberg v. Charter*, 836 F.3d 925, 93 (2015) (common law privacy origin of Cable Privacy Act).[3] It does not matter whether the law is passed by Congress or by a state legislature. *See Boelters v. Advance Magazine Publisher, Inc.*, 210 F. Supp. 3d 579, 590 (S.D. N.Y. 2016). Indeed, were it otherwise, longstanding requirements of lawyer/client confidentiality or the fiduciary duties owed by trustees to beneficiaries would be subject to strict scrutiny as discriminatory restrictions. As long as the nexus drawn by the state between the regulation and the differential treatment is reasonable, and there are no other reasons to suspect animus against a particular speaker, no claim of viewpoint discrimination lies. *National Amusements v. Town of Dedham*, 43 F.3d 731, 737-40 (1st Cir. 1995).

Plaintiffs' argument that permitting advertisement of an ISP's own additional communications products but not non-communication products triggers strict First Amendment scrutiny likewise fails. An ISP's own communications products are clearly relevant to the subscriber and the subscriber's existing use of the service. They are therefore a traditional part of

---

[2] *Id.* and at §1.4.1 *See also* Adam Candueb, "The Common Carrier Privacy Model," 51 U.C. Davis L. Rev. 805, 816-20 (2018).

[3] *See generally*, Niel M. Richards, "Reconciling Data Privacy and the First Amendment," 52 U.C.L.A. L. Rev. 1150 (2005); Peter A. Winn, "Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law," 33 Rutgers L.J. 617 (2002).

the contractual relationship that imposes the common law duty of confidentiality. By contrast, non-communications related products are not rationally related to the contracted service, and therefore fall within the general ambit of the traditional common law right Maine's ISP privacy law protects. Consistent with longstanding communications law, the ISP is simply prevented from using privileged and confidential information to unjustly enrich itself and give itself an unfair competitive advantage.

Finally, it should be noted that the bulk of behavior prohibited by the statute is not in the least expressive, and therefore enjoys no First Amendment protection. *Cf. Spence v. Washington*, 418 U.S. 405, 409-10 (1974) (conduct must actually intend to communicate something to qualify for First Amendment protection); *Barnes v. Glen Theatre*, 501 U.S. 560, 576-77 (1991) (Scalia, J. concurring). The ability to compile information into a database is not automatically a creative or expressive act. *See Feist Publications, Inc. v. Rural Tel. Serv. Co*. 499 U.S. 340 (1991). As the Supreme Court has observed, laws that are generally in service to protecting common law rights,[4] laws governing contracts,[5] and laws protecting competition[6] may have some incidental impact on speech without raising First Amendment issues.[7]

This point is emphasized by analysis of cases involving the analogous federal statute protecting Customer Proprietary Network Information (CPNI). *See* 47 U.S.C. § 222. As discussed in greater detail below, those cases finding a First Amendment interest at stake did so either because the parties agreed to apply the commercial speech test or because the court found a direct link to expressive conduct thwarted by CPNI.

---

[4] *See Cohen v. Cowles Media Co.*, 501 U.S. 663 (1991)
[5] *Id.*
[6] *See Associated Press v. United States*, 326 U.S. 1 (1945).
[7] *See Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011).

Furthermore, the "audience targeting" rationale discussed in *U.S. West v. FCC*[8] as the basis of applying Intermediate Scrutiny under the "Commercial Speech" test has been rightly criticized for a variety of reasons.[9] The district court should therefore decline to apply it here. But even if *U.S. West* applies, it does not change the outcome. *U.S. West* addressed only the provision governing advertising of the telecommunications provider's own, non-communications related products. It did not address the prohibition on the sale to third parties absent express consent. Even then, it simply found "opt in" overly burdensome as compared to "opt out," rather than striking down the law as a whole. *U.S. West* is therefore wholly distinguishable. Even if the Court here were to follow *U.S. West*, which the First Circuit has not done,[10] the strongest remedy ISP complainants may hope for is an injunction requiring opt out rather than opt in consent.

Selling a collection of data to be used as a tool to develop products, enhance a search engine, or develop marketing strategies is no more "expressive" than selling inside information to enhance a stock trade or selling paper at a retail outlet. The customer data is not commercial speech "proposing a transaction," it is the object of the transaction. By the ISPs' logic, regulations related to provision of electricity raise First Amendment concerns as electricity is also used in created digital products and digital advertisements. No one has ever found that the regulation of raw materials – such as marble or paper – that imposes incidental burdens on speakers as well as others raises First Amendment concerns. *Cf. Minneapolis Star & Tribune Co. v. Minnesota Commissioner of Revenue*, 460 U.S. 575 (1983) (tax on special ink used primarily

---

[8] 182 F.3d 1224 (10th Cir. 1999).

