IN THE SUPREME COURT OF THE STATE OF OREGON

THE STATE OF OREGON, Plaintiff-Respondent, Respondent on Review. v. RANDALL DE WITT SIMONS, Defendant-Appellant, Petitioner on Review,	Lane County Circuit Court Case No. 19CR43543 CA A177032 SC S070787

BRIEF OF AMICI CURIAE THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF OREGON

Review of the decision of the Court of Appeals
on an appeal from a judgement of the Circuit Court for Lane County
Honorable Karrie K. McIntyre, Judge

(*Attorneys listed on the next page*)

Nicola Morrow*
Michael W. Price, NY #4771697
National Association of Criminal
Defense Lawyers
1660 L St. NW, 12th Floor
Washington, DC 20036
Tel: (202) 872-8600
nmorrow@nacdl.org
*New York bar admission pending

Justin N. Rosas, OSB #076412
The Law Office of Justin Rosas
110 W. 11th St.
Medford, OR 97501
Tel: (541) 245-9781
justin@justinrosas.com

Jennifer Stisa Granick, CA #168423
American Civil Liberties
Union Foundation
425 California St., 7th Fl.
San Francisco, CA 94104
Tel: 415-343-0758
jgranick@aclu.org

Kelly Simon, OSB #154213
ksimon@aclu-or.org
ACLU Foundation of Oregon, Inc.
P.O. Box 40585
Portland, OR 97240
ksimon@aclu-or.org

Andrew Crocker, CA #296591
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Andrew@eff.org

Nathan Freed Wessler
Brett Max Kaufman
American Civil Liberties
Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
nwessler@aclu.org
bkaufman@aclu.org

Attorneys for Amici Curiae

ERNEST G. LANNET #013248
Chief Defender
Criminal Appellate Section
KYLE KROHN #104301
Senior Deputy Public Defender
Oregon Public Defense Commission
1175 Court Street NE
Salem, OR 97301
Kyle.Krohn@opds.state.or.us
Tel: (503) 378-3349

Attorneys for Petitioner on Review

ELLEN F. ROSENBLUM #753239
Attorney General
BENJAMIN GUTMAN #160599
Solicitor General
JOANNA HERSHEY #162665
Assistant Attorney General
400 Justice Building
1162 Court Street NE
Salem, OR 97301
Joanna.Hershey@doj.oregon.gov
Tel: (503) 378-4402

Attorneys for Respondent on Review

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTERESTS OF *AMICI CURIAE* ii

INTRODUCTION 3

ARGUMENT 4

I. The Fourth Amendment protects individuals' browsing history from warrantless government intrusion 4

II. A service provider's private terms of service cannot defeat an Internet user's reasonable expectation of privacy in their browsing history 12

A. Monitoring policies do not extinguish a user's reasonable expectation of privacy 13

B. The Court of Appeals' decision would apply to all Internet service providers, not just private businesses that offer public Wi-Fi networks 18

C. Distinguishing between an Internet user's reasonable expectation of privacy in browsing history based on where and how they access the Internet would disparately impact those with the fewest resources to protect themselves from government surveillance 21

CONCLUSION 28

CERTIFICATE OF COMPLIANCE 1

CERTIFICATE OF FILING AND SERVICE 2

TABLE OF AUTHORITIES

Cases

Andersen Consulting LLP v. UOP,
991 F Supp 1041 (ND Ill 1998).....17

Berger v. New York,
388 US 41 (1967).....19

Byrd v. United States,
584 US 395 (2018).....3, 15

Carpenter v. United States,
585 US 296 (2018)..... *passim*

In re Facebook, Inc. Internet Tracking Litigation,
956 F3d 589 (9th Cir 2020) 3, 10, 11

In re J C N-V,
359 Or 559, 380 P3d 248 (2016) 1

Kyllo v. United States,
533 US 27 (2001).....5, 6

Packingham v. North Carolina,
582 US 98 (2017).....9, 10

People v. Hughes,
506 Mich 512, 958 NW2d 98 (2020).....2

Rakas v. Illinois,
439 US 128 (1978).....15

Riley v. California,
573 US 373 (2014)..... *passim*

Smith v. Maryland,
442 US 735 (1979)..... 13, 16, 17, 28

Stanford v. Texas,
379 US 476, 485 (1965).....10

State v. Aranda,
370 Or 214, 516 P3d 1175 (2022) 1

State v. Bray,
363 Or 226, 422 P3d 250 (2018) 5

State v. Kennedy,
295 Or 260, 666 P2d 1316 (1983) 5

State v. Lien,
364 Or 750, 441 P3d 185 (2019) 5

State v. Mansor,
363 Or 185, 421 P3d 323 (2018) 5

State v. Nascimento,
360 Or 28, 379 P3d 484 (2016) 2

State v. Pittman,
367 Or 498, 479 P3d 1028 (2021) 2, 3

State v. Simons,
329 Or App 506, 540 P3d 1130 (2023)..... *passim*

State v. Turay,
371 Or 128, 532 P3d 57 (2023) 2, 3

United States v. Cotterman,
709 F3d 952 (9th Cir 2013) 10

United States v. Forrester,
512 F3d 500 (9th Cir 2008) 11

United States v. Ganias,
824 F3d 199 (2d Cir 2016) 2

United States v. Hasbajrami,
945 F3d 641 (2d Cir 2019) 2

United States v. Jones,
565 US 400 (2012).....1, 6

United States v. Kolsuz,
890 F3d 133 (4th Cir 2018) 10

United States v. Mohamud,
843 F3d 420 (9th Cir 2016) 3

United States v. Mullins,
992 F2d 1472 (9th Cir 1993) 17

United States v. Owens,
782 F2d 146 (10th Cir 1986) 16

United States v. Pineda-Moreno,
688 F3d 1087 (9th Cir 2012) 3, 27

United States v. Thomas,
447 F3d 1191 (9th Cir 2006) 16

United States v. Warshak,
631 F3d 266 (6th Cir 2010) 2, 3, 14

United States v. Weaver,
636 F Supp 2d 769 (CD Ill 2009) 17

Statutes

18 USC § 2510 (15) 17

18 USC § 2511(2)(a)(i) 19

18 USC § 2702 17

18 USC § 2703 17

U.S. Const. amend. IV 5

Other Authorities

"Internet Broadband Fact Sheet," Pew Research Center (Jan. 31, 2024),
https://www.pewresearch.org/Internet/fact-sheet/Internet-broadband 19, 22

Adie Tomer, et al., *Digital Prosperity: How Broadband Can Deliver Health and Equity to All Communities*, Brookings Inst. (Feb 27, 2020), https://www.brookings.edu/articles/digital-prosperity-how-broadband-can-deliver-health-and-equity-to-all-communities 23

