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* ACCESS NOW AND NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

Of Counsel:

Eric Null
Access Now
P.O. Box 20429
Greeley Square Station
4 East 27th Street
New York, NY 10001-9998
(802) 578-7223
eric@accessnow.org

Sharon Bradford Franklin
Ross Schulman
Christine Bannan
New America's Open Technology Institute
740 15th Street, NW, Suite 900
Washington, DC 20005
202-986-2700
franklin@opentechinstitute.org
ross@opentechinstitute.org
bannan@opentechinstitute.org

Sigmund D. Schutz
Preti Flaherty Beliveau & Pachios LLP
P.O. Box 9546
Portland, ME 04112-9546
(207) 791-3000
sschutz@preti.com

Laura M. Moy, *Pro Hac Vice*
Counsel of Record
Michael Rosenbloom
Lindsey Barrett
Of Counsel
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue NW
Suite 312
Washington, DC 20001
(202) 662-9547
laura.moy@georgetown.edu
Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

RULES

CASES

STATUTES

OTHER AUTHORITIES

INTERESTS OF *AMICI CURIAE*[1]

Access Now is a non-profit organization that defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, Access Now fights for human rights in the digital age. Access Now provides policy recommendations to the public and private sectors to ensure the Internet's continued openness and universality, and filed comments in the broadband privacy proceeding at the Federal Communications Commission in 2016.[2] Access Now is non-partisan, not-for-profit, and not affiliated with any government, corporation or religion.

New America's Open Technology Institute ("OTI") works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. New America is a Washington, D.C.–based think tank and civic enterprise committed to renewing American politics, prosperity, and purpose in the Digital Age. OTI works to ensure that the Internet remains an open forum that protects users' rights to privacy and free expression. This includes promoting broadband privacy at the federal level and in many states, including Maine. OTI filed

---

[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.

[2] Comments of Access Now, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Dkt. 16-106, May 27, 2016, https://ecfsapi.fcc.gov/file/60002078011.pdf.

comments in the broadband privacy proceeding at the Federal Communications Commission in 2016.[3]

Access Now and New America's OTI are both pro-privacy advocacy organizations that are committed to ensuring that communications networks and technologies are widely accessible and well trusted so that speech can flourish on the Internet.

SUMMARY OF ARGUMENT

Amici file this brief to offer a technical explanation of what information Internet service providers ("ISPs") have access to and how and why that information implicates privacy concerns. This brief is intended to assist the Court in understanding the context in which the challenged Maine statute is situated, and in particular some of the ways in which ISPs occupy a distinct position in Internet commerce.

ISPs sit in a privileged position. As gatekeepers to the Internet—an essential communications network and arguably the world's richest such network—ISPs are privy to a great deal of information regarding their customers' private online activities and communications. Everything a person does online must be funneled through the customer's ISP. Whether a customer is online to read and conduct research, to do their banking, to search for a job, to search for a soulmate, to monitor their child sleeping in another room, to turn their coffee maker on, or to check on their house when they're out

[3] Comments of New America's Open Technology Institute, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Dkt. 16-106, May 27, 2016, https://ecfsapi.fcc.gov/file/60002081381.pdf.

of town, the customer is dependent on an ISP to route their online data and commands to countless other parties.

The information that customers must share with their ISPs exposes intimate details of customers' private lives. Simple observation or more complex analysis of customers' online data can reveal details about the customer's health status, financial circumstances, children and family life, employment status, sleep and wake cycles, personal grooming habits, romantic and sexual preferences and activities, political viewpoints, and more. Due to the rich nature of Internet traffic data, the declining cost of long-term data storage, and the increasing power of computer-assisted data analysis, details that fall into the classic "sensitive" categories of health, financial, and children's information often can be inferred even from information that does not obviously pertain to those categories.

Customers cannot reasonably avoid sharing details of their private lives with ISPs. In the modern world, having an Internet connection—which requires forming a relationship with an ISP—is a necessity, not a luxury. In addition, customers often have only one or very few options when it comes to selecting an ISP, and once a customer has selected an ISP, it is very difficult to switch to a different one for a variety of reasons.

