No. 20-1204

IN THE

Supreme Court of the United States

MARK RINGLAND,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Eighth Circuit

BRIEF OF THE DKT LIBERTY PROJECT, REASON FOUNDATION, AND DUE PROCESS INSTITUTE AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

JESSICA RING AMUNSON
Counsel of Record
CAROLINE C. CEASE
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
jamunson@jenner.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS AND STATUTES

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*[1]

Amici curiae are non-profit organizations dedicated to the protection of individual liberties, especially those guaranteed by the Constitution of the United States. *Amici* have a particular interest in defending individual liberties against novel and unprecedented government encroachment in today's digital world. The vast amount of sensitive and personal information available in Americans' email accounts necessarily means that searches of those devices "would typically expose to the government far more than the most exhaustive search of a home." *Riley v. California*, 573 U.S. 373, 396-97 (2014). The decision of the Eighth Circuit below, therefore, poses a serious threat to individual liberty. *Amici* are the following:

The DKT Liberty Project was founded in 1997 to promote individual liberty against encroachment by all levels of government. The Liberty Project is committed to defending privacy, guarding against government overreach, and promoting every American's right and responsibility to function as an autonomous and independent individual. The Liberty Project espouses vigilance against government overreach of all kinds, but especially with respect to restrictions on individual civil liberties. In particular, over the past two decades the

---

[1] Pursuant to Rule 37.2(a), counsel for *amici curiae* provided timely notice to counsel of record for all parties of *amici*'s intention to file this brief. Counsel of record for Petitioner and Respondent have both consented to the filing of this brief. Pursuant to Rule 37.6, *amici* affirms that no counsel for a party authored this brief in whole or in part, and no person other than *amici* or their counsel made a monetary contribution to this brief's preparation or submission.

Liberty Project has filed briefs as *amicus curiae* with this Court in significant cases addressing the application of the Fourth Amendment to advances in technology, including *Kyllo v. United States* (No. 99-8508), *Riley v. California* (No. 13-132), and *Carpenter v. United States* (No. 16-402).

Reason Foundation is a national, nonpartisan, and nonprofit public policy think tank, founded in 1978. Reason's mission is to advance a free society by applying and promoting libertarian principles and policies—including free markets, individual liberty, and the rule of law. Reason supports dynamic market-based public policies that allow and encourage individuals and voluntary institutions to flourish. Reason advances its mission by publishing *Reason* magazine, as well as commentary on its websites, and by issuing policy research reports. To further Reason's commitment to "Free Minds and Free Markets," Reason participates as *amicus curiae* in cases raising significant constitutional or legal issues.

Due Process Institute is a nonprofit, bipartisan, public interest organization that works to honor, preserve, and restore procedural fairness in the criminal justice system because due process is the guiding principle that underlies the Constitution's solemn promises to "*establish justice*" and to "*secure the blessings of liberty*." U.S. Const., pmbl.

SUMMARY OF ARGUMENT

Access to an email account is rapidly becoming essential in today's interconnected world. Communications—and storage of personal documents—via email have become ubiquitous. Americans use their email accounts to carry out essential tasks in their day-to-day lives, like communicating with loved ones, working with colleagues, collaborating with fellow students and teachers, making appointments with physicians and therapists, and so much more. Email has become even more important during the COVID-19 pandemic as virtual connections have become the norm. Even the most basic tasks can require—or at least can be made easier by—email.

Like many Americans, and many internet users worldwide, petitioner Mark Ringland registered for and used Gmail addresses to send and receive emails. Through the use of "hashing,"[1] Google flagged possible illegal content in one of Mr. Ringland's email accounts. Google reviewed a subset of Mr. Ringland's emails, and then sent a larger set—including that reviewed subset—

---

[1] "[H]ash[ing]" has been described as "a sort of digital fingerprint," which assigns a "short string of characters generated from a much larger string of data" in a way that makes it "highly unlikely another set of data will produce the same value." *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016) (Gorsuch, J.). In other words, hashing is used to confirm and locate copies of the identified data that are identical, here allowing Google to match the contents of Mr. Ringland's files with files previously identified as containing unlawful content. *See generally* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38-39 (2005).