[9] *See* Niel M. Richards, "Reconciling Data Privacy and the First Amendment," 52 U.C.L.A. L. Rev. 1150 (2005) at 1193-95.

[10] *See generally Hennessy v. City of Melrose*, 194 F.3d 237 (1st Cir. 1999) (conduct must actually be clearly intended to express a specific message); *Conward v. Cambridge School Commission*, 171 F.3d 12 (1st Cir. 1999) (teacher handing student an unread flyer based on title that turned out to contain indecent content not an expressive act protected by First Amendment).

by newspapers uniquely targets press). Since the ISP privacy law targets the sale of data for any purpose, the majority of which are not expressive, the Court should find the law raises no First Amendment interest.

A. The Common Law and Competition Roots of ISP Privacy Laws

Laws governing the privacy of messages and the duty of messengers are of ancient vintage. As far back as the year 1000, the leading European Rabbinic authorities issued a religious ban on reading another person's private mail.[11] This duty of confidence arises in the common law well before the founding of the Republic in other matters dealing with private business and personal dealing.[12] The common law has therefore found an obligation on lawyers to maintain the confidences of their clients, doctors to maintain the confidentiality of patient information, and – of greatest relevance here – on deliverers of messages with regard to the messages or packages they deliver.[13] Laws protecting the privacy of telegraph communications were passed by a majority of the states in the 19th Century.[14] The Supreme Court, in a case involving a contract between Western Union and the New York Cotton Exchange, found that New York's state telegraph statute simply embodied the common law contractual requirement that a carrier may only disclose the content – or even the fact of transmission – of a message to the parties so directed.[15]

---

[11] Orthodox Union, "Gershom, Rabbeinu." Available at: https://www.ou.org/judaism-101/bios/leaders-in-the-diaspora/rabbeinu-gershom/ (last viewed May 26, 2020).

[12] *See generally*, Jack M. Balkin, "Information Fiduciaries and the First Amendment," 48 U.C. Davis L. Rev. 1183, 1205-08 (2016).

[13] Candeub, 51 U.C. Davis L. Rev. at 815-820.

[14] Solove, A Brief History of Information Privacy Law at §1.3.

[15] See *Moore v. NY Cotton Exchange*, 270 U.S. 593, 605 (1920).

Authorities in the 19th and early 20th Centuries provided multiple justifications for both the common law duty of confidentiality imposed on the telegraph service and for states to define the nature of the protections by statute. Overall, courts, legislatures and scholars identified three central reasons for such protections. The first was simple moral outrage at the violation of personal privacy – what Louis Brandies and Samuel Warren would famously call "the fundamental right to be let alone."[16] The second was contractual in nature. Implied in the contract to carry the message was a duty similar to that of lawyers, bankers and other trusted individuals to carry out the instruction of the client solely for the benefit of the client. For the telegraph, that meant delivering the message only to the person(s) directed by the client and keeping all information about the message confidential. To allow otherwise would allow a form of "unjust enrichment" since the telegraph operator was being paid to deliver the message and only came into possession of the information because of the contract.[17] Finally, legislators and judges observed that permitting disclosure of a client's telegraph information "would destroy the usefulness of this most important and valuable mode of communication" by undermining the willingness of businesses or individuals to transmit messages.[18]

The deployment of the telephone triggered a similar response, but with one critical difference. In addition to the regulation of telephone privacy at the state level by state public utility commissions, Congress created a national communications privacy statute in 1934 that governed all "interstate or foreign communication by wire and radio."[19] In doing so, Congress

---

[16] Samuel D. Warren and Louis D. Brandies, "The Right to Privacy," 4 Harvard L. Rev. 193 (1890).

[17] *See* Candueb at 817; Balkin at 1199-1200.

[18] History of Information Privacy, at 1-8.

[19] *See* 47 U.S.C. § 605. Congress also passed 47 U.S.C. § 414, which explicitly preserves any common law or state statutory cause of action in addition to the remedies available under the

simply codified what had become the existing common law right of privacy in communications. The statute prohibited anyone involved in transmission of a private communication from even "divulge[ing]" the existence of the communication, let alone any details relating to the communication, except with the express permission of the customer. *See* 47 U.S.C. § 605.[20]

B. Because the Maine Statute Follows the Traditional Common Law Approach, It Does Not Trigger First Amendment Scrutiny By "Singling Out" ISPs.

