UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

ACA CONNECTS – AMERICA'S COMMUNICATIONS ASSOCIATION, *et al.*, *Plaintiffs*, v. AARON FREY, in his official capacity as Attorney General of the State of Maine, *Defendant*.	Civil Action No. 1:20-cv-00055-LEW

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF MAINE, ELECTRONIC FRONTIER FOUNDATION, AND CENTER FOR DEMOCRACY AND TECHNOLOGY IN SUPPORT OF DEFENDANT'S OPPOSITION TO JUDGMENT ON THE PLEADINGS

Emma Bond
Zachary L. Heiden
ACLU Foundation of Maine
PO Box 7860
Portland, ME 04112
207.619.6224
zheiden@aclumaine.org
Counsel for Amici Curiae

Of Counsel:

Vera Eidelman
Arianna Demas
ACLU Foundation
125 Broad Street, 18th Fl.
New York, NY 10004
212.549.2500
veidelman@aclu.org

Adam Schwartz
Andrew Crocker
Kit Walsh
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109
415.436.9333
adam@eff.org

Emma Llansó
Center for Democracy & Technology
1401 K St NW, Ste 200
Washington, DC 20005
202.637.9800
ellanso@cdt.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union (ACLU) is a nationwide, nonprofit, nonpartisan organization with nearly 2 million members and supporters. The ACLU of Maine is a state affiliate of the ACLU. Both organizations are dedicated to defending the principles embodied in the Constitution and our nation's civil rights laws and, for decades, have been at the forefront of efforts nationwide to protect the full array of civil rights and liberties, including the rights to free speech and privacy. The ACLU and the ACLU of Maine have frequently appeared before courts throughout the country in First Amendment cases, both as direct counsel and as amici curiae.

The Electronic Frontier Foundation (EFF) works to ensure that technology supports freedom, justice, and innovation for all the people of the world. EFF is a non-profit organization with more than 30,000 members. EFF regularly advocates in courts and legislatures in support of free speech, data privacy, and other rights on the Internet.

The Center for Democracy and Technology (CDT) is a non-profit public interest organization. For more than 25 years, CDT has represented the public's interest in an open, decentralized internet and worked to ensure that the constitutional and democratic values of free expression and privacy are protected in the digital age. CDT's team has deep knowledge of issues pertaining to the internet, privacy, security, technology, and intellectual property, with backgrounds in academia, private enterprise, government, and civil society. This diversity of experience allows CDT to translate complex policy into action: it convenes stakeholders across the policy spectrum, advocates before legislatures and regulatory agencies, and helps educate courts.

[1] Amici confirm that no party or counsel for any party authored this brief in whole or in part, that no person other than amici or their counsel made any monetary contribution intended to fund the preparation or submission of this brief, and that both parties consent to the filing of this brief.

The ACLU, ACLU of Maine, EFF and CDT are each dedicated to both free speech and data privacy on the Internet. As such, the application of the correct First Amendment scrutiny to consumer data privacy laws is of immense concern to amici, their civil rights and civil liberties clients seeking justice, and their members and donors.

SUMMARY OF ARGUMENT

Our use of the Internet reveals deeply private information about us, from the contents of our communications to details about our finances, health, and exact location. Companies that sell broadband information access services (BIAS), including Plaintiffs, are uniquely positioned to surveil us and collect this information. BIAS providers have a proven track record of privacy-invasive practices, yet we have no choice but to rely on them for access to the Internet. And in much of the country, particularly in Maine, we have little, if any, choice among them. These realities pose a serious threat to our digital privacy, which in turn implicates our willingness to speak freely and our ability to remain secure, both online and in the physical world.

Maine's "Act to Protect the Privacy of Online Customer Information" (the Privacy Act) aims to address those threats by giving users control over how BIAS providers use and disseminate their personal information. Specifically, the Privacy Act requires BIAS providers to obtain a customer's opt-in consent before using or disclosing "customer personal information" (CPI), which includes (1) a customer's personally identifying information, such as billing information and social security number, and (2) information derived from a customer's use of broadband service, such as browsing history, application use, precise geolocation, financial and health information, device identifiers, and contents of communications. 35-A M.R.S. § 9301(1)(C).

As a regulation of the use and dissemination of information, the Privacy Act is a regulation of speech that is subject to First Amendment scrutiny. Specifically, as a regulation of

"expression related solely to the economic interests of the speaker and its audience," *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 561 (1980), that concerns "no public issue," *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc*., 472 U.S. 749, 762 (1985), the law is subject to intermediate scrutiny.

