Perspectives from FSF Scholars
April 9, 2020
Vol. 15, No. 17

Maine's ISP-Only Privacy Law Will Not Protect Consumers

by

Andrew Long *

Introduction and Summary

In June 2019, Maine enacted a privacy law that applies onerous and poorly defined limitations on the use of customer data exclusively to broadband Internet service providers (ISPs). Websites and apps with substantially greater access to individuals' personal information – and significantly higher shares of total digital advertising revenues – are exempt. So, too, are offline businesses. Should this statute survive judicial challenge and become effective later this year, it will harm Maine residents by failing to protect their privacy interests and by impeding competition in the Internet ecosystem.

There are two things that are true about the online experience. One is that Internet traffic does not recognize political boundaries. The other is that so-called "edge providers," such as Google, Facebook, Amazon, Netflix, eBay, and LinkedIn, vastly overshadow ISPs in the digital advertising marketplace. A state-level law that restricts the use of personal information by ISPs, but not edge providers, therefore cannot serve as an effective – or, for that matter, constitutional – tool to protect consumer privacy.

Nevertheless, Maine adopted Legislative Document (L.D.) 946, a law that requires broadband ISPs – and *only* broadband ISPs – to obtain "opt-in" consent before using a wide range of both sensitive and non-sensitive customer personal information. Of as much concern, it allows customers to "opt-out" from ISP use of what is *not* customer personal information, a category it neglects to define. The Maine law is scheduled to go into effect on July 1, but a group of trade associations representing ISPs have gone to court to prevent that from happening.

As those trade associations explain convincingly in their complaint, L.D. 946 is riddled with constitutional infirmities. For one thing, it implicates the First Amendment by discriminating between similarly situated speakers: ISPs are constrained in their ability to engage in commercial and non-commercial speech, while edge providers and offline businesses are not. For another, it runs afoul of the Supremacy Clause: both (1) Congress, through a joint resolution invalidating ISP-only FCC privacy rules, and (2) the FCC itself, through the regulatory reclassification of broadband access of an "information service" subject to FTC privacy oversight, have expressed a clear federal policy preference for even-handed treatment of all participants in the Internet ecosystem. Finally, numerous provisions of the statute (for example, the definitions of personal and non-personal consumer information) are so vague that they raise concerns under the Due Process Clause of the Fourteenth Amendment.

But it is not necessary to resort to legal arguments, however compelling they might be, to get to the heart of why L.D. 946 is so misguided. The basic facts of the digital advertising marketplace themselves tell the story. Compared to ISPs, edge providers have greater access to personal data, receive far more digital advertising dollars, and are the subject of vastly more FTC privacy-related enforcement actions. In addition, as a technical matter, the increasingly widespread adoption of encryption by websites and browser vendors limits the visibility that ISPs have into the online activity of their subscribers.

Below I will take you through a hypothetical "connected adventure" I constructed in order to highlight how small of an impact this ISP-focused statute will have on the actual use of Maine residents' personal information. While at home, in her car, and at a local coffee shop, Jane D. Consumer utilizes a number of methods – a wireline ISP, a wireless ISP, and "free" Wi-Fi – to access a wide range of online content and services. However, the combination of encryption and L.D. 946's burdensome requirement to obtain "opt-in" consent in order to use even non-sensitive information greatly limit the ability of the two ISPs to see, and make use of, her browsing and app history.

In contrast, L.D. 946 in no way constrains the websites Jane accesses (in this scenario, Facebook and Amazon), the apps she uses (Google Maps and Instagram), or the brick-and-mortar coffee shop she visits from collecting and using the personal information that she generates – an amount of data that far exceeds that which the ISPs can access.

Thus, it is clear that, to the extent state lawmakers truly have concerns regarding the use of Maine residents' personal information, L.D. 946 inevitably comes up short. Meaningful oversight of consumer online privacy simply cannot be accomplished by a statute that unjustifiably targets only ISPs.

Maine's Privacy Law Improperly Discriminates Against Broadband ISPs and Includes Overly Vague Language that Renders Compliance Impractical

Last June, the Governor of Maine signed into law L.D. 946, "An Act To Protect the Privacy of Online Customer Information."[1] If it survives judicial scrutiny, L.D. 946 will go into effect on July 1.