to the National Center for Missing and Exploited Children. Ultimately the emails were sent to state law enforcement, which—without obtaining a warrant—accessed and reviewed the files Google had transmitted. Based on that review, an investigator ultimately obtained a warrant to search Mr. Ringland's relevant email account. This same process then happened a second time, that time related to material from another of Mr. Ringland's accounts. After being charged, Mr. Ringland challenged the searches of the emails sent from Google, alleging that he had a reasonable expectation of privacy in his personal emails and that the search constituted a trespass. The district court and the Eighth Circuit upheld the searches under the private-search doctrine announced by this Court in *United States v. Jacobsen*, 466 U.S. 109 (1984); neither court addressed Mr. Ringland's trespass argument.

The decisions below were wrong to rely on the private-search doctrine without even considering whether the searches were a trespass. The private-search doctrine is insufficiently protective of Fourth Amendment interests, particularly when extended uncritically to digital media like emails. The emails of today are nothing like the letters of yesteryear, in capability, content, or size. Yet the courts below and courts across the country have rotely applied the private-search doctrine to email searches such as the one at issue here as if emails were equivalent to letters or documents in a cardboard box, without even considering the traditional understanding of the Fourth Amendment and the limits on its exceptions. Simply put, the private-search doctrine does not appropriately safeguard the

Fourth Amendment interests at issue when the search involves digital mediums like email accounts given the vast array of intimate details that can be learned about a person from the information accessible on her email account—personal communications, health information, education-related information, and financial statements, to name a few.

Instead, the traditional property-based understanding of the Fourth Amendment, which is grounded in whether the search was a trespass, is best equipped to handle searches of email. Unlike the scenario presented in *Jacobsen* of a DEA agent re-opening a cardboard box, a law enforcement officer confronted with a set of emails that have been accessed by a third party cannot possibly be certain of the emails' contents or that additional private information will not be disclosed. Nor can it seriously be maintained that a reasonable individual, by using an email account serviced by a third party, thereby grants an implied license *to the government* to rifle through her emails.

Without this Court's intervention, the vast amount of information accessible through an individual's emails will remain subject to warrantless searches. The government could use the private-search doctrine to justify warrantless searches into emails whenever a third-party service provider has some reason—correct or not—to believe the email contains evidence of a crime. Rejection of the trespass approach under circumstances such as this could lead to expansive warrantless searches and vast digital surveillance.

This Court should grant the petition for a writ of certiorari to clarify the applicability of the trespass

approach under the Fourth Amendment to warrantless searches of email such as those conducted here.

ARGUMENT

I. Email Is An Essential Feature Of Modern Life, Critical To Individuals' Liberty And Ability To Engage In Society.

Mr. Ringland owned and used a Gmail account to send and receive emails. His doing so was unexceptional. Email usage is ubiquitous in America today. As of 2019, there were approximately 3.9 billion active email users, and over 90% of all internet users in the United States use email.[2] Globally, more than 293 billion business and consumer emails are sent per day.[3] Since its launch in 2004, Gmail—the same email service Mr. Ringland used—has amassed more than 1.5 billion global active users,[4] and the service boasts more than 1.2 billion monthly active users.[5] One report estimates that,

---

[2] *See* Joseph Johnson, *Percentage of Internet Users in the United States Who Use E-Mail as of November 2019*, Statista (Jan. 27, 2021), https://www.statista.com/statistics/628372/us-email-usage-reach-by-gender/.

[3] Radicati Grp., Inc., *Email Statistics Report, 2019-2023*, at 2 (2019), https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf.

[4] Jennifer Elias & Magdalena Petrova, *Google's Rocky Path to Email Domination*, CNBC (Oct. 26, 2019), https://www.cnbc.com/2019/10/26/gmail-dominates-consumer-email-with-1point5-billion-users.html.