Alex Guarino, *Study Finds 89% of US Citizens Turn to Google Before Their Doctor*, WECT (June 24, 2019), https://www.wect.com/2019/06/24/study-finds-us-citizens-turn-google-before-their-doctor 8

Brandeis Marshall & Kate Ruane, *How Broadband Access Advances Systemic Equality*, ACLU (Apr. 28, 2021), https://www.aclu.org/news/privacy-technology/how-broadband-access-hinders-systemic-equality-and-deepens-the-digital-divide 21

Broadband and Digital Equity, City of Boston (last visited June 6, 2024) https://www.boston.gov/departments/broadband-and-cable/broadband-and-digital-equity 26

Cecilia Kang, *Parking Lots Have Become a Digital Lifeline*, N.Y. Times (May 5, 2020), https://www.nytimes.com/2020/05/05/technology/parking-lots-wifi-coronavirus.html 25, 26

City Bar Justice Center, *Homeless Need Internet Access to Find a Home* (May 2020), https://www.citybarjusticecenter.org/wp-content/uploads/2020/05/Homeless-Need-Internet-Access-to-Find-a-Home-2020-Report.pdf..... 21, 23

Daniel de Zayas, Note, *Carpenter v. United States and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 Am. U. L. Rev. 2209, 2209 (2019) 7

Darrell M. West & Jack Karsten, *Rural and Urban America Divided by Broadband Access*, Brookings (July 18, 2016), https://www.brookings.edu/articles/rural-and-urban-america-divided-by-broadband-access 23

Emotionalgoldmine, *ELI5: How did people "google" before Google existed?*, Reddit, https://www.reddit.com/r/explainlikeimfive/comments/3k24ua/eli5_how_did_people_google_before_google_existed 9

EPIC, *Public Opinion on Privacy* (2018), https://archive.epic.org/privacy/survey.....8

Hughesnet, *Acceptable Use Policy*, https://legal.hughesnet.com/AcceptableUsePolicy.....20

Hughesnet, *Hughes Subscriber Privacy Policy*, https://legal.hughesnet.com/SubscriberPolicies.cfm 20

Jeremy Nevy, *Internet Access and Inequality*, Social Policy Lab (Sept. 30, 2021), https://www.socialpolicylab.org/post/Internet-access-and-inequality..... 22, 25

Jessica Flores, *Oakland to Offer Free Internet for Public Housing Residents to Bridge Digital Divide*, S.F. Chronicle (May 7, 2023), https://www.sfchronicle.com/bayarea/article/oakland-free-Internet-access-18084366.php 26

Katherine De Leon (@kdeleon), X (Aug. 28, 2020, 12:42 PM), https://x.com/kdeleon/status/1299386969873461248 25

Katherine Haan, *Public Wi-Fi Risks*, Forbes, https://www.forbes.com/advisor/business/public-wifi-risks/ (last visited June 6, 2024).....26

Kendall Swenson & Robin Ghertner, Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services, *People in Low-Income Households Have Less Access to Internet Services – 2019 Update* (Mar. 2021), https://aspe.hhs.gov/sites/default/files/2021-07/internet-access-among-low-income-2019.pdf..... 22, 23

KTVZ News Staff, *Federal Funds Are Helping Oregon Address Barriers to Internet Access*, KTVZ (Apr. 24, 2024), https://ktvz.com/news/oregon-northwest/2024/04/24/federal-funds-are-helping-oregon-address-barriers-to-Internet-access 24

Lisa Guernsey, Sabia Prescott, & Claire Park, *Public Libraries and the Pandemic,* New America (2021) https://files.eric.ed.gov/fulltext/ED612400.pdf 24

Mark Saferstein, *Bridging the Digital Divide: Free Wi-Fi in Parks*, Parks & Recreation Magazine (May 18, 2018), https://www.nrpa.org/parks-recreation-magazine/2018/may/bridging-the-digital-divide-free-wi-fi-in-parks. 25

Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Rsch. Ctr. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance 8

Monica Anderson, *Mobile Technology and Home Broadband 2019*, Pew Rsch. Ctr.: Internet & Technology (June 13, 2019), https://www.pewresearch.org/Internet/2019/06/13/mobile-technology-and-home-broadband-2019. 24

Nathan Freed Wessler, *How Private is Your Online Search History?*, ACLU News & Commentary (Nov. 12, 2013), https://www.aclu.org/news/national-security/how-private-your-online-search-history 7

Oregon Broadband Office, *Oregon Digital Equity Plan* (April 2024), https://www.oregon.gov/biz/Publications/Broadband/ORDigitalEquityPlan.pdf 24, 25

Press Release, Bill & Melinda Gates Foundation, *Millions of People Rely on Library Computers for Employment, Health, and Education* (Mar. 25, 2010), https://www.gatesfoundation.org/ideas/media-center/press-releases/2010/03/millions-of-people-rely-on-library-computers-for-employment-health-and-education 27

Press Release, Chicago Public Schools, *Chicago Launches Groundbreaking Initiative to Bridge Digital Divide, Providing Free High-Speed Internet Access to Over 100,000 CPS Students* (June 25, 2020), https://www.cps.edu/press-releases/chicago-launches-groundbreaking-initiative-to-bridge-digital-divide-providing-free-high-speed-Internet-access-to-over-100000-cps-students 26

Rafi Goldberg, *New NTIA Data Show Enduring Barriers to Closing the Digital Divide, Achieving Digital Equity*, National Telecommunications and Information Administration (May 11, 2022), https://www.ntia.gov/blog/2022/new-ntia-data-show-enduring-barriers-closing-digital-divide-achieving-digital-equity. 23

Rohan Mattu, *Baltimore to Launch Free Public Wi-Fi in Effort to Bridge Digital Divide*, CBS News (Dec. 18, 2023), https://www.cbsnews.com/baltimore/news/baltimore-to-launch-free-public-wi-fi-in-effort-to-bridge-digital-divide.....26

Spectrum, "Spectrum Residential Internet Services Agreement," https://www.spectrum.com/policies/residential-Internet-services-agreement..... 16, 19

Spectrum, "Spectrum Subscriber Annual Privacy Notice (2023)," https://www.spectrum.com/policies/spectrum-customer-privacy-policy 19

Verizon, "Verizon Online Terms of Service for Verizon Internet and Value Added Services," https://www.verizon.com/about/terms-conditions/verizon-online-terms-service-verizon-business-Internet-and-value-added-services..... 16, 19, 20

Xfinity, "Our Privacy Policy," https://www.xfinity.com/privacy/policy#privacy-who..... 19, 20

Xfinity, "Web Services Terms of Service" (2024), https://www.xfinity.com/terms/web..... 16, 19, 20

INTERESTS OF *AMICI CURIAE*

The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers, with tens of thousands of members and affiliates throughout the country. NACDL is particularly interested in cases arising from surveillance technologies and programs that pose new challenges to personal privacy. It operates a dedicated initiative that trains and directly assists defense lawyers handling such cases to help safeguard privacy rights in the digital age. NACDL has also filed numerous amicus briefs in this Court and the Supreme Court on issues involving digital privacy rights, including: *Carpenter v. United States*, 585 US 296 (2018); *Riley v. California*, 573 US 373 (2014); *United States v. Jones*, 565 US 400 (2012); *State v. Aranda*, 370 Or 214, 516 P3d 1175 (2022); *In re J C N-V*, 359 Or 559, 380 P3d 248 (2016).