Without regulatory intervention, customers who wish to protect their privacy of their own information vis-a-vis their ISP are generally out of luck. The existence of widespread encryption does not alleviate privacy concerns because even with widespread encryption, ISPs still have access to extremely rich data about their customers' lives. The fact that customers sometimes switch from one device to another

does not alleviate privacy concerns, because ISPs still handle their customers' online traffic across multiple devices. Some customers who wish to shield certain details from their ISP may choose to route all of their online traffic through a "virtual private network," or VPN, but this is technically difficult to do, slows down one's connection considerably, and is not a viable solution for the average customer.

ARGUMENT

I. ISPs have access to a wealth of information about how their customers use the Internet

By virtue of their role as gatekeepers to the Internet, ISPs have access to a wealth of information about how their customers use the Internet.[4] Every single thing that an Internet user does online—from filing taxes, to checking a connected thermostat, to completing a book report, to dating—involves the transfer of data mediated by the user's ISP. Because of their role transmitting online communications, ISPs necessarily have access to details about when those communications take place, for how long, with whom, and of what volume. The information that customers of broadband service must share with their providers can reveal details about customers' private lives.

A. Customers' use of the Domain Name System reveals private details

Broadband providers typically have access to their customers' "Domain Name System," or "DNS," queries, which reveal highly private information. As users browse the Internet, their computers and mobile devices silently and constantly use the DNS like a phonebook for the Internet. This is because Internet traffic doesn't go directly to web addresses—also called "domain names"—such as "www.canceradvocacy.org" or "www.rocketmortgage.com"; instead, it navigates to IP addresses like "139.162.208.40" or "13.249.44.124." Connected devices typically are configured to use their ISP's DNS server by default to look up the correct IP addresses for users' online activities. The

[4] *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. Ill. L. Rev. 1417 (2009).

typical residential user's every online action therefore registers a query of the ISP's DNS server.[5]

Put more plainly, as users browse websites pertaining to their medical status, political viewpoints, romantic and sexual interests, financial status, and more, they necessarily expose all of these visits to their ISP via DNS lookups. Logging these queries and performing some sort of analysis on them is trivial and likely already done. Indeed, ISPs have long monitored their customers' DNS queries for security purposes.[6]

Adding to the potentially invasive nature of such monitoring, the increasing rate at which websites are encrypted does not protect users from DNS monitoring. Even when websites are encrypted, DNS queries typically are not.

B. IP addresses and other traffic metadata reveal private details

Even if a user were able to obscure DNS queries from their ISP, the user would still expose to their ISP a great deal of private information about all websites and online services that they patronized. This is because the user would still need to share with their provider the IP addresses of all their Internet traffic. Referring back to the example provided above, the ISP would still be capable of observing that the user communicated

---

[5] Neil J. Rubenking, *How (and Why) to Change Your DNS Server*, PCMag (May 17, 2019), https://www.pcmag.com/how-to/how-and-why-to-change-your-dns-server ("Your home network typically relies on a DNS Server supplied by your ISP.").

[6] *See* Aaron Rieke et al., *What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate* 6 (2016), https://perma.cc/L3RV-TSEQ ("In fact, ISPs already do monitor user DNS queries for valid network management purposes, including to detect potential infections of malicious software on user devices.") [hereinafter *What ISPs Can See*]; *see generally* Paul Hoffman, *Local and Internet Policy Implications of Encrypted DNS* 7 (Apr. 30, 2020), https://perma.cc/EJY3-SWWB ("One frequent reason for DNS filtering is to prevent malicious actors from attacking network users.").

with "139.162.208.40" or "13.249.44.124," even if the provider no longer sees "www.canceradvocacy.org" or "www.rocketmortgage.com." This information may seem more innocuous, but the reality is that IP addresses alone are almost just as revealing as domain names. Computer science researchers recently demonstrated that IP addresses alone can reveal the sites that an individual visits with great specificity because "over 95% of sites have a unique set of [IP addresses]."[7] Furthermore, IP address ranges strongly correlate with particular locations or organizations and therefore reveal that information to ISPs.[8]

Customers' typical use of broadband service further exposes private details via the timing, frequency, and duration of their communications with websites and online services. For example, a weekly hour-long visit to "thesundaymass.org" reveals key information about a user's religion, biweekly visits to "acecashexpress.com" reveals information about a user's financial status, and a sudden burst of visits to "suicidepreventionlifeline.org" reveals information about a user's mental health.