[5] Motek Moyen, *Gmail is Very Popular But Google Still Won't Fix a Security Vulnerability*, Seeking Alpha (July 17, 2017), https://seek

in the United States, nine in ten internet users send email regularly, "making it one of the most common digital activities in the" country.[6]

Emails largely have replaced (and drastically enhanced the amount of information that can be transmitted as compared to) letters as Americans' primary written communication method.[7] For example, in 2014, the U.S. Postal Service handled approximately 150 billion pieces of mail—which amounted to about the number of emails sent *every day* worldwide.[8] Not only that, emails can transmit far more information than one or a series of letters could provide. For example, a Gmail user can send up to 25 megabytes of material in one email alone.[9] That is the equivalent of at least 6,250

---

ingalpha.com/article/4088241-gmail-is-popular-google-still-wont-fix-security-vulnerability.

[6] Nicole Perrin, *Email Marketing 2019*, eMarketer (Oct. 10, 2019), https://www.emarketer.com/content/email-marketing-2019.

[7] Randolph E. Schmid, *You Never Write Any More; Well, Hardly Anyone Does*, NBC News (Oct. 3, 2011), https://www.nbcnews.com/id/wbna44760552 ("For the typical American household these days, nearly two months will pass before a personal letter shows up.").

[8] *See* Andrew G. Ferguson, *The "Smart" Fourth Amendment*, 102 Cornell L. Rev. 547, 599 (2017).

[9] *See* Stephanie Fisher, *3 Ridiculously Easy Ways You Can Email A Large File*, Mojo Media Labs (Aug. 31, 2018), https://www.mojomedialabs.com/blog/3-ridiculously-easy-ways-you-can-email-a-large-file.

single spaced pages of Microsoft Word documents.[10] What at one time would have required the space of multiple file cabinets can now be contained in a handful of emails.

In short, "millions of Americans everyday" use and transmit a wealth of information over email,[11] and usage has only grown since the COVID-19 pandemic began.[12] Americans use email to converse and share pictures and documents with family and friends, make appointments, receive receipts, and even to store data—users often scan documents and email the documents to themselves. Many email services also offer chat functions, such as G-Chat, in which the user may share additional personal information, including photographs. In short, email accounts are treasure troves of user information, which often is personal, proprietary, or private.

Moreover, an individual's liberty and ability to meaningfully engage in society now often depends on access to email. "Possession of an email account has

---

[10] Per Christensson, *How Many Pages of Text Will One Megabyte Hold?*, PC Help Center (July 3, 2005), https://pc.net/helpcenter/answers/how_much_text_in_one_megabyte#:~:text=And%20this%20is%20pretty%20simple,text%20to%20equal%20one%20megabyte.

[11] Orin S. Kerr, *The Fourth Amendment and New Technologies*, 102 Mich. L. Rev. 801, 869 (2004).

[12] *See* Minh Hao Nguyen, et al., *Changes in Digital Communication During the COVID-19 Global Pandemic*, Social Media + Society (July – Sept. 2020) (noting that 24% of U.S. adults reported an increase in email usage for communicating with friends and family compared to before the pandemic).

become a must . . . for both personal communication as well as professional communication" and "is considered of equivalent importance to that of having a cell-phone number."[13] Given its omnipresence, it can be exceedingly difficult for individuals to build a community, keep in touch with loved ones, or access basic services without email. For example, oftentimes one needs an email address to, among other things, apply for a job, order a package, make an appointment, pay a bill, and—these days—register for a COVID-19 vaccine.[14] From the critical to mundane, email remains a necessary feature of modern life.

Intimate family and friend associations are developed and maintained by email, particularly among young people.[15] A study found that 61% of respondents considered email most important for maintaining contact

---

[13] Rajani Mevada, *Significance of Email Communication in Today's World*, 2 Int'l J. Advance Rsch. Comput. Sci. & Mgmt. Stud. 40, 43 (Jan. 2014).

[14] *See, e.g.*, *Vaccine Management Patient Portal Guide*, Arizona Department of Health Services, https://www.azdhs.gov/documents/preparedness/epidemiology-disease-control/infectious-disease-epidemiology/novel-coronavirus/vaccine/patient-portal-user-guide.pdf (requiring the entry of an email address).