The **Electronic Frontier Foundation (EFF)** is a non-profit, member-supported digital civil liberties organization. Founded in 1990, EFF has 30,000 active donors and dues-paying members across the United States, including in Oregon. EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF regularly

participates both as direct counsel and as amicus in the U.S. Supreme Court, this Court, and many others in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g.*, *Carpenter v. United States*, 585 US 296 (2018); *Riley v. California*, 573 US 373 (2014); *State v. Pittman*, 367 Or 498, 479 P3d 1028 (2021) (en banc); *State v. Nascimento*, 360 Or 28, 379 P3d 484 (2016).

The **American Civil Liberties Union (ACLU)** is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The American Civil Liberties Union of Oregon (ACLU of Oregon) is the Oregon state affiliate of the national ACLU. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other state and federal courts in numerous cases implicating Americans' right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 585 US 296 (2018) and as amicus in *State v. Pittman*, 367 Or 498, 479 P3d 1028 (2021) (en banc), *State v. Turay,* 371 Or 128, 532 P3d 57 (2023), *People v. Hughes*, 506 Mich 512, 958 NW2d 98 (2020), *United States v. Ganias*, 824 F3d 199 (2d Cir 2016) (en banc), *United States v. Hasbajrami*, 945 F3d 641 (2d Cir 2019), and *United States v. Warshak*, 631 F3d 266 (6th Cir 2010). The ACLU of Oregon has appeared frequently before this Court and federal courts advocating for the right to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article I, section 9 of the

Oregon Constitution, including in *Pittman*, 367 Or 498, 479 P3d 1028, *Turay*, 371 Or 128, 532 P3d 57, *United States v. Mohamud*, 843 F3d 420 (9th Cir 2016), and *United States v. Pineda-Moreno*, 688 F3d 1087 (9th Cir 2012).

INTRODUCTION

People have a reasonable expectation of privacy in their Internet browsing histories. In this case, though, the Court of Appeals incorrectly concluded that Simons lacked a reasonable expectation of privacy in his browsing history when he repeatedly connected to a nearby restaurant's Wi-Fi network that was freely accessible from his home. *See State v. Simons*, 329 Or App 506, 508, 540 P3d 1130, 1133 (2023). It construed the existence of a private user agreement reserving the right of a private party—the restaurant—to monitor Internet usage on its network as a broad waiver of constitutional rights. This holding, if affirmed, would pose serious risks to Internet users everywhere, not only those who access the Internet through publicly accessible networks. Internet browsing history contains some of the most revealing and sensitive personal information that exists. *See, e.g.*, *Riley v. California*, 573 US 373 (2014); *Carpenter v. United States*, 585 US 296 (2018); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F3d 589, 603 (9th Cir 2020). Fourth Amendment privacy rights do not live and die by varying and ever-changing terms of service. *See Carpenter*, 585 US at 310; *United States v. Warshak*, 631 F3d 266, 287 (6th Cir 2010); *Byrd v. United States*, 584 US 395, 408 (2018).

Moreover, conditioning constitutional privacy rights on an individual's ability to pay for private Internet services would disparately impact those with the fewest resources in our society. Many people—including minorities and people who live in rural areas—rely on public Wi-Fi networks provided by libraries and public-facing businesses to participate in modern life. Distinguishing between an Internet user's reasonable expectation of privacy in browsing history based on where and how they access the Internet would only exacerbate the consequences of the digital divide in American life.

In this case, by warrantlessly capturing nearly a year's worth of private communications through the collection of Simons' Internet activity, the government violated Simons' Fourth Amendment rights. And if the opinion below is upheld, it will threaten the privacy rights of all Oregonians. For the reasons detailed below, *amici* urge this Court to overturn the Court of Appeals' ruling and remand to the trial court.

ARGUMENT

I. The Fourth Amendment protects individuals' browsing history from warrantless government intrusion.

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and

seizures." U.S. Const. amend. IV.[1] That right did not dissipate when Americans migrated their "papers" and "effects" from physical file cabinets to the digital cloud. Reflecting this reality, the United States Supreme Court has repeatedly explained that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, [courts must] 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 585 US at 305 (quoting *Kyllo v. United States*, 533 US 27, 34 (2001)) (last alteration in original).

[1] *Amici* recognize that this court considers state constitutional questions before federal constitutional questions. *State v. Kennedy*, 295 Or 260, 262, 666 P2d 1316, 1318 (1983). Article I, section 9 of the Oregon Constitution obliges this court to adopt specific rules in the digital data context that "ensure that an individual's right to computer privacy is adequately protected." *State v. Bray*, 363 Or 226, 252, 422 P3d 250, 267–68 (2018) (citing *State v. Mansor*, 363 Or 185, 421 P3d 323 (2018)). This Court has not issued many decisions about warrantless searches in the digital context. *Amici* have focussed their discussion on the Fourth Amendment as part of the "legal and social norms" that animate this court's analysis of Article I, section 9's protection of privacy. See *State v. Lien*, 364 Or 750, 759–60, 441 P3d 185, 190–91 (2019) ("In Oregon the right to privacy—the individual freedom from government scrutiny—protected by Article I, section 9 is not defined by private property or contractual rights…Rather, [it is] '*determined by social and legal norms of behavior…'* (internal quotations omitted)); *see also Mansor,* 363 Or at 222 (citing *United States v. Riley* with approval and recognizing that the U.S. Supreme Court's Fourth Amendment reasoning in protecting digital information "is persuasive and informs our understanding of the proper application of the Oregon warrant requirement to searches of computers and other digital devices"). Nevertheless, the scope of protection under the state constitution may well be broader than that under the Fourth Amendment.