The rise of each new communications technology has invariably raised the same questions of privacy and – sometimes sooner, sometimes later, sometimes only after some states had acted – Congress has responded by updating the applicable laws. For example, in 1984, Congress amended the Communications Act to provide privacy protections for cable

---

Communications Act. *See Aaronson v. Sprint Spectrum, L.P.*, 90 F. Supp. 662, 668 (W.D. Pa. 2000) (Section 414 demonstrates Congressional intent to preserve remedy of state privacy law).

[20] Given Plaintiffs' argument that the Maine statute is somehow defective for failing to incorporate the "sensitive" v. "non-sensitive" dichotomy used by the Federal Trade Commission and the repealed FCC regulations, it is particularly noteworthy that none of the common law duties, state statutes, or federal statutes discussed in this section or below rely on the "sensitive" v. "non-sensitive" dichotomy cited by complainants as the "norm" with which Maine's ISP privacy statute is supposedly out of step. This dichotomy did not exist in any statute or common law duty and is entirely a product of the FTC's efforts to address privacy in the digital age with the extremely limited tools given it by Congress. *See* Harold Feld, "Principles for Privacy Legislation: Putting People Back in Control of Their Information," Public Knowledge (2017) at 15-17. Available at: https://www.publicknowledge.org/documents/principles-for-privacy-legislation. The FCC did not initially propose such a dichotomy, *see* Protecting the Privacy of Customers of Broadband and Other Telecommunications Providers, *Notice of Proposed Rulemaking* 31 FCC Rcd 2500 (2016), and only adopted it in the final rules at the insistence of the ISPs themselves that the FCC should "harmonize" its rules with those of the FTC. Protecting the Privacy of Customers and Other Telecommunications Providers, *Report and Order*, 31 FCC Rcd 139111 (2016). As "big data" technology has increasingly allowed third parties to ascertain highly personal and sensitive information from supposedly "non-sensitive" data, the sensitive/non-sensitive dichotomy has been subject to increasing criticism as unworkable. *See generally* Jonathan Andrew, "Location Data and Human Mobility: An Evaluation of a Dissonance that Frames Data Protection and Privacy Rights," European University Institute (2018). Indeed, it is far more reasonable to suppose that Congress "legislatively vetoed" (see discussion below) the FCC's rules out of frustration with its departure from the traditional common law approach and a desire to see the states impose more traditional privacy protections grounded in long-established contract principles and fiduciary duties than to imagine that Congress intended to preempt the states.

subscribers,[21] and again in 2004 for satellite television subscribers.[22] In 1988, Congress passed the Video Privacy Protection Act (VPPA)[23]. In 1996, Congress dramatically expanded the scope and specificity of privacy protections afforded to telecommunications carriers as part of its effort to create a competitive telecommunications market, promote innovation, and ensure subscriber privacy.[24] In each case, Congress must specify what rights it intends to protect. Doing so does not "single out" a particular medium or speaker on the basis of content. *See National Amusements, Inc. v. Town of Dedham,* 43 F.3d 731, 737-40 (1st Cir. 1995).

Unfortunately, as was the case over a century ago with the telegraph, Congress has once again found itself paralyzed and unable to pass legislation to codify traditional common law principles for broadband. It therefore once again falls to the states to act first, as they did in the 19th Century. As a matter of necessity, this requires identifying the technology and specific businesses subject to the statute. Such specificity has been held to be content neutral regardless of whether the law in question is passed by a state rather than Congress. *See Boelter v. Advanced Magazine Publishers, Inc.*, 210 F. Supp. 3d 579 (S.D.N.Y. 2016) (rejecting strict scrutiny of state law prohibiting disclosure of information related to purchase, rental or borrowing of written materials based on analogy to VPPA).