Because it is narrowly drawn to directly advance Maine's substantial interests in protecting consumers' privacy, freedom of expression, and security, the Act easily survives such scrutiny. The law aims squarely at its target: information derived from BIAS use, which is both sensitive and personal, and accessible to BIAS providers, who are uniquely positioned to surveil us and face little if any market pressure to do otherwise. Moreover, the law does not fully prohibit the disclosure of customers' personal information; it merely requires consent first—directly addressing the security and privacy problem of loss of control over one's information.

This First Amendment challenge is neither novel nor meritorious. Courts around the country have rejected such challenges to similar laws after applying intermediate scrutiny. *See, e.g.*, *Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996, 1001–02 (D.C. Cir. 2009); *Trans Union Corp. v. FTC* (*Trans Union I*), 245 F.3d 809, 819 (D.C. Cir. 2001); *Trans Union Corp. v. FTC (Trans Union II)*, 267 F.3d 1138, 1140–41 (D.C. Cir. 2001); *Trans Union LLC v. FTC* (*Trans Union III*), 295 F.3d 42, 52–53 (D.C. Cir. 2002); *Boelter v. Hearst Commc'ns, Inc.* (*Boelter I*), 192 F. Supp. 3d 427, 450–51 (S.D.N.Y. 2016) (Torres, J.); *Boelter v. Advance Magazine Publishers Inc.* (*Boelter II*), 210 F. Supp. 3d 579, 602 (S.D.N.Y. 2016) (Buchwald, J.); *King v. Gen. Info. Servs., Inc*., 903 F. Supp. 2d 303, 306–07 (E.D. Pa. 2012). Those opinions should guide the Court in denying Plaintiffs' Motion for Judgment on the Pleadings (MJP).

ARGUMENT

I. The Privacy Act is a regulation of speech subject to Central Hudson scrutiny.

The Privacy Act restricts the ability of BIAS providers to use, disclose, sell, and provide access to customers' personal information. This "creation and dissemination of information [is] speech within the meaning of the First Amendment." *Sorrell v. IMS Health, Inc*., 564 U.S. 552, 568, 570 (2011).

But not all speech warrants 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). Similarly, "speech solely in the individual interest of the speaker and its specific business audience" that concerns "no public issue" warrants "reduced constitutional protection." *Dun & Bradstreet,* 472 U.S. at 762 & n.8.

Courts around the country have applied this logic to hold that, while regulations akin to the Privacy Act regulate speech, they are not subject to strict scrutiny. Instead, they must satisfy the *Central Hudson* test for commercial speech that is neither illegal nor misleading: "The State must assert a substantial interest to be achieved by [the] restriction[ ]" and the restriction must "directly advance" and be "narrowly drawn" to that interest. *Cent. Hudson*, 447 U.S. at 564–65.

The D.C. Circuit has applied *Central Hudson* scrutiny to a requirement that telecommunications carriers obtain customers' opt-in consent before disclosing information "relating to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer," *Nat'l Cable & Telecomms.,* 555 F.3d at 997, 1000 (quotation marks omitted), and to restrictions on financial institutions sharing, and recipients using, information "obtained by a financial institution in connection with

providing a financial product or service to a consumer." *Trans Union III*, 295 F.3d at 50, 52–53. *See also Trans Union II*, 267 F.3d at 1140–41 (invoking the commercial speech doctrine to conclude that consumer reports produced by consumer reporting agencies merit intermediate scrutiny). District courts have similarly applied *Central Hudson* intermediate scrutiny to a state law limiting "the sellers of certain products," including videos, "from disclosing the identity of individuals who purchase those products" to third parties, *Boelter I*, 192 F. Supp. 3d at 445–46; *Boelter II*, 210 F. Supp. 3d at 597, and to regulations of consumer reports, *King*, 903 F. Supp. 2d at 307.

The Supreme Court's decision in *Sorrell v. IMS Health*, 564 U.S. 552, does not change this analysis. Although *Sorrell* considered a law that regulated disclosure of private information obtained through commercial transactions, that law banned disclosure only to a very specific set of speakers seeking to communicate a very specific message: pharmaceutical "detailers—and only detailers" using the information to "effective[ly] . . . market[ ] . . . brand-name drugs." *Id.* at 564–65. "In its practical operation, [the] law [went] even beyond mere content discrimination, to actual viewpoint discrimination." *Id.* at 565 (quotation marks omitted). The Supreme Court held that the law violated the First Amendment because it "was too narrowly targeted at certain speakers who were but a minority of those able to acquire or use the protected information," the restriction "advanced the state's interest only indirectly," and "most importantly, the government created a 'regulation of speech because of disagreement with the message it conveys.'" *Boelter I*, 192 F. Supp. 3d at 450 (quoting *Sorrell*, 564 U.S. at 572–73, 576–79).