Accordingly, the Court has repeatedly updated old rules to account for novel surveillance technologies. In *Kyllo v. United States*, for example, the Supreme Court held that warrantless use of thermal imaging devices to monitor inside a home is unconstitutional, despite the lack of physical trespass. 533 US at 27. Similarly, in *United States v. Jones*, the Supreme Court distinguished digital location tracking from physical surveillance and the analog public-space doctrine. 565 US 400, 430 (2012) (holding that installing a GPS tracking device is a Fourth Amendment search); *id.* at 415 (Sotomayor, J., concurring) (longer-term GPS tracking violates reasonable expectations of privacy); *id.* at 430 (Alito, J., concurring in the judgment) (same). Likewise, in *Riley*, the Court held that the search-incident-to-arrest-doctrine does not apply to digital devices. 573 U.S. at 393 (conflating the search of a digital device and the search of "physical items. . .. is like saying a ride on horseback is materially indistinguishable from a flight to the moon"). And finally, in *Carpenter*, the Supreme Court held that the third-party doctrine does not apply to cell site location information, reinforcing the difference between analog and digital location surveillance. 585 US at 316–17.

Together, these cases help guarantee that people are free to pursue their private lives in the digital world without fear of unfettered government surveillance. Because warrantless access to Internet browsing history raises the same concerns identified in the U.S. Supreme Court's prior cases concerning Fourth Amendment

rights in the digital world, this Court should hold that people enjoy a reasonable expectation of privacy in their Internet activity.

An individual's browsing history contains "the privacies of life" that the Fourth Amendment was designed to protect. *See id.* at 304–05. In *Carpenter*, the Court explained that location history data "provides an intimate window into a person's life, revealing . . . his familial, political, professional, religious, and sexual associations," along with his most private thoughts and questions. *Id.* at 311 (quotation marks and citation omitted). This conclusion applies equally, if not more so to the detailed, substantive portrait that is a person's browsing history. *See generally* Daniel de Zayas, Note, *Carpenter v. United States and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 Am. U. L. Rev. 2209, 2209 (2019). Records of a person's Internet activity can paint a detailed profile of the user's medical diagnoses, religious beliefs, financial stability, sexual desires, relationship status, family secrets, political leanings, and more.[2]

Indeed, browsing history data will often be *more* sensitive and revealing than location history. For example, while location history might indicate that a person visited a particular medical practice, browsing history data can reveal in detail that

[2] Nathan Freed Wessler, *How Private is Your Online Search History?*, ACLU News & Commentary (Nov. 12, 2013), https://www.aclu.org/news/national-security/how-private-your-online-search-history.

person's medical diagnosis. A 2019 study found that 89 percent of patients search their health symptoms online before seeking medical care.[3] Those searches may be enormously helpful; they might even spur someone to seek life-saving care. But recording those online activities creates a deeply revealing digital profile.

Revealing someone's browsing history is akin to mind reading because people use the Internet to investigate their most private and sensitive thoughts and concerns. Indeed, polling and survey data on Internet activity and privacy reflects that Internet users know how revealing their Internet activity can be and that they expect their browsing history data remain private.[4]

Moreover, the use of the Internet, just like use of a modern cell phone, is not "voluntary" in any meaningful sense. *See Carpenter*, 585 US at 315. To the contrary, almost every aspect of life—personal, professional, and academic—requires Internet use. Using the Internet has become a natural and nearly automatic way for people to acquire information and communicate with their social and professional networks. For some people, Internet searches are the only form of reading, studying,

---

[3] Alex Guarino, *Study Finds 89% of US Citizens Turn to Google Before Their Doctor*, WECT (June 24, 2019), https://www.wect.com/2019/06/24/study-finds-us-citizens-turn-google-before-their-doctor.

[4] *See* Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Rsch. Ctr. (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance; EPIC, *Public Opinion on Privacy* (2018), https://archive.epic.org/privacy/survey.

communicating, and researching they have ever known.[5] Cell phones are indispensable today, and a major reason for that is people expect, and are expected, to always be connected to each other through the Internet. Guest Wi-Fi networks are more than just a courtesy; they are part of the infrastructure of modern communications.

Indeed, the Internet is "'such a pervasive and insistent part of daily life' that [using it] is indispensable to participation in modern society." *Carpenter*, 585 US at 315 (citing *Riley*, 573 US at 385) (comparing the world before cell phones where a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy with the modern world where people carry immense amounts of data with them). In *Packingham v. North Carolina*, the U.S. Supreme Court emphasized the importance of social media sites—a subset of the information available on the Internet—in holding that a person convicted of a sex crime nevertheless had a First Amendment right to access those sites: "Social media allows users to gain access to information and communicate with one another about it on any subject that might come to mind." 582 US 98, 107 (2017). As the Court explained, these websites are "the principal sources for knowing current

[5] Emotionalgoldmine, *ELI5: How did people "google" before Google existed?*, Reddit, https://www.reddit.com/r/explainlikeimfive/comments/3k24ua/eli5_how_did_people_google_before_google_existed.

events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge." *Id.*

Browsing history data is exactly the kind of personal information that deserves constitutional protection under the Fourth Amendment. Courts have repeatedly cited browsing history as an example of the type of deeply private information contained on a cell phone or laptop, suggesting that Fourth Amendment protections apply in part because these devices contain browsing history data.[6] *See Riley*, 573 US at 395–96 (observing that "[a]n Internet search and browsing history . . . could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD"); *United States v. Cotterman*, 709 F3d 952, 965 (9th Cir 2013) ("[e]lectronic devices often retain sensitive and confidential information … notably in the form of browsing histories …."); *United States v. Kolsuz*, 890 F3d 133, 145-46 (4th Cir 2018) (noting the "special sensitivity" of browsing history). And in a recent civil case, the U.S. Court of Appeals for the Ninth Circuit concluded that Internet users have a "reasonable expectation of privacy in their browsing histories." *See In re Facebook*, 956 F3d at 603 (citation omitted). That case involved a statutory violation by a private entity, but the court

[6] And because government acquisition of that information implicates First Amendment rights, Fourth Amendment protections must be applied with "scrupulous exactitude." *See Stanford v. Texas*, 379 US 476, 485 (1965).

acknowledged that the "Fourth Amendment imposes higher standards on the government than [] on private, civil litigants," explaining that "[a]nalogous cases decided in the Fourth Amendment context support a conclusion that the breadth of information allegedly collected would violate community norms. These cases recognize that individuals have a reasonable expectation of privacy in collections of information—including browsing history data—that reveal 'familial, political, professional, religious, and sexual associations.'" *Id.* at 604 n.7 (citing *Carpenter*, 585 US at 311; *see also Riley*, 573 US at 396; *United States v. Forrester*, 512 F3d 500, 510 n 6 (9th Cir 2008).