For legislation that claims to address online privacy, L.D. 946 makes an odd choice: it focuses exclusively on broadband ISPs. Edge providers like Google, Facebook, Amazon, Netflix, eBay, and LinkedIn inexplicably escape scrutiny, as do brick-and-mortar businesses. As Daniel Lyons, American Enterprise Institute Visiting Fellow and member of the Free State Foundation's Board of Academic Advisors, recently explained:

> Supporters justify this disparate burden by highlighting the allegedly 'privileged place' that ISPs occupy in the network, by controlling the wires that carry information to and from the consumer's home. But this is misleading. My home broadband provider can only gather, at most, information about my online activity while I am at home. By comparison, Google can capture all my activity while logged into my Google account whether at home, at work, or on mobile networks, if, like me, you use a phone powered by Google's Android operating system.… The notion that an ISP is in a privileged position vis-à-vis edge providers is, at best, questionable.[2]

Specifically, L.D. 946 states that, unless an exception applies,[3] broadband (but not dial-up) ISPs "may not use, disclose, sell or permit access to customer personal information" unless "the customer gives the provider express, affirmative consent."[4] (In other words, customers must "opt-in.") In addition, an ISP cannot refuse to serve a customer who does not opt-in, nor can it impose a penalty or offer a discount, based upon whether consent is or is not provided.[5] Thus, the statute prevents ISPs and their customers from engaging in informed transactions – that is, access to personal information for marketing purposes in exchange for financial compensation – that would generate clear consumer welfare benefits.

The statute defines "customer personal information" broadly to include not just "[p]ersonally identifying information about a customer, including but not limited to the customer's name, billing information, social security number, billing address, and demographic data," but also "[i]nformation from a customer's use of broadband Internet access service." The latter covers

---

[1] Legislative Document No. 946, "An Act To Protect the Privacy of Online Customer Information" (June 6, 2019), available at http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0275&item=1&snum=129.

[2] Daniel Lyons, "3 years later, privacy rules specifically for internet service providers remain bad policy," *AEIdeas* (February 27, 2020), available at https://www.aei.org/technology-and-innovation/3-years-later-privacy-rules-specifically-for-internet-service-providers-remain-bad-policy/.

[3] *See* Me. Stat. tit. 35-A, § 9301(2) (2019) (exempting the use of, disclosure of, sale of, or access to "customer personal information" to comply with certain provisions of state and federal law). *See also* Me. Stat. tit. 35-A, § 9301(4)(A)-(F) (2019). Exceptions under subsection (4) include providing and billing for broadband service; marketing communications-related services; complying with a lawful court order; preventing fraudulent, abusive, or unlawful use of the service; and responding to emergency service calls. *Id.*

[4] Me. Stat. tit. 35-A, § 9301(2), (3) (2019).

[5] *See* Me. Stat. tit. 35-A, § 9301(3)(b)(1), (2) (2019).

both sensitive information (for example, financial and health information) and non-sensitive information (for example, web browsing history, application usage details, and IP addresses).[6] As a general matter, the use of non-sensitive information typically does not warrant a requirement that customers "opt-in." Instead, an "opt-out" regime is sufficient.

L.D. 946 does allow ISPs to use, disclose, access, or sell information "that is not customer personal information" – but permits customers to "opt-out" from such use,[7] despite the fact that (1) the statute does not define what information falls into this category, and (2) by definition non-personal information does not implicate individual privacy.

ISPs also must "take reasonable measures to protect customer personal information from unauthorized use, disclosure or access"[8] and provide "customers a clear, conspicuous and nondeceptive notice at the point of sale and on the provider's publicly accessible website of the provider's obligations and a customer's rights under this section."[9]

Finally, L.D. 946 applies "to providers operating within the State when providing broadband Internet access service to customers that are physically located and billed for service received in the State."[10] This specific language raises legitimate questions as to whether residents of other states using mobile devices while within Maine's borders also are covered by the statute.

On February 14, 2020, four trade associations representing both wireline and wireless ISPs (ACA Connects – America's Communications Association, CTIA – The Wireless Association®, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association (collectively, the "ISP Groups")), filed a legal challenge to L.D. 946 in the United States District Court for the District of Maine.[11] The ISP Groups argue that L.D. 946 is unconstitutional and seek an injunction prohibiting its enforcement.

The legal issues that the ISP Groups raise can be sorted into two buckets: discriminatory treatment and administrative ambiguity. Their court filing goes into considerable detail and I recommend that interested readers review it. For current purposes, however, I will just highlight several key arguments.