None of those defects is present here: as discussed below, the Privacy Act is narrowly tailored to actors who are uniquely positioned to violate consumers' privacy and does not distinguish on the basis of message or viewpoint. After *Sorrell*, courts have applied *Central*

Hudson intermediate scrutiny to consumer privacy laws that, like the Privacy Act, do not share the defects of the law at issue in *Sorrell*. *Id.* (rejecting application of *Sorrell* to law governing dissemination of video rental records); *King*, 903 F. Supp. 2d at 308–09 (same for law governing dissemination of consumer reports because it "ha[d] nothing to do with the federal government trying to tilt the public debate in order to favor one form of speech over another" (quotation marks omitted)). *See also Nat'l Fire Adjustment Co., Inc. v. Cioppa*, 357 F. Supp. 3d 38, 45 (D. Me. 2019) (applying *Central Hudson* to a regulation of commercial speech notwithstanding plaintiff's argument that law's content-based and speaker-based distinctions required greater scrutiny under *Sorrell*).

The Privacy Act, like the laws considered in *Boelter* and *King*, regulates information on matters of private concern that businesses obtain about consumers through their commercial transactions, and that is related solely to the economic interests of those businesses and their audience. Further, it is not viewpoint-based. Thus, the Privacy Act is subject to *Central Hudson* scrutiny.

II. Maine has substantial interests in protecting users from BIAS provider surveillance.

Maine easily satisfies the first prong of *Central Hudson* scrutiny. It has substantial interests to be achieved by the Privacy Act—protecting consumers' privacy, speech, and information security.

Privacy interests. There is "no doubt" that the state's interest in protecting "the consumer's right to privacy . . . is substantial." *Trans Union I*, 245 F.3d at 818 (citation omitted). Indeed, the Supreme Court has recognized "the interest in individual privacy" as one "of the highest order." *Bartnicki v. Vopper*, 532 U.S. 514, 518 (2001).

Here, each of the categories of information about broadband usage that constitute CPI under the statute reveals sensitive private details about individuals' lives. Courts routinely hold that individuals have a reasonable expectation of privacy in their browsing histories, precise geolocation information, and the content of their communications. *See, e.g.*, *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 603 (9th Cir. 2020) (expectation of privacy in browsing history); *Riley v. California*, 134 S. Ct. 2473, 2490 (2014) ("Internet search and browsing history . . . could reveal an individual's private interests or concerns."); *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (geolocation information "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations" (quotation marks omitted)); *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010) (emails reveal everything from "sweet nothings" and "ambitious [business] plans" to "purchases" and "[doctor's] appointments").).

Courts have also recognized the sensitivity of the types of financial and medical information that can be derived from BIAS use. *See, e.g.*, *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1269 (9th Cir. 1998) ("One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health or genetic make-up."). *See also Sorrell*, 564 U.S. at 557 (noting that "it can be assumed" that a state's interest in "safeguard[ing] medical privacy" is "significant"). And those categories of information are also specifically protected by statute in various contexts. *See* Section III.A, *infra*.

Although identifiers like Internet Protocol (IP) and Media Access Control (MAC) addresses do not directly identify specific people, these identifiers can be—and are—used to

track users' movements and compile records of their interactions with others, generating mosaics from discrete tiles of information that together reveal a fuller picture.[2]

Courts have recognized the government's "substantial interest in protecting the privacy of customer information" when rejecting First Amendment challenges to other consumer privacy laws, including information derived from consumers' use of telecommunications services, *Nat'l Cable & Telecomms.*, 555 F.3d at 1000, and consumers' video rental, book purchase, and magazine subscription histories. *Boelter I*, 192 F. Supp. 3d at 445; *Boelter II*, 210 F. Supp. 3d at 597–98. *See also King*, 903 F. Supp. 2d at 309–10 (same for information in consumer credit reports). The state's interest in protecting information derived from individuals' BIAS use is equally, if not more, substantial and it will only grow as "[a]dvances in technology . . . increase the potential for unreasonable intrusions into personal privacy." *In re Facebook Internet Tracking Litig.*, 956 F.3d at 599 (quotation marks omitted). *See also Kyllo v. United States*, 533 U.S. 27, 33–34 (2001) (privacy protections must account for "the advance of technology").