In this case, the government had warrantless access to nearly an entire year's worth of Simons's browsing history, comprising a staggering 255,723 webpage visits—approximately 702 data points per day. *State v. Simons*, 329 Or App 506, 519 n.5 (2023). While any quantity of browsing history data is revealing, this vast trove of Internet activity would paint an intimately detailed portrait of any Internet user. *Cf. Carpenter*, 585 US at 302, 311 (explaining that "[m]apping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts" and illustrating that in that case, police obtained "an average of 101 data points per day"). This browsing history information is deeply private and contains the kind of sensitive information that the Fourth Amendment was meant to protect from government surveillance, giving Internet users—including the

defendant in this case—a reasonable expectation of privacy in it. The government cannot intrude on that expectation of privacy without a warrant.

II. A service provider's private terms of service cannot defeat an Internet user's reasonable expectation of privacy in their browsing history.

The Court of Appeals did not dispute that nearly a year's worth of Internet browsing history could be deeply revealing of private information. The court also assumed without deciding that the trial court correctly found the restaurant employee was acting as a government agent. *Simons*, 329 Or App at 511. But it concluded that because government agents captured Simons' browsing history from a business's publicly available Wi-Fi network as opposed to a standard Internet service provider (like Comcast or Verizon), his private browsing data was not constitutionally protected. *Id*. at 519, 522.

That logic is as dangerous as it is wrong. The court pointed to the business's "user agreement" that purported to limit use of its Wi-Fi network to lawful activity. *Id.* But what the court failed to appreciate was that because this user agreement mirrors those entered into by ordinary purchasers of Internet services in their homes, on their phones, or at their private places of business, there is no meaningful distinction between a user of a business's public Internet network like Simons and the millions of other Oregonians who use a paid Internet service. If private user agreements, contracts, or terms of service documents like those in this case could undermine state and federal constitutional privacy interests, the appellate court's

holding would open the door to warrantless tracking of all Internet histories, everywhere, at any time and for any reason. Requiring people to accept that kind of tracking in exchange for something as basic as Internet access, which is fundamental to "participation in modern society," *Carpenter*, 585 US at 315, is antithetical to the principles of the Oregon Constitution and the Fourth Amendment.

A. Monitoring policies do not extinguish a user's reasonable expectation of privacy.

People have an expectation of privacy in their digital letters, papers, and effects even when their service provider stores or monitors these records. The expectation of privacy analysis is intended to describe "well-recognized Fourth Amendment freedoms," not the messy and subjective business interests that are advanced in the fine print of commercial user agreements. *Smith v. Maryland*, 442 US 735, 740 n 5 (1979). And critically, the court of appeals' conclusion regarding the privacy-defeating effect of A&W's user agreement is not limited to browsing histories, but would undercut privacy rights in almost every digital context involving third-party hosting of private user content. Any user who kept emails, photos, or documents in a corporate entity's cloud service would see their reasonable expectation of privacy in that data hinge on the service's terms of service. That is not the law.

In the modern digital age, any data stored with a third-party cloud provider, including family photos, personal communications, and private documents, is

subject to terms of service (TOS) similar to the terms at issue in this case. As with email providers, cloud computing, software, and other Internet companies use TOS to protect their business interests. *See Warshak*, 631 F3d at 286. These terms protect the business's rights and property and limit its liability. They also almost always notify users that companies may conduct private searches as part of their goal to identify and stop illegal activity, or even to merely protect their business from objectionable conduct or content. Given the benefits a TOS provides to a business, it is no surprise that company lawyers draft the TOS to give the business broad latitude in its operation. Yet, these reservations of rights are never negotiated, and users have no choice but to click "I agree" just to engage in activities fundamental to modern life.

But the fact that private businesses may reserve the right to monitor a user's content or private activity to protect their own commercial interests does not license the *government* to sidestep a constitutional warrant requirement.

For example, in *United States v. Warshak*, a foundational federal case, the Sixth Circuit considered a person's expectation of privacy in email hosted on a third-party server. 631 F3d at 286. The court in that case concluded that a user maintains a reasonable expectation of privacy in the contents of their email messages even though the email service provider's user agreement included a monitoring clause like the one at issue in this case. *Id*. at 287.

Likewise, in *United States v. Byrd*, the Supreme Court rejected the assumption that a user agreement can undermine a constitutional privacy right. In that case, the Court found that a rental car driver has a reasonable expectation of privacy in her rental car even if she is in serious violation of the rental agreement. 584 US at 408. The Court reasoned that car rental agreements, like terms of service, "concern risk allocation between private parties" rather than the relationship between an individual and the government. *Id.* And *Carpenter* firmly dispensed with the idea that the government has free license to conduct warrantless surveillance just because an individual grants a third party access to private information to use an essential modern technology. 585 US at 310–11 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere. . . . Although [access to private information is granted] for commercial purposes, that distinction does not negate [a person's] anticipation of privacy in his [protected information]").

Just as the Supreme Court has cautioned "that arcane distinctions developed in property and tort law . . . ought not to control" the analysis of who has a "legally sufficient interest in a place" for Fourth Amendment purposes, *Rakas v. Illinois*, 439 US 128, 142–43 (1978), courts have repeatedly declined to find private contracts dispositive of individuals' expectations of privacy. In *Smith v. Maryland*, for example, the Supreme Court noted, "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of

protection would be dictated by billing practices of a private corporation." 442 US at 745. Similarly, in *United States v. Thomas*, the U.S. Court of Appeals for the Ninth Circuit held that the "technical violation of a leasing contract" is insufficient to vitiate an unauthorized renter's legitimate expectation of privacy in a rental car. 447 F3d 1191, 1198 (9th Cir 2006). And in *United States v. Owens*, the Tenth Circuit did not let a motel's private terms govern the lodger's expectation of privacy, noting, "[a]ll motel guests cannot be expected to be familiar with the detailed internal policies and bookkeeping procedures of the inns where they lodge." 782 F2d 146, 150 (10th Cir 1986).

If this Court allows Fourth Amendment rights to be dictated by various corporate contracts, then each Internet user would experience a different level of constitutional protection against government surveillance of their browsing history—or their emails, photos, and documents—depending on the relevant terms of service drafted by company offering the service.[7] This is not only an absurd result, but also an impracticable one. It would grant corporations—rather than courts and

[7] It is worth noting that companies change their terms of service regularly, often with little or no notice. *See, e.g.*, Xfinity, "Web Services Terms of Service" (2024), https://www.xfinity.com/terms/web (reserving the right to modify terms of service at any time); Spectrum, "Spectrum Residential Internet Services Agreement," https://www.spectrum.com/policies/residential-Internet-services-agreement (same); Verizon, "Verizon Online Terms of Service for Verizon Internet and Value Added Services," https://www.verizon.com/about/terms-conditions/verizon-online-terms-service-verizon-business-Internet-and-value-added-services (same).