In addition to IP addresses, users communicating over the Internet commonly reveal other forms of information through metadata wholly accessible to their ISP. For instance, when connecting to another device on the internet, the connection is made

---

[7] Simram Patil & Nikita Borisov, *What Can You Learn from an IP?*, *in* ACM Applied Networking Research Workshop 45, 50, https://perma.cc/5DNQ-BUZP.

[8] For example, the IP addresses listed at https://db-ip.com/as557 are assigned to the University of Maine System, and contacting any of those IP addresses reveals a connection to the University. Additionally, all IP addresses in the 171.64.*.* range are assigned to Stanford University, so repeated connections to addresses in that range associates the user with Stanford. *Stanford University List of IP Addresses*, DB-IP.com, https://db-ip.com/as32 (last visited May 30, 2020).

through a numbered "port." ISPs can see which ports a user connects through, and the usage of certain ports can reveal a whole range of specific information about a user's behavior, because different programs typically use different port numbers. For example, port 1194 is commonly used by the OpenVPN protocol,[9] and port 8019 is used by Intuit's Quickbooks accounting software.[10]

From its privileged position as Internet gatekeeper, an ISP is technically capable of combining IP address information and other metadata like timing, frequency, duration, and port number, which would permit a savvy party to generate a finely-tuned profile of the totality of a customer's Internet usage.

C. Information about connected devices reveals private details

ISPs can also learn private details about their customers' lives from the devices that customers have connected to the network. Because all devices that a customer connects to the Internet send and receive data via the ISP, ISPs frequently have the technical ability to infer what types of devices the customer operates in the privacy of their own home based on the behavior of those devices. As the "Internet of Things" grows, the personal information that customers expose via their connected devices grows as well.

---

[9] OpenVPN, *How To Guide: Set Up and Configure OpenVPN Client/Server VPN*, https://openvpn.net/community-resources/how-to/ (last visited May 31, 2020).
[10] *Set Up Firewall and Security Settings for QuickBooks Desktop*, QuickBooks Community, https://quickbooks.intuit.com/learn-support/en-us/access-data-remotely/set-up-firewall-and-security-settings-for-quickbooks-desktop/00/201468 (last visited May 31, 2020).

The mere presence of certain types of devices on a customer's home network can reveal private details about that person. For example, the presence of a connected hearing assistive device in one customer's home indicates that the customer likely is deaf or hard of hearing; the presence of a customer's connected baby monitor indicates that the customer likely has a baby or small child.

In addition, the amount of private information exposed by customers' connected devices is growing alongside the so-called "Internet of Things," or "IoT," in which everyday items are gradually being replaced by connected versions with new features. Homes today often feature a wide variety of connected devices, including baby monitors, door locks, children's toys, toothbrushes, and sex toys.

Beyond the presence of a connected device in a customer's home, much can be learned about a customer's private life by studying the timing, volume, and patterns of traffic to and from those devices. As then–FTC Commissioner Julie Brill pointed out in 2015, "[e]ven if an ISP just looks at the IP addresses to which you connect and the time at which connections occur, it can get an intimate portrait of your interests, daily rhythms, habits—as well as those of all members of your household."[11] Brill also noted that data exposed to ISPs "will become even more detailed and voluminous" as the Internet of Things expands.[12]

---

[11] Julie Brill, Comm'r, Fed. Trade Comm'n, *Net Neutrality and Privacy: Challenges and Opportunities* 6, Keynote Address at Georgetown Institute for Public Representation and Center for Privacy and Technology Symposium on Privacy and Net Neutrality (Nov. 19, 2015), *available at* https://perma.cc/R4ND-A7E7.