Speech interests. Maine has a substantial interest in protecting users' speech that relies on privacy. As the Supreme Court explained in *Bartnicki v. Vopper*, "the fear of public disclosure of private conversations might well have a chilling effect on private speech." 532 U.S. at 532–33. Ensuring privacy allows for uninhibited speech. "In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger . . . can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas." *Id.* (quoting *President's*

[2] *See* Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, EFF (2019), https://www.eff.org/wp/behind-the-one-way-mirror.

Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 202 (1967), available at https://www.ncjrs.gov/pdffiles1/nij/42.pdf).

The free speech value of privacy is also reflected in the First Amendment's longstanding protection of the right to speak anonymously. *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995). The right to withhold information (*i.e.*, the author's own name) is an aspect of privacy that advances speech, because "identification and fear of reprisal might deter . . . discussions of public matters of importance." *Talley v. California*, 362 U.S. 60, 65 (1960). *See also Watchtower Bible & Tract Soc'y v. Village of Stratton*, 536 U.S. 150, 166–67 (2002).

Information security interests. The state also has a substantial interest in protecting users' information security. By limiting the ability to sell such information without user consent, the law lowers the incentives for BIAS providers to amass troves of information, which are an inherent security hazard, as they can be subject to data breaches and employee misuse.[3] In the words of the D.C. Circuit, the existence of this threat is a matter of "common sense." *Nat'l Cable & Telecomms.*, 555 F.3d at 1001–02.

In addition, by ensuring that personal information is not used or disclosed without a user's consent, the law gives individuals control over their data, which is essential for information security. Those who seek to purchase CPI "are presumably interested in [it] for a reason: knowing what someone reads"—or does and consumes online—"may not only reveal

[3] Tara Siegel Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. Times (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html; Erik Ortiz, *Marriott Says Breach of Starwood Guest Database Compromised Info of Up to 500 Million*, NBC News (Nov. 30, 2018), https://www.nbcnews.com/tech/security/marriott-says-data-breach-compromised-info-500-million-guests-n942041;Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. Times (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

one's interests but also permit predictive inferences as to income level, marital status, and other lifestyle facts," all of which raise security concerns. *See Boelter II*, 210 F. Supp. at 599. Even identifiers that cannot necessarily be used on their own to identify an individual, like IP and MAC addresses, can enable someone to identify a specific person when combined with other information. This allows attackers to associate a given Internet traffic pattern, or browsing history, with a specific identity.[4] Likewise, Internet use patterns can give attackers a window into our personal lives—exposing, for example, when we are home and when we are not.

Disclosure of such information also facilitates phishing attacks by making it easier for an attacker to tailor its message to the receiver. Further, because many services allow a password reset based on personal information (*e.g.*, mother's maiden name), CPI in the wrong hands can enable fraudulent access.[5]

III. The Privacy Act directly advances and is narrowly drawn to Maine's substantial interests.

The Privacy Act also satisfies the second half of the *Central Hudson* test: it directly advances, and is narrowly drawn to, each of the state's substantial interests. To satisfy this prong, "[t]he government does not have to show that it has adopted the least restrictive means for bringing about its regulatory objective; it does not have to demonstrate a perfect means–ends fit; and it does not have to satisfy a court that it has chosen the best conceivable option." *Nat'l*

[4] *See, e.g.*, Dara Kerr, *Your Web Browsing History Is Totally Unique, Like Fingerprints*, CNET (Aug. 1, 2012), https://www.cnet.com/news/your-web-browsing-history-is-totally-unique-like-fingerprints/; Łukasz Olejnik, Claude Castelluccia & Artur Janc, *Why Johnny Can't Browse in Peace: On the Uniqueness of Web Browsing History Patterns*, in Proceedings of the 5th Workshop on Hot Topics in Privacy Enhancing Technologies (2012), available at https://petsymposium.org/2012/papers/hotpets12-4-johnny.pdf.

[5] *See, e.g.*, Kristen Kozinski & Neena Kapur, *How to Dox Yourself on the Internet*, NYT Open (Feb. 27, 2020), https://open.nytimes.com/how-to-dox-yourself-on-the-internet-d2892b4c5954.

Cable, 555 F.3d at 1002. "The only condition is that the regulation be proportionate to the interests sought to be advanced." *Id.*

The Privacy Act is tailored to the harms it addresses. It regulates BIAS providers—actors who are uniquely positioned to cause the harms the Act is meant to protect against. And it directly addresses the problem of individuals' losing control over their personal information by returning control to them in the form of consent, rather than by prohibiting the dissemination entirely.