legislatures—the power to determine the shape and scope of an Internet user's civil liberties. And it would mean that the Fourth Amendment and the State's constitutional protections would rise and fall according to courts' interpretations of various terms of service at different points in time. Certain users would be granted protection against warrantless government surveillance, while others would not. Such a policy would be burdensome to courts, opaque to the public, and antithetical to the very purpose of guaranteed constitutional rights and liberties. *See Smith*, 442 US at 745.[8]

[8] Moreover, A&W likely has customer privacy obligations under the Stored Communications Act, regardless of its TOS. *See* 18 USC §§ 2702; 2703. A&W would likely qualify as either an "electronic communications service" provider (ECS) or a "remote computing service" provider (RCS). *See* 18 USC § 2510 (15); *see also, e.g., United States v. Mullins*, 992 F2d 1472, 1478 (9th Cir 1993) (airline that provides travel agents with computerized travel reservation system accessed through separate computer terminals can be an ECS); *Andersen Consulting LLP v. UOP*, 991 F Supp 1041, 1042 (ND Ill 1998) (Andersen, which has internal e-mail system, is an ECS); *United States v. Weaver*, 636 F Supp 2d 769, 770 (CD Ill 2009) (concluding that Microsoft, which provided email service through the Hotmail website, was both an ECS provider and an RCS provider). Its designation as either an ECS or an RCS provider under the Stored Communications Act confers a responsibility to safeguard the privacy of customer information. And regardless of whether A&W technically qualifies as an "electronic communications service provider" or a "remote computing service provider," the reasoning under which the appellate court reached its conclusions about A&W would also apply to larger ISPs that provide Internet access pursuant to similar user agreements.

B. The Court of Appeals' decision would apply to all Internet service providers, not just private businesses that offer public Wi-Fi networks.

What the appeals court found unique about A&W's "user agreement" in this case is actually a common feature of almost every contract or similar "terms of service" document that regulates the private relationship between a user and a company that offers Internet (or cell phone) service. The Court of Appeals' insistence that its holding was limited to the "particular context" of A&W's user agreement falls flat, *see Simons*, 329 Or App at 514, because that user agreement is not unique at all.

While A&W is not the same kind of company as Comcast or Verizon, for all relevant purposes, it was acting as an Internet service provider when it offered Internet service to the public. Those familiar telecommunications companies, too, have contracts and terms of service that prohibit certain unlawful activity, among other things. As a result, there is no meaningful distinction to be made between customers who surf the web at A&W (who click through a user agreement before accessing the Internet) and the millions of Oregonians who subscribe to large Internet service providers at home (and agree to contracts or terms of service). The same is true of the people who connect to the Internet at their favorite cafes, their schools, and their places of work. Indeed, the same is true of telephone companies, which are authorized by statute to intercept, disclose, or use the contents of phone

calls in "the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." 18 USC § 2511(2)(a)(i). Yet the law is clear: the government may not intercept phone calls without obtaining a wiretap warrant. *See Berger v. New York,* 388 US 41, 62–64 (1967)*;* 18 USC § 2516 *et seq*.

The appeals court was wrong to view A&W's user agreement as unique. In fact, the relevant terms of service that the lower court cited as undermining Simons' privacy interest in his Internet activity also appear in the standard user agreements that many millions of Americans enter with their ISPs of choice.[9] Most ISPs reserve the right to monitor Internet activity and share information with law enforcement.[10] For example, Verizon prohibits subscribers from using its Internet access service "in ways that . . . violate any law" and "reserve[s] the right to provide information about

---

[9] *See* "Internet Broadband Fact Sheet," Pew Rsch. Ctr. (Jan. 31, 2024), https://www.pewresearch.org/Internet/fact-sheet/Internet-broadband; *see also* Xfinity, "Web Services Terms of Service" (2024), https://www.xfinity.com/terms/web (citing Xfinity, "Our Privacy Policy," https://www.xfinity.com/privacy/policy#privacy-who); Spectrum, "Spectrum Residential Internet Services Agreement," https://www.spectrum.com/policies/residential-Internet-services-agreement (citing Spectrum, "Spectrum Subscriber Annual Privacy Notice (2023)," https://www.spectrum.com/policies/spectrum-customer-privacy-policy); Verizon, "Verizon Online Terms of Service for Verizon Internet and Value Added Services," https://www.verizon.com/about/terms-conditions/verizon-online-terms-service-verizon-business-Internet-and-value-added-services.

[10] *See id.*

your account and your use of the [Internet access] Service to third parties" including law enforcement."[11] Xfinity requires users to agree to "not use the Web Services for any unlawful purpose," and reserves the right to disclose information about users "to enforce our rights under our terms of service."[12] Hughesnet, a satellite-based home Internet service particularly useful to rural Internet subscribers without wired broadband access, reserves the right to monitor Internet usage, prohibits use of its service "for any unlawful, improper or criminal purpose or activity," and provides that the company "may disclose your information as necessary, if we believe you have acted in violation of our Terms of Use."[13] Given the wide deployment of these terms, the Court of Appeals was wrong to conclude that the "concerns . . . about public Wi-Fi networks becoming state tracking devices . . . is not the issue before [the Court]." *Simons*, 329 Or App at 518–19. In fact, that *is* the issue. If the Court affirms the lower court's ruling, it will threaten to give the police a green light to warrantlessly obtain the browsing histories of all Internet users in Oregon, apart from the very few individuals who can create and operate their own ISPs.

---

[11] *Verizon Online Terms*, https://www.verizon.com/about/terms-conditions/verizon-online-terms-service-verizon-business-Internet-and-value-added-services.

[12] Xfinity, *Web Services Terms of Service*, https://www.xfinity.com/terms/web; Xfinity, *Our Privacy Policy*, https://www.xfinity.com/terms/web.

[13] Hughesnet, *Hughes Subscriber Privacy Policy*, https://legal.hughesnet.com/SubscriberPolicies.cfm; Hughesnet, *Acceptable Use Policy*, https://legal.hughesnet.com/AcceptableUsePolicy.

C. Distinguishing between an Internet user's reasonable expectation of privacy in browsing history based on where and how they access the Internet would disparately impact those with the fewest resources to protect themselves from government surveillance.