This distinguishes the Maine ISP privacy law from the pharmacy privacy law at issue in *Sorrell v. IMS Health, Inc*., 564 U.S. 552 (2011). In *Sorrell*, the statute made it illegal for

---

[21] Pub. L. 98-549 §9, codified at 47 U.S.C. §551.
[22] Codified at 47 U.S.C. §338(i).
[23] *See Yershov v. Gannet Satellite Information Network*, 820 F.3d 482, 485 (1st Cir. 2016).
[24] Harold Feld, Charles Duan, John Gasparini, Tennyson Holloway and Meredith Rose, "Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission's Privacy Rules for the Digital World," Public Knowledge (2016). Available at: https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper.pdf.

pharmacies to disclose personally identifying information without consent "for marketing," and prohibited makers and marketers of pharmaceuticals from acquiring and using personally identifiable information "for marketing." The statute permitted other forms of disclosure without customer consent, even encouraging disclosure for a list of approved purposes.[25] The Court had no difficulty finding that the Vermont law made a distinction between favored types of content, such as academic research, and disfavored forms of speech, such as direct marketing to physicians.

This speaker-based limitation on accesses is a far cry from the statute at issue here, which embodies the traditional quasi-contract common law duty preventing ***any*** disclosure to third parties without express permission, and prohibits ***any*** appropriation of the information for purposes other than those for which the customer or client disclosed the information. It is one thing for the state to provide protection of a traditional common law right or enforce a traditional implied quasi-contract claim. *See Cohen v. Cowles Media Co.*, 501 U.S. 663 (1991) (applying state law of promissory estoppel to newspaper to protect anonymity of story source). It is a wholly different matter for a law to apply such protection selectively based on viewpoint. It would be as if Maine passed a law saying, "an ISP shall not disclose personal information to a Democrat" or "an ISP shall only disclose personal information to a labor union." The discrimination against speaker and viewpoint in such a case would not lie in identifying the ISP as the subject of the privacy rule (especially in light of the history discussed above), but with identifying exceptions that have no rational relationship to the stated purpose of the statute. *See*

[25] *Sorrell*, 564 U.S. at 563-64.

National Amusements v. Town of Dedham, 43 F.3d 731, 738 (1st Cir. 1995) (strict scrutiny where differential treatment had no relationship to the underlying purpose).

To hold otherwise would be to subject a host of common law disclosure limitations to strict scrutiny under the First Amendment. Lawyer/client confidentiality is one of the oldest restrictions on speech imposed by the common law. Like the Maine ISP privacy statute, it prohibits a lawyer from divulging information provided by a client for purpose of legal representation. Like the common law duty applicable to messenger services such as the telegraph and the telephone, this duty arises out of a combination of implied contract, moral outrage at the disclosure of highly confidential information, and an equitable protection against unjust enrichment from appropriating information disclosed by a client for express purpose of receiving a promised service. But to operate, the lawyer/client confidentiality singles out lawyers engaged in legal practice, and those under their supervision. If complainants were to prevail on their strict scrutiny argument, lawyer/client confidentiality, doctor/patient confidentiality, and the restrictions on speech imposed on various fiduciaries such as trustees, members of corporate boards, and corporate officers would all be subject to strict scrutiny as a form of viewpoint discrimination.

For the same reason, permitting ISPs to use the information to market their communications related products does not raise a First Amendment concern. Since the traditional common law duty protected by the statute arises in part from implied contract, it follows that the contours of the law and its exceptions follow commercial expectations. Subscribers anticipate when they subscribe to an ISP that the ISP will periodically offer new products or offer to review their services with them in an effort to retain customers. The Maine ISP law, like its federal analog and other similar laws such as the VPPA, therefore permits the ISP to market to the

customer the sort of related communications products customers would expect. What customers do not expect, and what the law therefore does not allow, is that the ISP will use the information to market unrelated products. Not only does this go beyond the bounds of the common law quasi-contractual limitation, it raises significant concerns regarding unjust enrichment and unfairly advantages the ISP as against other, non-ISP competitors in the marketplace. As discussed above, preventing this sort of unfair competition and unjust enrichment was another significant component in the development of similar state laws and common law duties in the 19th Century with regard to telegraph operators.

Again, the analogy with lawyer/client confidentiality is helpful. As the Supreme Court has held, lawyers may refer clients to one another and directly advertise to potential clients. *Bates v. State Bar of Arizona*, 433 U.S. 350 (1977). But this right of a lawyer to propose a commercial transaction to a potential client does not void all other aspects of lawyer/client confidentiality, or subject them to strict scrutiny. Similarly, where the exceptions in the Maine ISP privacy statute arise either from a rational connection with the stated purpose or follow the traditional contours of the common law right the statute protects, they cannot trigger strict scrutiny.

C. The Conduct Prohibited by Statute Is Also Largely Non-Expressive Conduct, and Therefore Raises No First Amendment Interest.