[12] *Id.*

In 2018 two journalists conducted an experiment to test this and found that monitoring the Internet traffic of a smart home could indeed reveal intimate details of its inhabitants' lives. The online traffic patterns of one journalist and her family revealed "what time they wake up, when they turn their lights on and off, when their child wakes up and falls asleep [and] when [the journalist] brushes her teeth."[13]

D. There is no clear distinction between "sensitive" and "non-sensitive" categories of personal information

In light of the fact that ISPs have access to enormous amounts of customer information revealing highly private details of people's lives, the Privacy Act wisely steers clear of applying the terms "sensitive" and "non-sensitive" to ISP customers' private information. As Defendants note in their Opposition, the Privacy Act does "identif[y] categories of data warranting different levels of protection," consistent both with FCC past practice and with other privacy laws, rendering the use or avoidance of the term "sensitive" little more than semantic. In addition, however, it is appropriate to move away from use of the term "sensitive"—and to adopt an expansive definition of information deserving of opt-in protection—because in the modern era there is no bright line technical distinction between information that is sensitive and information that is not.

One reason it is difficult to distinguish sensitive from non-sensitive information is because classically sensitive information about health, finances, and children can be

[13] Surya Mattu & Kashmir Hill, *The House that Spied on Me*, Gizmodo (Feb. 7, 2018), https://gizmodo.com/the-house-that-spied-on-me-1822429852.

inferred from other, more mundane information. For example, as explained above, the fact that a person has a connected hearing assistive device can reveal that the person is deaf or hard of hearing. And the fact that the person has a connected hearing assistive device may not be disclosed directly by the customer, but instead be revealed because the customer routinely sends data to and from an IP address associated with the device vendor or because the device has a unique identifier that falls within a range of identifiers assigned to the device vendor.[14] This means that a party collecting network data, such as an ISP, may not describe the data in its possession as health data, even though it is.

Similarly, in the experiment described above conducted by two journalists, online traffic patterns revealed information about one journalist's child, including when the child woke up and went to sleep. But until it was analyzed to reveal those details, the data would not have been understood to be descriptive of a child's sleep and wake patterns, even though it plainly contained that information. Nor would it be obvious that logs maintained of the destination IP addresses and times of a customer's online

[14] For example, MAC addresses beginning with 84-77-78 are assigned to a company called Cochlear Limited, which only makes hearing assistance devices. *See List of MAC Addresses by Company*, IEEE, http://standards-oui.ieee.org/oui/oui.txt (last visited May 30, 2020); *True Wireless Cochlear Implant Accessors*, Cochlear, https://www.cochlear.com/us/en/home/products-and-accessories/our-accessories/true-wireless-range (last visited May 30, 2020). It is not clear that ISPs can always access the MAC addresses of their customers' connected devices; however, it is possible that ISPs may collect this information through network routers that they supply to their customers. *See* Michael Horowitz, *Avoid ISP Routers*, Router Security (June 4, 2015), https://perma.cc/P6BJ-XYXN ("Even without outside influence, an ISP may well put a backdoor in the devices they give to their customers..."); Harrison Sand, *Your ISP is Probably Spying On You*, Harrison's Sandbox (Feb. 14, 2018), https://perma.cc/J9AJ-CEWJ.

communications included information about the customer's financial status, but a search of those logs for IP addresses associated with payday or mortgage lenders could convert portions of those logs into financial data instantaneously.

Conducting the analysis necessary to convert seemingly meaningless lists of numbers and times into a treasure trove of private details is a trivial feat with modern technology. Digital storage is plentiful and computing power inexpensive. There was a time when, due to storage or computing limitations, a party could not, as a practical matter, make use of large amounts of data that could be used to make further inferences about the data subjects' lives. Today, however, there are few practical or technical limits that constrain a resourced party's ability to retain data for a long time and apply powerful mining techniques to it to extract valuable details.

It is also difficult to distinguish between sensitive and non-sensitive data because there is no consensus regarding what types of information should be considered sensitive and what should not. In 2012, upon processing the public comments of numerous stakeholders, the FTC concluded that "at a minimum," the "sensitive" distinction extended to data about children, financial and health information, Social Security numbers, and certain geolocation data, because commenters were in broad agreement that at least these types of information were sensitive.[15] The FTC noted, however, that some commenters would extend the sensitive distinction to far more, such as information related to race, religious beliefs, ethnicity, sexual orientation,

[15] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change* 47 n. 214, 58 (2012), https://perma.cc/J2YL-LPMC ("FTC Privacy Report").

biometrics, genetics, and consumers' online communications or reading and viewing habits.[16] The FTC stated that it was "cognizant . . . that whether a particular piece of data is sensitive may lie in the 'eye of the beholder' and may depend upon a number of subjective considerations."[17]

Indeed, the FTC itself has somewhat expanded its definition of sensitive data since the 2014 report. In 2017 the FTC filed a complaint (which it later settled) against television vendor Vizio for spying on customers' viewing habits. The FTC's complaint alleged that television viewing activity is sensitive and therefore subject to an opt-in consent requirement. Complaint at ¶ 32, Fed. Trade Comm'n v. Vizio, Inc. (D.N.J. Feb. 6, 2017) (2:17-cv-00758).