L.D. 946 applies exclusively to broadband ISPs, even though other entities, both online and offline, have access to, and utilize for similar purposes, at least as much personal information. As the ISP Groups explain, this raises substantial legal issues under the First Amendment by discriminating between similarly situated speakers. Specifically, in restricting both the commercial and non-commercial speech of (only) broadband ISPs, the statute triggers a "strict

---

[6] *See* Me. Stat. tit. 35-A, § 9301(1)(C)(1), (2)(a)-(i) (2019).
[7] Me. Stat. tit. 35-A, § 9301(3)(C) (2019).
[8] Me. Stat. tit. 35-A, § 9301(5) (2019).
[9] Me. Stat. tit. 35-A, § 9301(6) (2019).
[10] Me. Stat. tit. 35-A, § 9301(7) (2019).
[11] *Complaint for Declaratory Judgment and Injunctive Relief* (filed February 14, 2020), available at https://acaconnects.org/wp-content/uploads/2020/02/200214-Complaint-404pm-R2226412xAB81A.pdf (*ISP Groups' Complaint*).

scrutiny" analysis.[12] And under Supreme Court precedent, "government regulation may not favor one speaker over another."[13]

This law also implicates the Supremacy Clause. Both Congress and the FCC have expressed, in no uncertain terms, a national policy preference for even-handed oversight of the privacy practices of all participants in the Internet ecosystem. During the Obama Administration, and in the wake of an FCC Democratic majority's decision to reclassify broadband Internet access service as a "telecommunications service" subject to common carrier regulation under Title II of Communications Act,[14] the Commission adopted broadband privacy rules that applied solely to ISPs.[15] However, those rules were invalidated in 2017 by a Congressional Review Act (CRA) joint resolution.[16] That Congress and the President went to such extraordinary lengths to invoke the rarely used CRA to pass legislation undoing the work of an independent agency left no doubt that the rules the FCC had adopted were not consistent with national policy. As the White House Press Secretary explained at a briefing, passage of the joint resolution "allow[s] all service providers to be treated fairly and consumer protection and privacy concerns to be reviewed on an equal playing field."[17]

Moreover, in 2018, under the leadership of Republican Chairman Ajit Pai, the FCC re-reclassified broadband as an "information service" subject to minimal regulation under Title I of the Communications Act.[18] In doing so, the agency noted approvingly that:

> By reinstating the information service classification of broadband Internet access service, we return jurisdiction to regulate broadband privacy and data security to the Federal Trade Commission (FTC), the nation's premier consumer protection agency and the agency primarily responsible for these matters in the past. Restoring FTC jurisdiction over ISPs will enable the FTC to apply its extensive privacy and data security expertise to provide *the uniform online privacy protections that consumers expect and deserve*.[19]

---

[12] *Id*. at 20.
[13] *Id*. at 21 (*citing Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 828 (1995)). *See also id*. ("The Statute cannot survive strict scrutiny because Maine cannot 'prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest.'") (*citing Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2231 (2015)).
[14] *See generally Protecting and Promoting the Open Internet*, WC Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015).
[15] *See generally Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, 31 FCC Rcd 13911 (2016) (*2016 Privacy Order*).
[16] *See* Glenn G. Lammi, "The Nullification Of FCC's Broadband Privacy Rules: What It Really Means For Consumers," *Forbes* (April 12, 2017), available at https://www.forbes.com/sites/wlf/2017/04/12/the-nullification-of-fccs-broadband-privacy-rules-what-it-really-means-for-consumers/#43245e1479ba.
[17] *See* "Press Briefing by Press Secretary Sean Spicer" (March 30, 2017), available at https://www.whitehouse.gov/briefings-statements/press-briefing-press-secretary-sean-spicer-033017/. *See also* Brian Fung, "Trump has signed repeal of the FCC privacy rules. Here's what happens next.," *The Washington Post* (April 4, 2017), available at https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/ (reporting that a statement released by FCC Chairman Ajit Pai declared that "American consumers' privacy deserves to be protected regardless of who handles their personal information").
[18] *See generally See Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd. 311 (2018) (*Restoring Internet Freedom Order*).
[19] *Id*. at ¶ 181 (citations omitted) (emphasis added).