Plaintiffs argue that even if the statute evades strict scrutiny, the Court should apply the "commercial speech" test under *Central Hudson Gas & Electric Corp. v. Public Service Commission*, 447 U.S. 557 (1980). This argument fails, however, because Plaintiffs fail to identify any expressive conduct prohibited by the Maine ISP privacy law, which is a precondition for applying any level of First Amendment analysis. Because the law permits ISPs

to advertise directly to their subscribers, their own speech is not impacted. What is impacted is either their non-expressive use of their customers' personal information, such as development of new products, or the sale of their customers' personal information to others so that these third parties can take advantage of the information.

It is axiomatic that to trigger First Amendment scrutiny, the conduct must be "intended to convey particularized message under circumstances in which the likelihood is great that the message would be understood by those to whom it was addressed." *Hennessy v. City of Melrose*, 194 F.3d 237, 246 (1st Cir. 1999) (internal quotes and citations omitted). The ISPs have not identified ***any*** message, let alone any particularized message or specific audience, they intend to express or to what audience they plan to express it. There is no *a priori* reason to consider the accumulation of facts with no desire to convey any particular message or express any "speech,"[26] particularly not where the party moving for a preliminary injunction has the burden of proof. Here, where Plaintiffs do not even pretend to care about the specifics of the data collected or its expressive content, it would be wrong to conclude that the Maine privacy statute triggers any First Amendment interest. Marble may be carved into a work of art, but that does not make the sale of marble an expressive act in and of itself. A law regulating the quarrying of data from one's subscribers is no more a burden on speech than a law regulating the quarrying of marble – even if this incidentally burdens would-be artists among the quarry's clients.

Sorrell makes this point explicitly:

> It is true that restrictions on protected expression are distinct from restrictions on economic activity or, more generally, on nonexpressive conduct. It is also true that the First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech. That is why a ban on race-based hiring may require

[26] *See generally* Richards,"Reconciling Data Privacy," 51 U.C. Davis. L. Rev. at 1168-74 (explaining 'sliding scale' of expressive activity and ranking trade in databases as non-expressive).

> employers to remove 'White Applicants Only' signs, why an ordinance against outdoor fires might forbid burning a flag, and why antitrust laws can prohibit agreements in restraint of trade.

Sorrell, 564 U.S. at 567 (citations and internal quotes omitted).

An analysis of cases finding a First Amendment interest under the comparable federal law, 47 U.S.C. § 222, underscores that, absent a clear burden on expressive conduct, there is simply no First Amendment matter at issue. *See Verizon California, Inc. v. FCC*, 555 F.3d 270 (D.C. Cir. 2009) (regulation prohibiting direct speech to customer); *NTCA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (assuming applications of *Central Hudson* because all parties stipulated to application of *Central Hudson*); *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999) (advertising non-communications related products). Accordingly, the provisions entirely unrelated to the ISPs' own speech – such as non-expressive use of subscriber information to develop products, or sale of subscriber information to third parties – raises no First Amendment question.

This court took a similar approach in *Catholic Charities of ME, Inc. v. City of Portland*, 304 F. Supp. 2d 77 (D. Me. 2004). There, Catholic Charities argued that a local ordinance requiring it to extend family employee benefits to registered domestic partners violated Catholic Charities' First Amendment right, since by withholding such benefits "it sends a message about Roman Catholic teachings on non-family relationships." *Id.* at 95. Observing that "not all conduct intended to express an idea can be labelled speech," this Court found that managing employee benefit funds was simply not "particularized" enough to qualify as protected expression. *Id.* Similarly, mere collection of information with the intent to somehow exploit it in the future cannot be considered "particularized" or "expressive" enough to warrant First Amendment scrutiny.

The only element of the Maine ISP privacy law that arguably raises a First Amendment question is the requirement of opt in consent for advertising by the ISP for its non-

communications related products. Even here, however, the link is highly tenuous and relies on the questionable reasoning of the 10th Circuit's 1999 decision in *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999). The *U.S. West* case has faced considerable criticism both for its failure to consider the importance of the common law right of privacy, *see NCTA v. FCC*, 555 F.3d at 1001, and because of its tenuous chain of reasoning between the activity restricted and the supposed speech interest. *See* Richards, *supra*, 52 U.C.L.A. L. Rev. 1150 (2005) at 1193-94.