A. The Privacy Act is tailored to specific commercial actors.

Far from triggering strict judicial scrutiny, as Plaintiffs insist, *see, e.g.*, MJP at 11, the Privacy Act's exclusive focus on BIAS providers reflects the legislature's tailoring to its specific interests. Legislatures routinely enact consumer data privacy laws on a sector-specific basis without violating the First Amendment. And that approach is highly appropriate in the BIAS context because (1) everyone needs broadband to get to the Internet, (2) BIAS providers have unique power to surveil their customers, (3) many people do not have a choice among providers, and (4) BIAS providers have a long history of violating their customers' privacy. As with other consumer privacy laws that have survived First Amendment scrutiny, the Privacy Act "aim[s] directly at its intended target": the mosaic of personal information that can be derived from BIAS use. *See Trans Union II*, 267 F.3d at 1142. *See also Nat'l Cable & Telecomms.*, 555 F.3d at 1001. "The law limits the dissemination of precisely the kind of information with which the state is concerned, and targets those most likely to disseminate it." *Boelter II*, 192 F. Supp. 3d at 449.

1. Many consumer data privacy laws are sector-specific.

Many consumer data privacy laws are sector-specific, applying to particular entities only. For example, the Cable Privacy Act, 47 U.S.C. § 551, and the Video Privacy Protection Act, 18

U.S.C. § 2710, limit how cable operators and video service providers, respectively, may process the personal information of their customers. But neither law applies to other kinds of businesses that also deliver movies to consumers. Likewise, the Health Insurance Portability and Accountability Act, 45 C.F.R. § 160, and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, apply to defined entities that process, respectively, health information and financial information. But other kinds of entities that process the same types of information are not covered. *See also, e.g.*, the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 (regulating just consumer reporting agencies); the Telecommunications Act, 47 U.S.C. § 222 (regulating just telecommunications carriers); the Stored Communications Act, 18 U.S.C. § 2701 (regulating just electronic communication services and remote computing services); and the Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (regulating just websites).

Under Plaintiffs' theory of the case, courts have erred in routinely applying intermediate scrutiny in First Amendment challenges to such sector-specific consumer data privacy laws. *See, e.g.*, *Trans Union I*, 245 F.3d 809 (applying intermediate scrutiny to FCRA regulations of how credit reporting agencies, but not other businesses, sell mailing lists); *Nat'l Cable & Telecomms.*, 555 F.3d 996 (same for Telecommunications Act regulations of how phone companies, but not other communication services, process communications metadata). But courts are correct to do so where, as here, the regulated sector threatens unique privacy harms.

2. BIAS providers are uniquely situated to invade customers' privacy and evade market discipline.

People use the Internet to learn, and to share their most intimate thoughts. It is essential that they be able to speak and learn safely online, without unwanted intrusion from the carrier they pay to simply transfer their information. A customer must entrust a BIAS provider to carry their online communications—much like UPS or FedEx carry physical packages or letters. This

unique position gives BIAS providers the opportunity to rifle through customers' online lives. Such privacy invasions would be deeply troubling if done by FedEx or UPS, and they are all the more troubling when conducted by BIAS providers, for several reasons.

First, robust competition simply does not exist for broadband Internet service, particularly in Maine. For high-speed broadband, most Americans have one option, if any, and the statistics are even more dire for less densely-populated areas. In the most rural 25 percent of the country, 93.1 percent of Americans have at most a single option for high-speed (250 Mbps) broadband Internet, and the next quartile of rural areas is little better, at 77.6 percent.[6] Even in the densest 25 percent of the country, a majority of Americans do not have access to competition for broadband.[7] And even for the slowest speed that is still considered broadband (25 Mbps), a majority of Maine residents have only one option.[8] At a more modern speed of 100 Mbps, an overwhelming 91 percent of Maine residents are left without any choice.[9] Maine ranks 42nd in the nation for Internet access, according to the most recent *U.S. News* study.[10]

Second, even in the unusual case where a consumer can choose between two BIAS providers, switching is expensive and time-consuming. It's not a matter of driving to the UPS

[6] FCC Communications Marketplace Report, FCC 18-181, at 102 Fig. D-10 (Dec. 2018). This report systematically overestimates service availability by classifying a service as 'available' throughout an entire census block if even one address is served. *Id.* at 128 ¶ 242.

[7] *Id.* at 102 Fig. D-10.