L.D. 946 also includes poorly drafted and overly broad statutory provisions that make compliance difficult, if not impossible, thereby likely running afoul of the Due Process Clause of the Fourteenth Amendment. As the ISP Groups point out, "[i]t is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined."[20] The statute implicates the vagueness doctrine in a number of ways. For one, the definition of "[p]ersonally identifying information" includes a non-exhaustive list of examples – and ISPs seeking to stay on the right side of this law should not be expected to fill in the gaps regarding what other data might fall within that definition. For another, L.D. 946 does not even attempt to define the non-personal information that ISPs are barred from using in the event that a customer submits an "opt-out" request. Finally, it is unclear whether the law would apply to non-residents using mobile devices while in the state.

The Increasing Use of Encryption Has Further Restricted the Ability of ISPs to Access Customer Information

Technically speaking, the manner in which consumers access the Internet has evolved in two important ways since the FCC adopted its since-invalidated ISP-only privacy rules. As a consequence, L.D. 946 stands on even shakier ground now than it might have earlier. Specifically, the use of encryption has increased significantly.

First, HTTPS encryption limits the visibility that ISPs have into the web browsing activity of their customers.[21] When a customer accesses content on a site that utilizes HTTPS encryption (*e.g.*, https://www.freestatefoundation.org), the ISP can see what site he or she has visited, but encryption prevents it from discovering what specific pages the customer has viewed, what searches he or she conducted, what information he or she has provided, etc. By contrast, HTTPS encryption does not prevent the website itself from tracking the customer's activity during his or her visit.

In the *2016 Privacy Order*, the FCC concluded that "truly pervasive encryption on the Internet is still a long way off, and that many sites still do not encrypt."[22] The use of encryption is much more prevalent today. Fortinet found that 87 percent of web traffic was encrypted as of early 2019, up from 53 percent in 2016.[23]

---

[20] *ISP Groups' Complaint* at 25 (*citing Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972)).
[21] *See* "Google Transparency Report," available at https://transparencyreport.google.com/https/overview?hl=en ("HTTPS helps keep your browsing safe by securely connecting your browser or app with the websites you visit…. Our goal is to achieve 100% encryption across our products and services."). *See also ISP Groups' Complaint* at 9 (noting that "[r]ecent technological developments have limited ISPs' access to consumers' data when transmitted over their Internet connection" and describing the impact of HTTPS encryption on ISPs' access to customer web-browsing data).
[22] *2016 Privacy Order* at ¶ 34 (citations omitted).
[23] *See* Fahmida Y. Rashid, "Encryption, Privacy in the Internet Trends Report," *Decipher* (June 12, 2019), available at https://duo.com/decipher/encryption-privacy-in-the-internet-trends-report (*citing* Mary Meeker, "Internet Trends 2019" (June 11, 2019), available at https://www.bondcap.com/#view/title?mod=article_inline).

Second, web browsers increasingly support,[24] and in at least one instance utilize by default,[25] DNS-over-HTTPS (DoH), a protocol that encrypts DNS queries (that is, requests to translate domain names (*e.g.*, www.freestatefoundation.org) into IP addresses (*e.g.*, 34.83.19.155)).[26] When a customer uses DoH, his or her ISP has no visibility into even the identity of websites visited.[27] Again, this creates a drastically different situation today than the one that existed at the time of the *2016 Privacy Order*, in which the Commission concluded that ISPs "can see DNS lookups *every time* a customer uses the service to go to a new site."[28]

Thus, as a technical matter ISPs have even less insight today into the online activity of their customers than when the FCC adopted its since-invalidated rules. By contrast, the ability of edge providers to obtain personal information from consumers is unaffected by both HTTPS encryption and DoH, which obfuscate the path between end user devices and the online destination but do not interfere with edge providers' visibility into what consumers do on their sites or within their apps.[29]

Edge Providers Overshadow ISPs in Terms of Both Digital Advertising Revenues and FTC Enforcement Actions

It's important not to forget that edge providers far surpass ISPs in the provision of targeted advertising: in 2019, the top three players – Google, Facebook, and Amazon – alone were the beneficiaries of nearly 70 percent of all digital advertising spending.[30] That dominant position likely will only continue to the extent that statutes like L.D. 946 impede the ability of ISPs to offer meaningful competition.[31]

---

[24] *See* Catalin Cimpanu, "Here's how to enable DoH in each browser, ISPs be damned," *ZDNet* (February 26, 2020), available at https://www.zdnet.com/article/dns-over-https-will-eventually-roll-out-in-all-major-browsers-despite-isp-opposition/ (reporting that "[a]ll six major browser vendors have plans to support DNS-over-HTTPS (or DoH)").