In its opinion below, the Court of Appeals asserted that "[u]nlike having a cell phone, having access to private businesses' guest Wi-Fi networks, while convenient, is not "necessary for participation in modern life.'" *Simons*, 329 Or App at 520 (internal citation omitted). Characterizing public Wi-Fi networks as merely "convenient" ignores not only the centrality of the Internet in modern life but also the well-documented inequality of access to high-quality paid Internet services that often tracks racial and class-based marginalization.[14] Fourth Amendment rights are held by everyone, not just those with their own private residences and a monthly budget for a private, password-protected high-speed Wi-Fi network. It would be deeply unfair to subject people without access to their own private Internet connection to warrantless government surveillance just because they cannot afford their own Wi-Fi networks. Poor people, no less than affluent ones, require access to

[14] *See, e.g.*, Brandeis Marshall & Kate Ruane, *How Broadband Access Advances Systemic Equality*, ACLU (Apr. 28, 2021), https://www.aclu.org/news/privacy-technology/how-broadband-access-hinders-systemic-equality-and-deepens-the-digital-divide; City Bar Just. Ctr., *Homeless Need Internet Access to Find a Home* (May 2020), https://www.citybarjusticecenter.org/wp-content/uploads/2020/05/Homeless-Need-Internet-Access-to-Find-a-Home-2020-Report.pdf.

the Internet to "participat[e] in modern society"—to read the news, peruse job listings, research political candidates, and more. *Carpenter*, 585 US at 315.

Studies show that lower-income Americans and racial minorities are significantly more likely to lack home broadband, and thus, more likely to rely on public Wi-Fi options. Research from the Social Policy Data Lab shows a 75 percent correlation between median household income and broadband access across all U.S. counties,[15] and data from the Pew Research Center indicates that individuals with lower levels of income and formal education are less likely to have broadband service at home.[16] According to the U.S. Department of Health and Human Services, more than one in six people in poverty had no Internet access in 2019 whereas people with higher incomes were more likely to have Internet access in their households.[17] In 2021, 26 percent of people in households with incomes under $25,000 per year had no Internet service subscriptions at all.[18] The homeless population is particularly

---

[15] Jeremy Nevy, *Internet Access and Inequality*, Social Policy Lab (Sept. 30, 2021), https://www.socialpolicylab.org/post/Internet-access-and-inequality.

[16] *Internet/Broadband Fact Sheet*, Pew Rsch. Ctr.: Internet & Technology (January 31, 2024), https://www.pewresearch.org/Internet/fact-sheet/Internet-broadband/?tabItem=480dace1-fd73-4f03-ad88-eae66e1f4217.

[17] Kendall Swenson & Robin Ghertner, Office of the Assistant Secretary for Planning and Evaluation, U.S. Dep't of Health and Hum. Servs., *People in Low-Income Households Have Less Access to Internet Services – 2019 Update* 1 (Mar. 2021), https://aspe.hhs.gov/sites/default/files/2021-07/internet-access-among-low-income-2019.pdf.

[18] Rafi Goldberg, *New NTIA Data Show Enduring Barriers to Closing the Digital Divide, Achieving Digital Equity*, Nat'l Telecomms. and Info. Admin. (May 11,

vulnerable, with many shelters not providing any Wi-Fi access at all.[19] Moreover, nearly half of the digitally disconnected population in the United States consist of people of color. Asian and White individuals are more likely to have household Internet access than other racial/ethnic groups like Latino or Black Americans.[20] Compared to 90 percent of White households and 86 percent of Latino households, only 82 percent of Black households have the Internet at home.[21] Further, rural communities face a disproportionate lack of Internet access because Internet service providers are less incentivized to develop broadband in these areas due to high development costs and digital redlining.[22]

2022), https://www.ntia.gov/blog/2022/new-ntia-data-show-enduring-barriers-closing-digital-divide-achieving-digital-equity.

[19] City Bar Just. Ctr., *Homeless Need Internet Access to Find a Home* (May 2020), https://www.citybarjusticecenter.org/wp-content/uploads/2020/05/Homeless-Need-Internet-Access-to-Find-a-Home-2020-Report.pdf.

[20] Kendall Swenson & Robin Ghertner, Office of the Assistant Secretary for Planning and Evaluation, U.S. Dep't. of Health and Hum. Servs., *People in Low-Income Households Have Less Access to Internet Services – 2019 Update* (Mar. 2021), https://aspe.hhs.gov/sites/default/files/2021-07/internet-access-among-low-income-2019.pdf.

[21] Adie Tomer, et al., *Digital Prosperity: How Broadband Can Deliver Health and Equity to All Communities*, Brookings Inst. (Feb 27, 2020), https://www.brookings.edu/articles/digital-prosperity-how-broadband-can-deliver-health-and-equity-to-all-communities.

[22] Darrell M. West & Jack Karsten, *Rural and Urban America Divided by Broadband Access*, Brookings (July 18, 2016), https://www.brookings.edu/articles/rural-and-urban-america-divided-by-broadband-access.

According to the Pew Research Center, roughly one in four Americans lack high-speed Internet access at home, primarily due to the cost or limited service in rural areas.[23] In the United States this connectivity deficiency affects over 77 million people,[24] with older Americans, veterans, Native Americans, Black, Latino, and low-income households disproportionately represented among those without adequate home Internet access.[25] These trends apply both nationally and in Oregon. According to the Oregon Broadband Office, there are over 170,000 residencies in the state with no or slow Internet access.[26] This digital divide is particularly pronounced among low-income individuals. The 2024 Oregon Digital Equity Plan, submitted to the U.S. Department of Commerce, states that "low-income households struggle to consistently afford broadband Internet services, Internet-enabled computing devices, and technical support."[27] The report also underscores that "digital equity allows

---

[23] Monica Anderson, *Mobile Technology and Home Broadband 2019*, Pew Rsch. Ctr.: Internet & Technology (June 13, 2019), https://www.pewresearch.org/Internet/2019/06/13/mobile-technology-and-home-broadband-2019.

[24] Lisa Guernsey, Sabia Prescott, & Claire Park, *Public Libraries and the Pandemic,* New America, at 10 (2021) https://files.eric.ed.gov/fulltext/ED612400.pdf.

[25] *Id*.

[26] KTVZ News Staff, *Federal Funds Are Helping Oregon Address Barriers to Internet Access*, KTVZ (Apr. 24, 2024), https://ktvz.com/news/oregon-northwest/2024/04/24/federal-funds-are-helping-oregon-address-barriers-to-Internet-access.

