IN THE SUPREME COURT OF THE STATE OF OREGON

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

BRIEF OF *AMICI CURIAE* NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS ELECTRONIC FRONTIER FOUNDATION

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

Opinion Filed: December 13, 2023
Author of Opinion: Aoyagi, P.J.
Before: Aoyagi, Presiding Judge, and Joyce, Judge, and Jacquot, Judge.

JUSTIN N. ROSAS, #076412
Board of Directors,
National Association of Criminal
Defense Lawyers, Local Counsel
110 W. 11th St.
Medford, OR 97501

Cover continued on next page

ELLEN F. ROSENBLUM #753239
Attorney General
BENJAMIN GUTMAN #160599
Solicitor General
JENNIFER LLOYD #943724
Senior Assistant Attorney General

March 6, 2024

justin@justinrosas.com
Telephone: 541-245-9781

NICOLA MORROW*
MICHAEL W. PRICE NY 4771697
National Association of Criminal Defense Lawyers
1660 L St. NW, 12th Floor
Washington, DC 20036
(202) 872-8600
nmorrow@nacdl.org
* New York bar admission pending
Attorneys for Amicus Curiae for the National Association of Criminal Defense Lawyers

ANDREW CROCKER
CA SBN #296591
Electronic Frontier Foundation 815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org
Attorney for Amicus Curiae for Electronic Frontier Foundation

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
Phone: (503) 378-3349
Attorneys for Petitioner on Review

1162 Court St. NE
Salem, Oregon 97301-4096
jennifer.lloyd@doj.state.or.us
Telephone: (503) 378-4402
Attorneys for Respondent on Review

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

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 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400 (2012); *State v. Aranda*, 370 Or. 214 (2022); *In re J. C. N.-V.*, 359 Or. 559 (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 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014); *State v. Pittman*, 367 Or. 498 (2021); *State v. Nascimento*, 360 Or. 28 (2016)

INTRODUCTION

Internet users have a reasonable expectation of privacy in their browsing histories. They do not contract away their Fourth Amendment rights when they click through private user agreements. The Court of Appeals, however, incorrectly concluded that Mr. Simons did not have a reasonable expectation of privacy in his internet browsing history when he connected to a local restaurant's Wi-Fi network. *See* Opinion, *State v. Simons*, No. 19-cr-43543 (Dec. 13, 2023). In so doing, the Court ignored relevant case law affirming that internet browsing history contains some of the most revealing and sensitive personal information that exists, thereby warranting constitutional protection. *See, e.g., Riley v. California*, 573 U.S. 373 (2014); *Carpenter v. United States*, 585 U.S. 296 (2018); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 603 (9th Cir. 2020). The Court of Appeals was also mistaken in conflating the existence of a private user agreement containing a monitoring clause with a waiver of constitutional rights. Fourth Amendment privacy rights do not live and die by the varying and ever-changing

terms of service that appear in contracts of adhesion. *See Carpenter*, 585 U.S. at 310; *United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010); *Byrd v. United States*, 584 U.S. 395, 408 (2018).

When the government monitored and tracked Mr. Simons' internet activity without a warrant[1]—capturing over a years' worth of private communications—it conducted an unconstitutional search, violating Mr. Simons' Fourth Amendment rights. This case concerns important constitutional questions that threaten to compromise not only Mr. Simons' rights, but also the rights of all Oregonians. For the reasons detailed below, *amici* urge this Court to grant Mr. Simons' Petition for Review.

ARGUMENT

I. Mr. Simons Has A Reasonable Expectation of Privacy in His Browsing History Because It Contains the "Privacies of Life."