[8] FCC, Fixed Broadband Deployment Area Summary: Maine (June 2019), https://broadbandmap.fcc.gov/#/areasummary?version=jun2019&type=state&geoid=23&tech=acfow&speed=25_3&vlat=45.23384563389331&vlon=-68.98468600000001&vzoom=5.409724731019012. Broadband of this quality is essential to many modern uses of the Internet, such as multi-party video conferencing, high-quality streams, and transferring large bodies of data for journalism, research, or personal uses.

[9] *Id.*

[10] *Infrastructure Rankings*, U.S. News and World Report, https://www.usnews.com/news/best-states/rankings/infrastructure.

store next time instead of the FedEx store. A technician must be scheduled to physically connect and disconnect wires or even run new ones, particularly in the rural markets that make up much of Maine. This may require customers to miss work, and to pay new installation fees. Thus, even in the rare case when it's possible to switch, and even if the competitor has better privacy practices than the incumbent, the costs of switching insulates the incumbent from market pressure.

Third, once a user subscribes to a BIAS provider, that provider sees everything that goes in and out of their devices, and if the user switches to another BIAS provider, that provider will instead. A user's BIAS provider is the only one that carries packets to and from their computer; it is the gatekeeper that controls the last segment of wire (or wireless connection) linking the user to the broader Internet. No matter how much competition there is, the provider will always be able to gather a uniquely complete picture of the user's Internet use. Even when a user encrypts their web traffic to protect its content, the BIAS provider can see which web servers they visit to exchange encrypted content. Because of BIAS providers' privileged position as the carrier of a user's data, they are also able to track even those consumers who enable privacy-protecting browser plugins that defend against third-party tracking.

Courts have upheld other consumer privacy laws that target businesses because they are in uniquely privacy-invasive positions. For example, "given consumer reporting agencies' unique access to a broad range of continually-updated, detailed information about millions of consumers' personal credit histories, . . . it [is] not at all inappropriate for Congress to have singled out consumer reporting agencies for regulation." *Trans Union I*, 245 F.3d at 819 (quotation marks omitted). *See also Boelter I*, 192 F. Supp. 3d at 449. Likewise here, given BIAS providers' unique access to a plethora of information about consumers' Internet usage, from the

websites they visit to the communications they send, Maine's decision to single them out for regulation does not violate the First Amendment as underinclusive, or heighten the necessary level of scrutiny; rather, it shows that the law is narrowly drawn.

3. BIAS providers have a long history of violating customer privacy.

The Privacy Act's narrow fashioning is further supported by recent history showing that BIAS providers do not respect user privacy unless they are legally required to do so. As far back as 2008, Charter Communications, one of the largest BIAS providers in Maine, tested the idea of recording everything their customers did online into profiles using Deep Packet Inspection technology (the digital equivalent of opening all of a resident's incoming and outgoing packages to snoop around). The company relented only after bipartisan condemnation from Congress.[11]

In 2011, BIAS providers engaged in "search hijacking" in coordination with a company called Paxfire, monitoring customers' Internet search queries in order to reroute them, thereby exposing private search information and redirecting traffic to commercial affiliates instead of connecting the subscriber with the search engine they requested.[12] Other invasive efforts include AT&T's tampering with Internet traffic to insert ads, tracking technology, and code into websites requested via their network.[13] Even small rural BIAS providers have engaged in ad injection to advertise on behalf of third parties.[14]

[11] Press Release, *Markey, Barton Raise Privacy Concerns About Charter Communications* (May 16, 2008), https://www.markey.senate.gov/news/press-releases/may-16-2008-markey-barton-raise-privacy-concerns-about-charter-comm.

[12] Christian Kreibech, et al., *Widespread Hijacking of Search Traffic in the United States*, EFF (Aug. 4, 2011), https://www.eff.org/deeplinks/2011/07/widespread-search-hijacking-in-the-us.

[13] Jonathan Mayer, *AT&T Hotspots: Now with Advertising Injection*, Web Policy Blog (Aug. 25, 2015), http://webpolicy.org/2015/08/25/att-hotspots-now-with-advertising-injection.