The *U.S. West* court began its decision with a declaration of the need of the court to protect industry and innovation from "deference to agency action." *U.S. West*, 182 F.3d at 1228. It then proceeded to cast aside the legislative history of Section 222 in favor of its own speculation, ignoring the legislative intent to protect and enhance competition. *Id*. at 1229. The *U.S. West* court went on to invent a new First Amendment interest, the ability to "target" a specific audience by using its position as a messenger to whom individuals must expose information for a specific contractual purpose. *Id*. at 1232. Unsurprisingly, the *U.S. West* decision offered no prior precedent for this "targeting" rationale, relying on cases that dealt with direct speech in the form of advertising rather than on the ability to use information collected for one purpose to "target" customers for other purposes. The *U.S. West* court acted as if it were dealing with a blank slate, failing to address over 100 years of state and federal common law finding messengers contractually barred from using the information collected from customers for precisely this sort of unjust enrichment. Finally, the *U.S. West* court disparaged the entire concept of the common law and statutory rights of privacy in communications, stating that the only possible interest in protecting the information would be to protect subscribers from "embarrassment." *Id.* at 1235.

Even without the history discussed above, the *U.S. West* decision has not aged well. The considerable harms from the abuse of personal information collected by intermediaries has become abundantly clear in the more than 20 years since the 10th Circuit issued *U.S. West.* Most importantly, however, the First Circuit has never adopted the highly questionable First Amendment right to collect data for the purpose of "targeting" an audience outside the scope of the understood common law agreement between the parties, and contrary to the important purposes of protecting competition and preserving trust in the networks of communications providers. This Court should not do so for the first time here.

Finally, even if the court were to apply *U.S. West*, Plaintiffs would not be entitled to a preliminary injunction against enforcement of the statute. Non-expressive uses of customer data, including disclosure to third parties, raise no First Amendment concern. The only element here subject to even intermediate scrutiny under *U.S. West* would be an ISP using customer information to advertise its own non-communications related products. Given that Plaintiffs have provided no proof of how they are irreparably harmed by obtaining prior customer consent first, they fail to meet their burden for a preliminary injunction. Additionally, the only remedy they would be entitled to is an injunction requiring "opt out" consent rather than "opt in" consent."

In short, ISPs have failed to show that the statute impinges on any First Amendment conduct because ISPs primarily wish to use the information for non-expressive uses. The one real exception, advertising related products, is permitted under the statute. The Court here should reject the questionable First Amendment reasoning of *U.S. West* as unsupported and contrary to circuit precedent.

II. NO FEDERAL LAW PREEMPTS THE MAINE STATUTE

The starting point for any preemption analysis is "the basic assumption that Congress did not intend to displace state law," *Maryland v. Louisiana*, 451 U.S. 725, 746 (1981). When Congress does preempt states, "It may do so through express language in a statute... [or] through 'field' pre-emption or 'conflict' pre-emption." *Oneok, Inc. v. Learjet, Inc.*, 135 S. Ct. 1591, 1595 (2015).

Express preemption occurs when Congress explicitly preempts states with clear and unambiguous language. It is absent here. More than absent, the Communications Act explicitly preserves as complementary any additional existing common law or statutory remedies. 47 U.S.C. § 414. Federal district courts have held that this section explicitly preserves state privacy laws from preemption. *See Aronson v. Sprint, L.P.*, 90 F. Supp. 2d 662, 668 (W.D. Pa. 2000); *Ashley v. Southwestern Bell Tel. Co.*, 410 F. Supp. 1389, 1392 (W.D.TX 1976) ("the Communications Act does not purport to preempt state law in the area of remedies for invasion of privacy").

As discussed below, the Congressional Review Act rejection of the ISP Privacy Order cannot be given any preemptive effect, the Restoring Internet Freedom (RIF) Order, 33 FCC Rcd 311 (2017), neither conflicts with the Maine statute nor occupies the field of ISP privacy regulation, and it is possible for ISPs to comply with both the Maine statute and federal laws.

A. Congressional Review Act Rejection Carries No Preemptive Effect

Plaintiffs do not cite any support for their unique concept that the legislative vacatur of a federal law or regulation preempts states from stepping in to fill the gap, because there isn't any.

Plaintiffs contend that Congress came to a "judgment that an ISP-specific privacy regime is not in the public interest." Mot. for J. on the Pleadings with Incorporated Mem. at 18, *ACA v. Frey*, No. 1:20-cv-00055-LEW (D. Me.) (ISP Motion). But Congress did no such thing.