There are times when a particular group of individuals may consider sensitive a category of information that the majority of people do not. For example, many people would not consider a user's movie ratings to be sensitive. But in a 2009 privacy class action brought against Netflix, the class representative was a person who alleged that her Netflix viewing record revealed her sexual orientation. According to the complaint, "were her sexual orientation public knowledge, it would negatively affect her ability to pursue her livelihood and support her family and would hinder her and her children's ability to live peaceful lives...." Complaint at ¶ 76, *Doe v. Netflix, Inc.* (N.D. Cal. Dec. 17, 2009) (Co9-05903).

[16] *Id.* at 59.
[17] *Id.*

Based on consumer research, it is also clear that people find far more information to be sensitive than just that which falls into the traditional definition of sensitive. According to a survey conducted by Pew Research Center in 2014, among the categories of information that respondents considered to be very or somewhat sensitive were the phone numbers they had called or texted (75%), their relationship history (71%), and the websites they had visited (70%).[18]

Perhaps because of the difficulty distinguishing between sensitive and non-sensitive information, when the FCC promulgated its federal broadband privacy rule in 2016, it declared customers' web browsing and application usage history, and their functional equivalents, sensitive.[19] In fact, the FCC's existing privacy regulations pertaining to phone carriers do not distinguish between sensitive and non-sensitive information.[20]

II. Customers cannot reasonably avoid sharing details of their private lives with ISPs

Not only is the information to which ISPs enjoy privileged access highly private, but customers cannot reasonably avoid exposing this data to their ISP. To gain access to the Internet, subscribers must connect through an ISP. Individuals cannot simply connect their own devices to the Internet; rather, they must pay another party for

---

[18] Mary Madden, *Americans Consider Certain Kinds of Data to Be More Sensitive than Others*, Pew Research Center (Nov. 12, 2014), https://perma.cc/66F8-T8ZT.
[19] Report and Order, *Protecting Privacy of Customers of Broadband and Other Telecommunications Services*, Dkt. 16-106, 81 Fed. Reg. 87274 (Jan. 3, 2017), 31 FCC Rcd 13911, 13982 ¶ 181 (Nov. 2, 2016).
[20] FCC Customer Proprietary Network Information Rule, 47 C.F.R. §§ 64.2001–64.2011 (2017); 47 U.S.C. § 222.

access. They cannot route their own online traffic either; instead, they must rely on an ISP to route traffic from Point A to Point B at their request.[21]

A. Broadband customers lack a choice of provider

Internet connectivity is widely understood to be an essential service, meaning that customers cannot simply forgo the service due to privacy concerns. Indeed, according to a survey Cumberland County, Maine conducted of its residents in 2019, 85% strongly agree that Internet service is "as important as electricity and telephone service."[22]

Nor can customers escape ISPs that engage in particularly privacy-violative practices. Not only must customers go through *some* ISP to get online, they often have insufficient choice with respect to *which* ISP to use because the broadband market lacks competition. According to updates to the FCC's *2018 Communications Marketplace Report*, by the end of 2018 over 30% of all Americans, rising to two-thirds of rural Americans, still had fewer than two options for a provider of 25 Mbps/3 Mbps fixed broadband

[21] Recent developments in encryption of DNS queries ("DNS Over HTTPS" or "DoH") do not significantly reduce user dependency on an ISP, as not only are the resulting queries still made over the ISP's network, but DoH is also very new and not in common use. *See* Ross Schulman, *DNS Over HTTPS: The Big Privacy Win Behind this Acronym Soup*, New America (Nov. 18, 2019), https://www.newamerica.org/oti/blog/dns-over-https-big-privacy-win-behind-acronym-soup.