[14] *See, e.g.*, Phillip Dampier, *ISP Crams Its Own Ads All Over Your Capped Internet Connection; Banners Block Your View*, Stop The Cap! (Apr. 3, 2013),

BIAS providers also manipulate the software in the devices they sell. For example, AT&T, Sprint, and T-Mobile preinstalled "Carrier IQ" on their phones, which gave them the capability to track everything users did with those phones, from the websites they visited to the applications they used.[15] The carriers abandoned the practice only after a class-action lawsuit.[16]

Perhaps most egregiously, in 2014 Verizon tagged every one of its mobile customers' HTTP connections with a semi-permanent "super-cookie," which it used to enable third parties such as advertisers to target individual customers.[17] This "super-cookie" allowed unaffiliated third parties to track an individual, no matter what steps users took to preserve their privacy. AT&T followed suit but quickly retreated after Verizon faced an FCC enforcement action.[18]

Even in the face of the 2015 Title II Open Internet Order, which applied communications privacy law to the industry until it was repealed by the current administration, BIAS providers continued to collect and sell private customer information. In 2015, BIAS providers partnered with SAP's Consumer Insight 365 to "ingest" data from cellphones close to 300 times a day

http://stopthecap.com/2013/04/03/isp-crams-its-own-ads-all-over-your-capped-internet-connection-banners-block-your-view.

[15] Marcia Hofmann, *Carrier IQ Tries to Censor Research With Baseless Legal Threat*, EFF (Nov. 21, 2011), https://www.eff.org/deeplinks/2011/11/carrieriq-censor-research-baseless-legal-threat.

[16] *In re Carrier IQ, Inc. Consumer Privacy Litigation*, Case No. 12-md-023330 - EMC, available at http://www.carrieriqsettlement.com (detailing the terms of the settlement).

[17] Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls*, EFF (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh.

[18] Federal Communications Commission, FCC Settles Verizon "Supercookie" Probe, Requires Consumer Opt-in for Third Parties: Verizon Wireless to Obtain Affirmative Consent from Consumers Before Sending Unique Identifier Headers to Third Parties, available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-338091A1.pdf.

every day across 20 to 25 million mobile subscribers.[19] That data has been used to inform retailers about customer browsing info, geolocation, and demographic data.

Since then, BIAS providers' privacy promises have been issued to *sound* reassuring. But they narrowly define the information they promise to protect, leaving highly personal information such as browsing history and app usage up for grabs.[20] Even in areas with a degree of competition between carriers, BIAS providers have abused their position to invade customers' privacy. The danger is all the greater in Maine, where even those modest competitive pressures are lacking for most customers. This history highlights the necessity of legal protections like those provided by the Privacy Act.

B. The Privacy Act's opt-in consent requirement is narrowly drawn to Maine's substantial interests.

The Privacy Act's requirement of opt-in consent to use or disclose customer personal information is narrowly drawn to directly advance Maine's interests in privacy, speech, and information security. As courts have recognized, "the individual's control of information concerning his or her person" lies at the center of our privacy rights. *DOJ v. Reporters Comm.*, 489 U.S. 749, 763 (1989). And the Act fixes the problem of users' lost control over their personal information by simply returning it to them. "The [law's] means and ends are thus one, leaving no possibility of a careless or imperfect 'fit.'" *Trans Union II*, 267 F.3d at 1143.

In addition, this approach to regulating BIAS providers' speech "is not absolute: the statute allows disclosure of identifying information . . . with a consumer's consent[.]" *Boelter I*,

[19] Kate Kaye, *The $24 Billion Data Business That Telecos Don't Want to Talk About*, AdAge (Oct. 26, 2015), http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058/.

[20] Jeremy Gillula & Kate Tummarello, *Hollow Privacy Promises from Major Internet Service Providers*, EFF (Apr. 18, 2017), https://www.eff.org/deeplinks/2017/04/major-internet-service-providers-privacy-promises-ring-hollow.

192 F. Supp. 3d at 449. This, too, shows that the law is narrowly drawn. *See Boelter II*, 210 F. Supp. 3d at 602 (holding that consumer privacy law is "sufficiently narrowly drawn" when "it permits disclosure for any reason with the customer's permission").

Many other consumer data privacy laws likewise require businesses—including cable providers, 47 U.S.C. §§ 551(b)(1) & (c)(1), video tape providers, 18 U.S.C. § 2710(b)(2), and telecommunication carriers, 47 U.S.C. § 222—to obtain opt-in consent before processing their consumers' personal information. And numerous cases have upheld such requirements against First Amendment challenge. *See, e.g., Nat'l Cable & Telecomms.*, 555 F.3d at 1001–02 (upholding FCC rule under the Telecommunications Act requiring opt-in consent to disclose customer proprietary network information, included who called whom and when, to third-party marketers); *Trans Union I*, 245 F.3d at 819 (upholding FTC rule under the FCRA requiring opt-in consent to sell targeted marking lists of names and addresses of people who meet particular credit history criteria); *Boelter I*, 192 F. Supp. 3d at 450–51 (upholding state law requiring opt-in consent for a magazine company to sell subscribers' personal information); *Boelter II*, 210 F. Supp. 3d at 602 (upholding different state law requiring same).