[27] Oregon Broadband Office, *Oregon Digital Equity Plan* 4 (April 2024), https://www.oregon.gov/biz/Publications/Broadband/ORDigitalEquityPlan.pdf.

people from diverse backgrounds to fully participate in the economy of innovation and creativity, which helps to foster the goal of economic opportunity."[28]

As a result of these disparities, much of the public is forced to rely on publicly available Internet networks in order to stay connected. To access free Wi-Fi, many Americans depend on public spaces like restaurants, parks,[29] libraries and cafes, and even parking lots.[30] Particularly during and after the COVID-19 pandemic, many people lost access to these public spaces. In August 2020, a photo went viral after two girls in Los Angeles were seen studying on the ground in a Taco Bell parking lot to use the nearby Wi-Fi.[31] Los Angeles County alone has 268,000 students without Internet.[32]

Many individuals rely on public Wi-Fi because they do not have home Internet or because their home Internet is too slow to support a family or multiple devices. In more urban areas, high-speed Wi-Fi can be unaffordable, leading many to seek

---

[28] *Id*. at 2.
[29] Mark Saferstein, *Bridging the Digital Divide: Free Wi-Fi in Parks*, Parks & Recreation Magazine (May 18, 2018), https://www.nrpa.org/parks-recreation-magazine/2018/may/bridging-the-digital-divide-free-wi-fi-in-parks.
[30] Cecilia Kang, *Parking Lots Have Become a Digital Lifeline*, N.Y. Times (May 5, 2020), https://www.nytimes.com/2020/05/05/technology/parking-lots-wifi-coronavirus.html.
[31] Katherine De Leon (@kdeleon), X (Aug. 28, 2020, 12:42 PM), https://x.com/kdeleon/status/1299386969873461248.
[32] Jeremy Nevy, *Internet Access and Inequality*, Social Policy Lab (Sept. 30, 2021), https://www.socialpolicylab.org/post/Internet-access-and-inequality.

alternative access points.[33] The most commonly used locations for public Wi-Fi are cafes and restaurants, hotels, and libraries.[34] Many cities, including Boston,[35] Baltimore,[36] Chicago,[37] and Oakland,[38] have also launched free public Wi-Fi initiatives across the city as part of efforts to bridge the digital divide and bring reliable, high-speed Internet to underserved communities.

Libraries are particularly important resources for people who lack private Internet access. Americans across all age groups reported that they use library computers and Internet access. In 2010, the Gates foundation conducted a study of

---

[33] Cecilia Kang, *Parking Lots Have Become a Digital Lifeline*, N.Y. Times (May 5, 2020), https://www.nytimes.com/2020/05/05/technology/parking-lots-wifi-coronavirus.html.

[34] Katherine Haan, *Public Wi-Fi Risks*, Forbes, https://www.forbes.com/advisor/business/public-wifi-risks (last visited June 6, 2024).

[35] *Broadband and Digital Equity*, City of Boston, (last visited June 6, 2024) https://www.boston.gov/departments/broadband-and-cable/broadband-and-digital-equity.

[36] Rohan Mattu, *Baltimore to Launch Free Public Wi-Fi in Effort to Bridge Digital Divide*, CBS News (Dec. 18, 2023), https://www.cbsnews.com/baltimore/news/baltimore-to-launch-free-public-wi-fi-in-effort-to-bridge-digital-divide.

[37] Press Release, Chicago Public Schools, *Chicago Launches Groundbreaking Initiative to Bridge Digital Divide, Providing Free High-Speed Internet Access to Over 100,000 CPS Students* (June 25, 2020), https://www.cps.edu/press-releases/chicago-launches-groundbreaking-initiative-to-bridge-digital-divide-providing-free-high-speed-Internet-access-to-over-100000-cps-students.

[38] Jessica Flores, *Oakland to Offer Free Internet for Public Housing Residents to Bridge Digital Divide*, S.F. Chronicle (May 7, 2023), https://www.sfchronicle.com/bayarea/article/oakland-free-Internet-access-18084366.php.

77 million people who could not access Internet at home and thus relied on the Internet at public libraries.[39] The study found that 32 million people (42 percent of visitors) used library computers for educational purposes, with 37 percent of these respondents using their local library computer to do homework. 30 million people (40 percent of visitors) used the Internet to apply for jobs. And 28 million people (37 percent of visitors) used library computers for health issues—82 percent of these respondents logged on to learn about a disease, illness, or medical condition and 33 percent searched for doctors or health care providers.[40]

Under the Court of Appeals' ruling, without the ability to afford private home Wi-Fi networks, those with less will be increasingly subject to the warrantless surveillance of their Internet activity. "Yet poor people are entitled to privacy, even if they can't afford all the gadgets of the wealthy for ensuring it." *Pineda-Moreno*, 617 F3d at 1123 (Kozinski, J., dissenting from denial of rehearing en banc). Under our Constitution, privacy should not be cost-prohibitive for some while available to others.

---

[39] Press Release, Bill & Melinda Gates Foundation, *Millions of People Rely on Library Computers for Employment, Health, and Education* (Mar. 25, 2010), https://www.gatesfoundation.org/ideas/media-center/press-releases/2010/03/millions-of-people-rely-on-library-computers-for-employment-health-and-education.

[40] *Id*.

CONCLUSION

The Court of Appeals incorrectly concluded that Simons does not have a constitutionally protected privacy interest in his Internet browsing history. The Court of Appeals' holding and reasoning advances an inconsistent and unsustainable standard for conducting the reasonable expectation of privacy analysis in the realm of Internet activity. There are important constitutional questions at stake in this case, and if this Court denies Simons's petition, it risks jeopardizing closely held Fourth Amendment rights and creating a "crazy quilt of the Fourth Amendment." *Smith,* 442 US at 745. For the foregoing reasons, *amici* urge this Court to overturn the Court of Appeals' ruling and remand to the trial court.

Respectfully submitted,

/s/ Kelly Simon
Kelly Simon, OSB #154213
ksimon@aclu-or.org
ACLU Foundation of Oregon, Inc.
P.O. Box 40585
Portland, OR 97240

Attorney for Amici Curiae

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the word count limitation in ORAP 5.05(1)(b)(ii)(A).

I certify that the size of the type in this brief is not smaller than 14 point for both the text of the brief and footnotes as required in ORAP 5.05(1)(d)(ii).

Dated this 20th day of June, 2024.

/s/ Kelly Simon
Kelly Simon, OSB #154213
ksimon@aclu-or.org
ACLU Foundation of Oregon, Inc.
P.O. Box 40585
Portland, OR 97240

Attorney for Amici Curiae

CERTIFICATE OF FILING AND SERVICE

I certify that on the 20th day of June, 2024, I filed the foregoing with the Appellate Court Administrator by electronic filing, and electronically served upon the following persons by using the court's electronic filing system:

KYLE KROHN #104301
Oregon Public Defense Commission
1175 Court Street NE
Salem, OR 97301
Kyle.Krohn@opds.state.or.us
Tel: (503) 378-3349

JOANNA HERSHEY #162665
400 Justice Building
1162 Court Street NE
Salem, OR 97301
Joanna.Hershey@doj.oregon.gov
Tel: (503) 378-4402

I further certify that I will provide a courtesy copy to the parties via electronic mail at the e-mail addresses listed above.

Dated this 20th day of June, 2024.

/s/ Kelly Simon
Kelly Simon, OSB #154213
ksimon@aclu-or.org
ACLU Foundation of Oregon, Inc.
P.O. Box 40585
Portland, OR 97240

Attorney for Amici Curiae