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. That right did not dissipate when Americans migrated their "papers" and "effects" from physical file cabinets to the digital

[1] Mr. Simons' briefing below explains the agency relationship between the government and the service provider. It also provides a detailed description of the government's conduct and correctly characterizes it as an invasive search. *See* Appellant's Opening Brief at 12–18, *State v. Simons*, No. 19-CR-43543 (Or. Ct. App. Aug. 10, 2022).

cloud. Reflecting this reality, the United States Supreme Court has for decades endeavored to ensure that people enjoy the same degree of privacy in the digital age that they did when the Fourth Amendment was adopted. *Carpenter*, 585 U.S. at 305. This endeavor has required updating 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 U.S. 27 (2001). Similarly, in *United States v. Jones*, the Supreme Court distinguished digital location tracking from physical surveillance and the analog public space doctrine. 565 U.S. 400 (2012) (holding that installing a GPS tracking device without a warrant violated the Fourth Amendment). 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 U.S. at 316–17. Together, these cases emphasize that people should be free to pursue their private lives in the digital world without fear of unfettered government surveillance. That freedom includes the right to browse the internet in private.

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). If this conclusion applies to a collection of GPS coordinates, then it certainly applies to the detailed, substantive portrait that is a person's browsing history. Instead of merely tracking a visit to the doctor, browsing history data can describe in detail a person's medical diagnosis. Instead of exposing a trip to a "potentially revealing" location, internet activity can explicitly relay a person's political and religious affiliations, sexual orientation, and immigration status. 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.[2] Browsing history data is exactly the kind of personal information that deserves constitutional protection under the Fourth Amendment.

---

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

In *Riley*, the Supreme Court cited browsing history repeatedly as an example of the type of deeply private information contained on a cell phone, suggesting that a warrantless search of a cell phone is unconstitutional in part because cell phones contain browsing history data. 573 U.S. 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"). The Ninth Circuit took this theory a step further in a civil case, concluding that internet users have a "reasonable expectation of privacy in their browsing histories." *See In re Facebook*, 956 F.3d at 603 (citation omitted). That case involved a statutory violation by a private entity, but the Court acknowledged that the "Fourth Amendment imposes higher standards on the government than those 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 U.S. at 304–05); *see also Riley*, 573 U.S. at 397–99; *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008).

It is worth noting that in the instant case, the government did not have access to only a limited slice of Mr. Simons' browsing history; to the contrary, police tracked his internet activity for over a year without a warrant. While any amount of browsing history data is revealing, a year's worth of internet activity paints an intimately detailed portrait of the internet user. As in *Carpenter*, this Court should consider that the privacy interest only increases as the duration of surveillance increases. *See Carpenter*, 585 U.S. at 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").

Relevant case law reflects the fact that because internet activity is deeply private and contains the kind of sensitive information that the Fourth Amendment was meant to protect from government surveillance, internet users—including the defendant in this case—possess a reasonable expectation of privacy in their browsing history. The government cannot intrude on that expectation of privacy without a warrant.

II. "User Agreements" Cannot Vitiate Constitutional Rights and Liberties.

Users have a reasonable expectation of privacy in their internet browsing histories even when the internet service provider includes monitoring terms in its user agreement. 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 U.S. 735, 740 n.5 (1979). The fact that private businesses may monitor internet activity to protect their own commercial interests does not license the *government* to sidestep a constitutional warrant requirement. The loss of constitutional privacy rights should not be the price of "participation in modern society." *Carpenter*, 585 U.S. at 315.

In *Warshak*, for example, the Sixth Circuit found a reasonable expectation of privacy in subscriber information even though the email service provider's user agreement included a monitoring clause like the one at issue in this case. 631 F.3d at 287. And in *Byrd*, the Supreme 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 U.S. 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.* *Carpenter* 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 U.S. 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]").

It is common practice for communications companies to notify users about monitoring policies put in place to identify and stop illegal or objectionable activity on the company's private platform. *See, e.g., Warshak*, 631 F.3d at 287. But these reservations of rights are almost never negotiated, and if users want to participate in activities "indispensable to participation in modern society"—like sending emails or accessing the internet—they have no choice but to click "I agree." *Carpenter*, 585 U.S. at 315 (citing *Riley*, 573 U.S. at 385); *see also Warshak*, 631 F.3d at 287. In its opinion below, the Court of Appeals challenged this analogy, asserting 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.'" Opinion, *State v. Simons*, No. 19-cr-43543 (Dec. 13, 2023). But nearly all of us rely on Wi-Fi networks outside of our own homes. We open our laptops at a local coffee shop to send work emails and read the news; we log on to a computer at the library to place a book on hold; we connect to a friend's Wi-Fi network on a weekend afternoon to stream a film or get started on our taxes. Characterizing public Wi-Fi networks as merely "convenient" does not acknowledge the centrality of the internet in modern life or the well-documented inequality of internet access that often tracks racial and class-based