Congress's judgment in this case is that it "disapproves" the FCC's ISP Privacy Order, and that "such rule shall have no force or effect." Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017). A disapproval under the CRA simply makes it "as though such rule had never taken effect," 5 U.S.C. § 801, which as the FCC found merely brought back the status quo ante, including bringing back into force rules the ISP Privacy Order had itself repealed. 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. The Supreme Court "has observed repeatedly that pre-emption is ordinarily not to be implied absent an 'actual conflict.'" *English v. General Elec. Co.*, 496 US 72, 90 (1990). There is no "actual conflict" between the absence of an FCC ISP privacy regime and the presence of a state one because there is nothing for state law to conflict with. There is no preemptive "federal scheme" at all, including one of non-regulation. *Mozilla Corp. v. FCC*, 940 F.3d 1, 130-33 (D.C. Cir. 2019). Indeed, the lack of federal rules on this issue is precisely what creates room for the states. If Congress wanted to expressly prevent state lawmaking in this area it could have done so. Instead, it did the opposite. One could just as easily infer that Congress viewed the federal rules as insufficiently stringent.

This nullification was pursuant to the Congressional Review Act, which prevents agencies from reenacting the same rule that Congress had just disapproved. 5 U.S.C. § 801(b). It does not prohibit states from enacting rules on the same subject, Plaintiffs' use of the term "a fortiori" notwithstanding. As all CRA actions take the same form, Plaintiffs' position would necessitate that each successful CRA action impliedly preempts the states from enacting rules on the same subject matter, such as "Teacher Preparation Issues" and "Employer's Continuing

Obligation To Make and Maintain an Accurate Record of Each Recordable Injury and Illness."[27] Reading the CRA to create such broad and open-ended preemption would be contrary to the entire preemption jurisprudence that has existed thus far while eviscerating principles of federalism. The "teaching of this Court's decisions . . . enjoin[s] seeking out conflicts between state and federal regulation where none clearly exists." *Huron Portland Cement Co. v. Detroit*, 362 U. S. 440, 446 (1960). Plaintiffs' argument must therefore be rejected.

B. The Restoring Internet Freedom Order Does Not Preempt State Privacy Laws

Plaintiffs attempt to argue that the FCC's RIF Order "carries the full preemptive force of federal law." ISP Motion 19. It does not. The DC Circuit has vacated the portion of the RIF Order that attempts to expressly preempt states from regulating broadband, finding that the Commission's voluntary abdication of broadband oversight did not constitute a "policy" that limits states from regulating in this area. *Mozilla Corp. v. FCC,* 940 F.3d 1, 130-33 (D.C. Cir. 2019). The RIF Order itself states that the FCC "return[s] jurisdiction to regulate broadband privacy and data security to the Federal Trade Commission." ¶ 181. The ISPs do not explain how the FCC can preempt in an area where it concededly has no jurisdiction.

The best the ISPs can do is to point to the ISP transparency rule, observing in a footnote, ISP Motion 19 n.9, that despite *Mozilla* striking down the FCC's attempt to expressly preempt states, conflict preemption may still be possible for what remains of the RIF Order. But the transparency rule neither conflicts with state ISP privacy laws nor occupies the field. The RIF Order's transparency rule states,

---

[27] George Washington University Congressional Review Act Tracker, https://regulatorystudies.columbian.gwu.edu/sites/g/files/zaxdzs3306/f/downloads/CRA/GW%20Reg%20Studies_CRATracker_03.12.20.pdf.

> Any person providing broadband Internet access service shall publicly disclose accurate information regarding the network management practices, performance, and commercial terms of its broadband Internet access services sufficient to enable consumers to make informed choices regarding the purchase and use of such services and entrepreneurs and other small businesses to develop, market, and maintain Internet offerings. Such disclosure shall be made via a publicly available, easily accessible website or through transmittal to the Commission.

¶ 215. The FCC later explains that "commercial terms" includes privacy policies. ¶ 223. Maine's law would affect what the ISP's privacy policies could be. It does not conflict with the federal requirement that they disclose them. It is not "impossible for a private party to comply with both state and federal requirements," *English v. General Elec. Co.*, 496 US 72, 79 (1990), and does not stand as an "obstacle" to transparency reporting. Id. (citing *Hines v. Davidowitz*, 312 U. S. 52, 67 (1941)).[28]

Beyond extended discussion on why the FCC neither can nor should regulate broadband privacy, the RIF order contains little discussion of privacy otherwise, which is perhaps why the ISPs cite as a "determination" of the FCC a sentence about "tilting the playing field against ISPs" ISP Motion 19 (citing RIF Order ¶ 140), that has nothing to do with privacy at all. This minimal disclosure requirement and thin discussion of an area where the FCC has conceded it has no authority to regulate cannot rise to the level of a "scheme of federal regulation... so pervasive as to make reasonable the inference that Congress left no room for the States to supplement it." *Rice v. Santa Fe Elevator Corp.*, 331 US 218, 230 (1947).