[15] *See, e.g.*, Amanda Lenhart *et al.*, *Teens, Technology, & Friendships*, Pew Rsch. Ctr., at 10 (2015), http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/08/Teens-and-Friendships-FINAL2.pdf.

with extended family.[16] With respect to work, email is critical. When searching for work, applicants regularly use email to follow up on applications with prospective employers.[17] And, for those who have employment, one study showed that on average employees spend more than five hours a day using email, either reading emails or sending them.[18]

The record in this case, then, reflects the position many individuals are likely to find themselves in today: establishing an email account and filling that account with private correspondence, documents, and photographs. What most people fail to realize is that the service provider of that email account—for example, Google—may use hashing technology to algorithmically identify content in that user's email account. The application of hashing technology may be applied to a user's account even if the service provider has absolutely no suspicion that the user is engaging in criminal conduct. But if hashing does identify content in a user's account that the service provider believes may constitute illegal activity, the service provider then can

---

[16] Judy Wajcman, Michael Bittman & Judith E. Brown, *Families Without Borders: Mobile Phones, Connectedness and Work-Home Divisions*, 42 Sociology 635, 646 (2008).

[17] Aaron Smith, *Searching for Work in the Digital Era*, Pew Rsch. Ctr., at 2 (2015), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2015/11/PI_2015-11-19-Internet-and-Job-Seeking_FINAL.pdf.

[18] Abigail Johnson Hess, *Here's How Many Hours American Workers Spend on Email Each Day*, CNBC: MakeIt (Sept. 22, 2019), https://www.cnbc.com/2019/09/22/heres-how-many-hours-american-workers-spend-on-email-each-day.html.

review that content and send it on to law enforcement for review. And all of this occurs without any warrant issuing. Thus, Mr. Ringland's situation is not unique; it is likely to recur with some frequency.

II. Given The Vast Amount Of Material Stored In Email Accounts, Rejection Of The Trespass Approach Could Lead To Expansive Warrantless Searches.

The Fourth Amendment protects the right of people to be secure in their "houses, papers, and effects." U.S. Const. amend. IV. As described above, in today's world, a person's papers and effects often are predominantly housed in emails. Given these practicalities, emails could be conceived of as "akin to a residence in terms of the scope and quantity of [the] private information [they] may contain." *United States v. Ulbricht*, 858 F.3d 71, 99 (2d Cir. 2017) (quotation marks omitted) (first bracket added), *abrogated on other grounds by Carpenter v. United States*, 138 S. Ct. 2206 (2018). Indeed, emails can provide access to even more information than can be found in the "sanctity of the home," where, this Court has long maintained, "*all* details are intimate." *Kyllo v. United States*, 533 U.S. 27, 37 (2001). Emails, like cell phones, hold "the privacies of life," *Riley v. California*, 573 U.S. 373, 403 (2014) (quotation marks omitted).

The lower courts' rote application of the private-search doctrine announced in 1984 to today's digital world does not account for the Fourth Amendment interests at stake. "When confronting new concerns wrought by digital technology," this Court has "been careful not to uncritically extend existing precedents." *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018).

And yet, the lower courts simply have equated the search of a cardboard box in *Jacobsen* with the search of email accounts in cases like Mr. Ringland's without questioning whether the Fourth Amendment's traditional protections—beyond those based in a reasonable expectation of privacy—are applicable and would better provide a bulwark against Fourth Amendment violations.

This Court has been careful when it comes to the Fourth Amendment's application to new technology. As this Court has recognized in both *Riley* and *Carpenter* when concluding that the rationales underpinning other exceptions to the warrant requirement did not map onto the realities of today's digital devices, technology permits an individual to hold a significant amount of information in one place. In *Riley*, this Court unanimously refused to extend the search-incident-to-arrest exception to permit warrantless searches of cell phones because cell phones "differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person." 573 U.S. at 393. Likewise, in *Carpenter*, this Court declined to apply the third-party doctrine to a person's historical cell-site records because those records supply an "all-encompassing record of the holder's whereabouts" and can provide "an intimate window into a person's life" with "just the click of a button." 138 S. Ct. at 2217-18. This Court explained that applying those exceptions to cell phones would, in effect, closely approach the very same general warrants that the Fourth Amendment was intended to reject. *See, e.g.*, *Riley*, 573 U.S. at 403.