[22] Cumberland County, *Cumberland County Broadband Playbook* 99 (2019), https://perma.cc/U3RM-MFW4.

service.[23] In a significant number of cases, broadband customers therefore will not be able to switch providers to avoid privacy violative practices.

Even in markets in which consumers may theoretically choose from among multiple available ISPs, high switching costs make it difficult to exercise the choice between providers.[24] Broadband customers wishing to switch from one provider to another face multiple barriers.[25] First, there may be significant financial costs, in terms of canceled contracts, installation fees, or bundle discount.[26] Second, these customers may have to invest a substantial amount of time and effort in the form of finding a new provider, installing new equipment, or taking time off of work to wait for technicians to come to their home.[27] Third, even if a customer wishes to switch and is prepared to do so, a lack of certainty that a new provider will be better may discourage the customer from actually going through with the switch..[28] These factors all create strong incentives for customers to stay at their current provider, removing any potential benefits of competition over privacy practices.

---

[23] *FCC Releases Certain Data Updated as of December 31, 2018 for the Communications Marketplace Report*, 35 FCC Rcd 1479 (2020), https://us-fcc.app.box.com/s/tijhz8cupitst0kg4l8c81dtzdyyduu9.

[24] Barbara van Schewick, *Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like* 36 (2012), https://perma.cc/67EY-FTD5 ("Switching costs in the market for Internet services are substantial. . . . . Further, switching providers may require a customer to invest a significant amount of time and effort.").

[25] Report and Order on Remand, Declaratory Ruling, and Order, *Protecting and Promoting the Open Internet,* Dkt. 14-28, 30 FCC Rcd 5601, 5631-32 ¶ 81 (Mar. 12, 2015) ("2015 Open Internet Order"); *see generally* Robert Kenny & Aileen Dennis, *Consumer Lock-in for Fixed Broadband* (2013), https://perma.cc/2AVM-G7R3.

[26] 2015 Open Internet Order at ¶ 81.

[27] Kenny & Dennis, *supra* note 25, at 27.

[28] *Id*. at 7.

B. Widespread encryption is not sufficient to alleviate privacy concerns

Even though there is a general trend toward websites adopting encryption to protect the contents of visitors' communications and activities online, this offers insufficient protection for privacy vis-a-vis ISPs. This contradicts Plaintiffs' assertion that "[w]idespread encryption is 'pervasively limiting the ability of ISPs to see Internet activity.'" Compl. ¶ 26 (citing Peter Swire, et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* 25, Alston & Bird LLP (Feb. 29, 2016), https://b.gatech.edu/2Hn2ULi).[29]

Contrary to Plaintiffs' argument, ISPs enjoy privileged access to their customers' private lives even as encryption becomes more popular. As described by technologists back in 2016,

> Even with HTTPS, ISPs can still see the domains that their subscribers visit. This type of metadata can be very revealing, especially over time. And ISPs are already known to look at this data—for example, some ISPs analyze DNS query information for justified network management purposes, including identifying which of their users are accessing domain names indicative of malware infection.[30]

In addition, the authors observed,

> Encrypted Internet traffic itself can be surprisingly revealing. In recent years, computer science researchers have demonstrated that network operators can learn a surprising amount about the contents of encrypted traffic without breaking or weakening encryption. By examining the features of network traffic—like the size, timing and destination of the encrypted packets—it is possible to uniquely identify

[29] The plaintiffs' source for their claim is a 2016 policy report substantially funded by Broadband for America, an industry association that counts three of the four plaintiffs among its members.

[30] *What ISPs Can See*, *supra* note 6, at 1.

> certain web page visits or otherwise obtain information about what the traffic contains.[31]

Encryption provides critical safeguards for users' privacy. However, encrypting the *contents* of network communications, as HTTPS does, does not meaningfully conceal other important information from ISPs seeking to collect it, and it cannot substitute for legal privacy protections.