marginalization.[3] Fourth Amendment rights are held by everyone, not just those with their own private residences and a monthly budget for a private, password-protected Wi-Fi network.[4] It would be deeply unfair to subject people without access to their own private internet connection to warrantless government surveillance, people who invariably require access to the internet to "participat[e] in modern society"—to read the news, peruse job listings, research political candidates, and more—just because they cannot afford their own Wi-Fi networks.

Finally, the lower court's decision threatens to make a "crazy quilt of the Fourth Amendment." *Smith*, 442 U.S. at 745 (holding that the reasonable expectation of privacy analysis cannot be dictated by private corporate practices); *see also United States v. Thomas*, 447 F.3d 1191, 1198 (9th Cir. 2006) (holding that the "technical violation of a leasing contract" is insufficient to vitiate an unauthorized renter's legitimate expectation of privacy in a rental car); *United States v. Owens*, 782 F.2d 146, 150 (10th Cir. 1986) (holding that a motel's private terms do not govern the lodger's expectation of privacy). If this Court allows

---

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

[4] This is the principle that animates the Fourth Amendment is Not for Sale Act. *See* H.R. 4639, Fourth Amendment Is Not For Sale Act, *available at* https://www.cbo.gov/publication/59756#:~:text=Summary,companies)%20from%20a%20third%20party.

Fourth Amendment rights to be dictated by various corporate contracts of adhesion, then each internet user would experience a different level of constitutional protection against government surveillance of their browsing history depending on the relevant terms of service drafted by the service provider.[5] This is not only an absurd result, but also an impracticable one. If the Court of Appeals' holding and rationale prevails, Fourth Amendment 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 the Constitution. *See Smith*, 442 U.S. at 745.

CONCLUSION

The Court of Appeals was wrong in concluding that Mr. Simons does not have a constitutionally protected privacy interest in his internet browsing history and advanced an inconsistent and unsustainable standard for conducting the reasonable expectation of privacy analysis. There are important constitutional questions at stake in this case, and if this Court denies Defendant's petition, it risks jeopardizing closely held Fourth Amendment rights and creating a "crazy quilt of

[5] It is worth noting that companies change their terms of service regularly, often with little or no notice.

the Fourth Amendment." *Id*. at 745. For the foregoing reasons, *amici* urge this Court to accept Defendant's petition for review.

Respectfully Submitted,

/s/ Justin N. Rosas
Justin N. Rosas, OSB 076412
Nicola Morrow*
Michael Price
Attorneys for Proposed Amicus
National Association of Criminal
Defense Lawyers

*Pending Admission in NY

/s/ Andrew Crocker
Andrew Crocker
Attorney for Proposed Amicus
Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE

I certify that (1) BRIEF OF *AMICUS CURIAE* complies with the word count limitation in ORAP 9.05(3)(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 by ORAP 5.05(3)(b).

/s/ Justin N. Rosas

JUSTIN N. ROSAS, OSB #076412
Attorney for *Amicus Curiae*
National Association of Criminal
Defense Lawyers

NOTICE OF FILING AND PROOF OF SERVICE

I certify that on March 6, 2024, I filed Brief of Amici Curiae in Support of Petition for Review to be electronically filed with the Appellate Court Administrator, Appellate Records Section, by using the electronic filing system.

I further certify that counsel for the petitioner, Kyle Krohn and respondent, Jennifer Lloyd, will be served via the efiling system.

/s/ Justin N. Rosas

Justin N. Rosas OSB 076412
Board of Directors, NACDL
justin@justinrosas.com
Attorney for *Amicus Curiae*
National Association of Criminal
Defense Lawyers