[25] *See* Catalin Cimpanu, "Mozilla enables DOH by default for all Firefox users in the US," *ZDNet* (February 25, 2020), available at https://www.zdnet.com/article/mozilla-enables-doh-by-default-for-all-firefox-users-in-the-us/ ("Starting today, all new Firefox installs in the US will have DoH enabled by default. Furthermore, Mozilla also plans to silently enable the DoH feature for all Firefox US users in the coming weeks.").

[26] *See id*. ("DoH works by taking the DNS query at the browser level, encrypting it, and then hiding it inside all the other HTTPS encrypted web traffic that originates from a browser.").

[27] *See* Jon Brodkin, "Firefox turns encrypted DNS on by default to thwart snooping ISPs," *Ars Technica* (February 25, 2020), available at https://arstechnica.com/information-technology/2020/02/firefox-turns-encrypted-dns-on-by-default-to-thwart-snooping-isps/ ("DNS over HTTPS helps keep eavesdroppers from seeing what DNS lookups your browser is making, potentially making it more difficult for Internet service providers or other third parties to monitor what websites you visit").

[28] *2016 Privacy Order* at ¶ 31 (*citing* Upturn Comments at 6 ("DNS queries are almost never encrypted.")) (emphasis added).

[29] *See ISP Groups' Complaint* at 10 ("These same developments have not affected the ability of edge providers and software developers to access Internet-usage information.").

[30] *See* Greg Sterling, "Almost 70% of digital ad spending going to Google, Facebook, Amazon, says analyst firm," *Marketing Land* (June 17, 2019), available at https://marketingland.com/almost-70-of-digital-ad-spending-going-to-google-facebook-amazon-says-analyst-firm-262565 (referencing an eMarketer report).

[31] *See* Daniel Lyons, "3 years later, privacy rules specifically for internet service providers remain bad policy," *AEIdeas* (February 27, 2020), available at https://www.aei.org/technology-and-innovation/3-years-later-privacy-rules-specifically-for-internet-service-providers-remain-bad-policy/ (explaining how "a regulatory regime that makes it harder for ISPs, but not edge providers, to collect and monetize data not only tilts the playing field, it tilts it in favor of incumbents and against innovation").

Edge providers also feature prominently in high-profile privacy controversies, breaches, and settlements with the FTC. These include:

- Facebook's record-breaking $5 billion fine for "deceiving users about their ability to control the privacy of their personal information;"[32]
- The largest-ever civil penalty under the Children's Online Privacy Protection Act of 1998 (COPPA) – $170 million –imposed upon Google and its subsidiary YouTube for allegedly failing to obtain parental consent before collecting kids' personal information;[33]
- A $5.7 million settlement with the company behind the popular TikTok app, also for alleged COPPA violations;[34]
- A $575 million+ settlement with Equifax in connection with a breach that affected over 147 million individuals.[35]

Edge providers far and away earn the lion's share of digital advertising revenue. They also are the subject of the vast majority of FTC privacy enforcement actions. And yet Maine's attempt to protect the online privacy of state residents does not apply to edge providers.

A Real-World Hypothetical Reveals How L.D. 946 Cannot Achieve Its Stated Objective

Rather than focusing on the likelihood that the ISP Groups will prevail on the legal merits – a result that, incidentally, I do regard as likely – instead I want to step back and look at this through a more practical, consumer-oriented lens. The state of Maine wants to protect consumer privacy. While I would prefer that such oversight be conducted exclusively by the FTC at the federal level, I do recognize that other states are active in this sphere. That trend likely will continue until and unless Congress passes preemptive federal law – and I hope that it does. As things stand, however, any state-level statute that purports to protect consumer privacy should actually do so. As the following hypothetical which I constructed makes plain, L.D. 946 does not.

The date is August 1, 2020. L.D. 946 has been effective for a month. Social distancing is no longer required, and Jane D. Consumer has plans to join some friends at a local coffee shop. She logs on to Facebook using the Firefox browser on her desktop PC to view the details of her upcoming meetup. Firefox by default supports DoH,[36] *so her wireline ISP does not see what website she is visiting or what she does during that visit. However, that website – Facebook –*

---

[32] *See* Press Release, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook" (July 24, 2019), available at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (highlighting that "[t]he $5 billion penalty against Facebook is the largest ever imposed on any company for violating consumers' privacy and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide").