C. It is not Impossible for an ISP to Comply with Both Federal and State Law Here

[28] At most, the FCC's "full purposes and objectives" are that the FTC and not the FCC should be the federal broadband privacy enforcer. This would imply that if any agency were to attempt to preempt the states with respect to broadband privacy it would have to be the FTC, assuming it had the legal authority to do so. But this question is moot as it has not done so. The FCC's belief that some other agency might have the authority to preempt states in an area where it claims to lack jurisdiction cannot itself be given preemptive effect.

Plaintiffs claim that the Maine statute prohibits them from "using" customer billing addresses for the purposes of complying with FCC Form 477 reporting requirements. But Form 477 does not require that billing addresses be disclosed, and the internal tallying of subscriber counts does not constitute the prohibited "use" of customer billing addresses. The word "use" in the context of this statute—accompanied by "disclose, sell or permit access"—implies a measure of third-party disclosure not present here, not mere internal use. *See U.S. v. Williams*, 553 U.S. 285, 294 (2008) (the meaning of a word is "narrowed by the commonsense canon of *noscitur a sociis* — which counsels that a word is given more precise content by the neighboring words with which it is associated."). Neither have Plaintiffs described how Form 477 requires the disclosure of information "pertaining to a customer that is not customer personal information" at all. As the FCC's detailed guidance makes plain, Form 477 only requires the disclosure of coarse-grained information pertaining to the availability of services in locations such as census blocks.[29]

Plaintiffs' argument that compliance with civil discovery is not permitted by the Maine statute is false, as compliance with discovery procedures is mandatory and ultimately subject to "court order." 35-A M.R.S. § 9301(4)(C).

Finally, to the extent that any FCC requirements do require disclosure or use of subscriber information, there is still no conflict that requires even a partial preemption analysis, as complying with federal law is "necessary to the provision of such service." 35-A M.R.S. § 9301(4)(A).

[29] FCC, Instructions for Filings as of December 31, 2019, https://us-fcc.app.box.com/v/Form477Instructions. This information does not "pertain" to individual subscribers.

III. CONCLUSION

Public Knowledge respectfully asks that the Court deny the Plaintiffs' motion for judgment on the pleadings. The statute is constitutional, is not preempted by federal law, and Maine should not be barred from enforcing it.

Dated at Portland, Maine this 1st day of June, 2020.

/s/ Russell B. Pierce, Jr.
Russell B. Pierce, Jr., Esq.
Attorney for *Amicus Curiae*
Public Knowledge

NORMAN, HANSON & DeTROY, LLC
Two Canal Plaza
P.O. Box 4600
Portland, ME 04112-4600
(207) 774-7000
rpierce@nhdlaw.com

John Bergmayer (*pro hac vice* pending)
Legal Director
Public Knowledge
1818 N St. NW, Suite 410,
Washington DC 20036
(202) 861-0020
john@publicknowledge.org

Of Counsel:

Harold Feld
Senior Vice President
Public Knowledge
1818 N St. NW, Suite 410
Washington DC 20036
(202) 861-0020
hfeld@publicknowledge.org

Sara Collins
Policy Counsel

Public Knowledge
1818 N St. NW, Suite 410
Washington DC 20036
(202) 861-0020
sara@publicknowledge.org

CERTIFICATE OF SERVICE

I, Russell B. Pierce, Jr., attorney for *Amicus Curiae* Public Knowledge, hereby certify that on June 1, 2020, I electronically filed the above BRIEF OF PUBLIC KNOWLEDGE AS *AMICUS CURIAE* SUPPORTING DEFENDANT as Exhibit 1 to the Motion of Public Knowledge for Leave to file Brief as Amicus Curiae, with the Clerk of Court using the CM/ECF system which will send notification of such filing to all persons registered for ECF in this matter.

/s/ Russell B. Pierce, Jr.
Russell B. Pierce, Jr., Esq.

NORMAN, HANSON & DETROY, LLC
Two Canal Plaza
P. O. Box 4600
Portland, Maine 04112-4600
Telephone: (207) 774-7000
rpierce@nhdlaw.com