In doing so, the courts squarely rejected the argument Plaintiffs present here that an opt-in requirement fails intermediate First Amendment scrutiny because it is more burdensome for BIAS providers than an alternative opt-out scheme would be. Opt-out is only "marginally less intrusive" than opt-in, *Nat'l Cable & Telecomms.*, 555 F.3d at 1002 (quotation marks omitted), and the existence of "some alternative solution [that] is marginally less intrusive" does not void the rule. *Boelter I*, 192 F. Supp. 3d at 450. Under *Central Hudson* scrutiny, legislatures "ha[ve] no obligation to choose the least restrictive means of accomplishing its goal." *Trans Union I*, 245

F.3d at 819. *See also Boelter II*, 210 F. Supp. 3d at 602 (the restraint need not be "absolutely the least severe that will achieve the desired end" (citation omitted)).

Moreover, while an opt-in requirement may be marginally more burdensome for BIAS providers, it is far *less* burdensome for Internet users and therefore more directly advances the state's interests in the Privacy Act. Empowering consumers to opt-out of their BIAS providers' use and disclosure of their personal information is not an adequate substitute for empowering them to decide whether to opt-in, because most consumers simply do not change the defaults of the technology they use.[21] *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), an older case that Plaintiffs urge this Court to follow, *cf.* MJP at 14—and which *National Cable*, *Trans Union I, Boelter I*, and *Boelter II* all refused to follow—did not address this reality.

Many users who strongly wish to protect their privacy may be deterred by an opt-out requirement. Users may lack technical knowledge or be unaware of the option to change a default. Or they may be too busy. As the dissent in *U.S. West* persuasively argued, "the opt-out method simply does not comply with [the statute's] requirement of informed consent. In particular, the opt-out method, unlike the opt-in method, does not guarantee that a customer will make an informed decision. … To the contrary, the opt-out method creates the very real possibility of 'uninformed' customer approval." *U.S. West*, 182 F.3d at 1246–47. "The [law]'s opt-in consent scheme presumes that consumers do not want their information shared unless they expressly indicate otherwise; an opt-out scheme … presumes the opposite." *Nat'l Cable & Telecomms.*, 555 F.3d at 1002. The Maine legislature properly chose the former: a default that respects consumers' desire to protect their privacy.[22]

[22] Equally, the Act is not under-inclusive or content-based merely because it allows use of customer information without opt-in consent for limited purposes, including for responding to a

CONCLUSION

For the foregoing reasons, the Court should deny Plaintiffs' Motion for Judgment on the Pleadings.

Date: May 28, 2020

Respectfully Submitted,

/s/ Emma E. Bond
Emma E. Bond
/s/ Zachary L. Heiden
Zachary L. Heiden
ACLU Foundation of Maine
PO Box 7860
Portland, ME 04112
207.619.6224
zheiden@aclumaine.org
Counsel for Amici Curiae

Of Counsel:

Vera Eidelman
Arianna Demas
ACLU Foundation
125 Broad Street, 18th Fl.
New York, NY 10004
212.549.2500
veidelman@aclu.org

Adam Schwartz
Andrew Crocker
Kit Walsh
Electronic Frontier Foundation

customer's call for emergency services. "[T]his differentiation simply recognizes that . . . privacy interests in personal information are 'defined not only by the content of the information, but also by the identity of the audience and the use to which the information may be put.'" *Boelter II*, 210 F. Supp. 3d at 601 (quoting *Trans Union II*, 267 F. 3d at 1143). The same is true for the law's opt-out approach to BIAS providers using or disclosing non-CPI, which the State views as less private. And, because it is information BIAS providers gather through their relationship with customers, Dkt. 28 at 6, the opt-out requirement is also narrowly drawn to directly advance the state's interests. Finally, the law's requirement that BIAS providers not refuse service, charge a penalty, or withhold a discount if a consumer withholds consent, 35-A M.R.S. § 9301(3)(B), is needed to protect the consumer's right to autonomously decide whether to consent. Otherwise, BIAS providers could use economic pressure to extract phony "consent." This would create a society of privacy "haves" and "have nots," because some customers are less able than others to pay a privacy premium.

815 Eddy St.
San Francisco, CA 94109
415.436-9333
adam@eff.org

Emma Llansó
Center for Democracy & Technology
1401 K St NW, Ste 200
Washington, DC 20005
202.637.9800
ellanso@cdt.org