The same is true here, and demonstrates why the trespass approach is more appropriate than the private-search doctrine in cases such as this involving searches of email. Like a cell phone, email accounts and other forms of electronic storage can contain a "greater quantity and variety of information than any previous storage method," increasing the likelihood that "highly personal information, irrelevant to the subject of" any lawful investigation, may also be searched. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 105 (1994). Permitting law enforcement to evade the warrant requirement by use of the private-search doctrine for email accounts is inconsistent with this Court's decisions in *Riley* and *Carpenter*.

In *United States v. Jones*, 565 U.S. 400 (2012), this Court emphasized that separate and apart from the reasonable expectations standard (which underlies the private-search doctrine), a "physical intrusion" by the government to "occup[y] private property for the purpose of obtaining information" always constitutes a search within the meaning of the Fourth Amendment. 565 U.S. at 404-05. Thus, the Fourth Amendment is "understood to embody a particular concern for government trespass upon the areas" enumerated in the amendment. *Id.* at 406. Under the trespass approach, it matters not whether a private party first engaged in the trespass; the government is not permitted to trespass upon "persons, houses, papers, and effects" full stop. U.S. Const., amend. IV; *see* Andrew MacKie-Mason, *The Private Search Doctrine After* Jones, 126 Yale L.J. F. 326, 331 (2017) (under trespass theory, "[t]he fact that

someone has previously entered or interfered does almost nothing to erode the interest in exclusion").

A reasonable individual, by using an email service, would not consider herself to have relinquished her possessory interest in her property to any and all third-parties. And certainly it cannot seriously be maintained that an individual using an email service provider has granted an implied license *to the government* to rifle through her emails just by signing up for an email account. The decision below, which flatly ignored Mr. Ringland's trespass theory, cannot be squared with *Jones*.

Indeed, a rejection of the *Jones* trespass approach could open the door for the government actually to compel email service providers to search for—and provide to the government—anything that could be evidence of illegality. For example, the government could compel email service providers to search for and transmit to the government evidence of copyright infringement, *see* 18 U.S.C. § 506 (criminal copyright infringement), trade secret theft, *see* 18 U.S.C. § 1832 (criminal theft of trade secrets), or any other number of crimes.

The power to compel a private entity to search for and produce evidence of criminal conduct is problematic on many fronts, but not least because it asks the private company to determine how to identify the information and what to send to the government. While perhaps some small number of entities may be well-equipped under certain circumstances to identify certain limited information, history has shown that a private company's use of algorithms often ends poorly. *See, e.g.*, Sang Ah

Kim, *Social Media Algorithms: Why You See What You See*, 2 Geo. L. Tech. Rev. 147, 152-54 (2017) (discussing shortcomings of algorithms, which are "written by humans" and therefore "flaw[ed] and bias[ed]").

In other words, a failure to consider the search of emails as a trespass would permit law enforcement—without obtaining a warrant—to (1) compel private companies to search for material, which in turn requires those companies to determine on their own whether the material might be probative of the crime at issue, (2) then require those companies hand over that material to the government, which could (3) again, without a warrant, then review the material *regardless* of whether the emails had *any* relation to a crime. Simply put, a company employing a particularly bad algorithm might find itself sending the government the user's personal and entirely lawful emails to his mother, his privileged emails to his attorney, emails to a business partner containing proprietary information, or his emails to his physician about medical issues for which he seeks advice.

That result is irreconcilable with the Fourth Amendment. The warrant requirement "serves a high function" by interposing "a magistrate between the citizen and the police" to neutrally "weigh the need to invade [an individual's] privacy in order to enforce the law," and to particularly describe the scope and limits of any subsequent search. *McDonald v. United States*, 335 U.S. 451, 455 (1948). Allowing the lower courts' decisions to stand could permit government officials to circumvent this warrant requirement for a vast amount of information—about which it cannot be certain, or even

confident, relates to any crime (much less the specific crime at issue)—contained in an individual's email account.

Emails are necessary to individuals' everyday lives and their ability to engage with society. But they also make accessible a vast array of intimate information. This Court should grant review to reconsider the approaches taken by the lower courts that have insulated expansive warrantless searches of email by law enforcement from Fourth Amendment protection.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

April 14, 2021

Respectfully submitted,

JESSICA RING AMUNSON
Counsel of Record
CAROLINE C. CEASE
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
jamunson@jenner.com

Counsel for Amici Curiae