C. Switching devices offers customers insufficient privacy protection

The fact that broadband customers today often use multiple connected devices also does not sufficiently protect their privacy. Again citing the same 2016 industry-funded paper mentioned above, Plaintiffs assert that because customers frequently switch between multiple devices, ISPs are afforded "mere episodic glimpses of a customer's Internet usage." Compl. ¶ 27 (internal quotation omitted). But this argument, too, misses the mark—and was responded to back in 2016 by credible parties. As computer science professor Nick Feamster then explained,

> [A] user's increased mobility by no means implies that a single ISP cannot track users' activities in their homes. Our previous research has shown that the traffic that users send in their home networks—typically through a single ISP—reveals significant information about user activity and behavior. The median home had about five connected devices at any give [sic] time. Simply by observing traffic patterns (i.e., without looking at any packet contents), we could determine the types of devices that users had in their homes, as well as how often (and how heavily) they used each device. In some cases, we could even determine when the user was likely to be home, based on diurnal traffic usage patterns. We could determine the most popular domains that each home visited.[32]

---

[31] *Id.* at 1–2.

[32] Nick Feamster, *What Your ISP (Probably) Knows About You*, Freedom to Tinker (Mar. 4, 2016), https://perma.cc/88Q6-2Y46.

If anything, having two ISPs makes the privacy problem worse. Instead of sharing private information, such as websites visited, with one ISP, the customer must share that information with two ISPs. A person may begin researching a disease they may have on their commute home from work, and then switch to their home computer to engage in more research. Having multiple ISPs actually compounds the privacy problem, rather than somehow solving it, as Plaintiffs appear to argue.

D. "Virtual private network" technology is no substitute for substantive privacy protections

It is possible, in theory, for broadband users to conceal some of their own information from ISPs using a "virtual private network," or VPN; however, the technical skills, inconvenience, and resources required to do so are beyond most users. Even sophisticated users may accidentally reveal details to their ISP when using a VPN, as the quality of VPN varies widely.

A VPN conceals a customer's information from their ISP by routing all of the customer's network traffic through an encrypted connection to a third party. An ISP can detect the connection between a customer using a VPN and the VPN provider, but cannot examine the same metadata that it otherwise could collect.

Although VPNs can help protect the privacy of their users, VPNs have significant downsides and do not constitute a scalable solution for broadband privacy. First, VPNs are not widely understood by the average user. To use a VPN, a customer must know what a VPN is, seek one (of over a hundred options) that they are confident is privacy protective, subscribe to a VPN service, and install and use specialized VPN

software. Second, VPNs typically charge subscription fees, requiring users to pay more on a monthly basis beyond the fees they already pay to ISPs. Third, use of a VPN significantly slows down everything a user does online, because traffic routed through a VPN must first travel through the VPN's potentially distant servers before making its way to its destination. Fourth, VPNs only conceal network activity if they are properly configured to do so—something that a user must have sufficient technical knowledge and discipline to do so well and consistently. Finally, VPNs only prevent ISPs from collecting data on their users because the VPN is put in the position to be able to collect that data instead, raising many of the very same privacy issues. The use of a VPN merely changes who can collect this broad swath of information.

CONCLUSION

Amici urge the Court to recognize the distinctly privileged position in which ISPs are situated and the highly private details to which ISPs have access. *Amici* respectfully ask the Court to deny Plaintiffs' Motion for Judgment on the Pleadings. Without regulatory intervention, customers who wish to protect their privacy of their own information vis-a-vis their ISP will not be able to do so.

Filed: June 1, 2020

Respectfully submitted,

/s/ Sigmund D. Schutz
Preti Flaherty Beliveau & Pachios LLP
P.O. Box 9546
Portland, ME 04112-9546
(207) 791-3000
sschutz@preti.com

/s/ Laura M. Moy
Laura M. Moy, *Pro Hac Vice*
Counsel of Record
Michael Rosenbloom
Lindsey Barrett
Of Counsel
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue NW
Suite 312
Washington, DC 20001
(202) 662-9547
laura.moy@georgetown.edu
Counsel for Amici Curiae

Of Counsel:

Eric Null
Access Now
P.O. Box 20429

Greeley Square Station
4 East 27th Street
New York, NY 10001-9998
(802) 578-7223
eric@accessnow.org

Sharon Bradford Franklin
Ross Schulman
Christine Bannan
New America's Open Technology Institute
740 15th Street, NW, Suite 900
Washington, DC 20005
202-986-2700
franklin@opentechinstitute.org
ross@opentechinstitute.org
bannan@opentechinstitute.or