[33] *See* Federal Trade Commission, "Privacy & Data Security Update: 2019," available at https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf, at 9.

[34] *See id*. at 9-10.

[35] *See id*. at 6.

[36] *See* Jon Brodkin, "Firefox turns encrypted DNS on by default to thwart snooping ISPs," *Ars Technica* (February 25, 2020), available at https://arstechnica.com/information-technology/2020/02/firefox-turns-encrypted-dns-on-by-default-to-thwart-snooping-isps/ ("Firefox will start switching browser users to Cloudflare's encrypted-DNS service today and roll out the change across the United States in the coming weeks.").

knows much about Jane. After all, she's been a member since she was a college sophomore. While logged in, she confirms her plans to attend the coffee shop gathering via Messenger and scrolls through her timeline, commenting on a photo in which she was tagged and wishing her cousin a happy birthday.

Details in hand, Jane heads outside and gets into her car. It has been a while since she last visited said coffee shop, so she uses her smartphone, along with her mobile broadband subscription, to look up directions using Google Maps. Google, too, is quite familiar with Jane, who is logged in to her Google account on her Android device. As she travels from point A to point B, Google adds a little bit more about Jane to its data arsenal.

Upon arriving at the coffee shop, Jane sees the loyalty program sign-up sheet by the register – upon which customers have written names, phone numbers, and email addresses for anyone to see – and recalls that she joined the previous year. Her friends are running late, so after purchasing a beverage with her member discount – specifically, a medium vanilla latte, which the point-of-sale software dutifully associates with her profile – she logs onto the free Wi-Fi and passes the time by shopping online at Amazon, yet another edge provider with whom she has an account.

Her friends soon arrive, and they have a pleasant time catching up. To capture the moment, Jane takes and posts to Instagram a group selfie. After an hour or so she says her goodbyes and heads home.

Let's retrace Jane's steps with an eye towards their privacy implications:

- Her home ISP learned little – perhaps nothing – about Jane's comings-and-goings, as https://www.facebook.com uses HTTPS encryption and her Firefox browser automatically encrypts DNS lookups using DoH.
- Facebook, however, was able to glean additional information about her (and perhaps her friends) during her session, consistent with its terms of service and privacy policy.
- In the car, Jane's mobile broadband provider may have had some visibility into online activity, but Jane hasn't gotten around to responding to the email requesting that she "opt-in" to the use of her customer personal information – she intends to, as she appreciated the discounted offers she received via targeted advertising prior to the effective date of L.D.946 – so her wireless ISP is barred from making use of that data.
- By contrast, L.D. 946 in no way restricts Google Maps ability to collect and use information derived from Jane's travels – again, as set forth in its public disclosures – both to and from the coffee shop.
- Similarly, L.D. 496 does not apply to brick-and-mortar establishments like the coffee shop – despite the fact that it, too, provides Jane with access to the Internet via "free" Wi-Fi – so the coffee shop was able to gather data about both her drink purchase and online activity.
- Likewise, both Amazon and Instagram (as it happens, a subsidiary of Facebook) were able to collect and use information about Jane's online activity without regard to L.D. 496.

In summary, Jane's connected adventure involved two ISPs, multiple edge providers, and an offline business establishment that also happens to make Internet access available. But L.D. 946, which purports to protect online privacy, constrained the actions of only the ISPs – ironically, the entities that, as a technical matter, have the least insight into Jane's online activity. The practical takeaway for the real-world residents of Maine: L.D. 946 does not address in any meaningful way how, and to what extent, their personal data is used.

Conclusion

To the extent that consumers require additional online privacy protections, federal law is the appropriate vehicle to achieve this objective. Generally speaking, state-specific laws produce conflicting obligations that apply to only portions of the border-agnostic national/international Internet marketplace, leading to confusion for consumers and compliance headaches for businesses. In this specific case, Maine's ISP-focused statute does not, and cannot, achieve its stated goal of protecting residents' personal data, as ISPs constitute but one small segment of the digital advertising marketplace. By contrast, edge providers without question are the major collectors of personal information, and L.D. 946 will exacerbate that situation by constraining unreasonably ISPs' access to similar data. As a consequence, both consumers and competition will suffer.

* Andrew Long is a Senior Fellow of the Free State Foundation, an independent**,** nonpartisan free market-oriented think tank located in Rockville, Maryland.