No. 16-402

IN THE
Supreme Court of the United States

TIMOTHY IVORY CARPENTER,
Petitioner,
v.

UNITED STATES,
Respondent.

ON WRIT OF CERTIORARI TO THE
UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

BRIEF FOR TECHNOLOGY COMPANIES AS AMICI CURIAE IN SUPPORT OF NEITHER PARTY

SETH P. WAXMAN
Counsel of Record
JONATHAN G. CEDARBAUM
CATHERINE M.A. CARROLL
ROBBIE MANHAS
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Ave., NW
Washington, DC 20006
(202) 663-6000
seth.waxman@wilmerhale.com

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES iii

STATEMENT OF INTEREST 1

SUMMARY OF ARGUMENT 9

ARGUMENT 12

I. FOURTH AMENDMENT DOCTRINE MUST ADAPT TO THE CHANGING REALITIES OF THE DIGITAL ERA 12

A. Digital Data And Devices Are Pervasive, Personal, And Often Necessary To Modern Life 14

B. Users Of Digital Technologies Cannot Avoid Transmitting Sensitive Data To Service Providers, But They Expect That Data To Remain Private 17

C. Amici's Compliance With Law-Enforcement Requests Respects User Privacy 21

II. RIGID ANALOG-ERA RULES SHOULD YIELD TO CONSIDERATION OF REASONABLE EXPECTATIONS OF PRIVACY IN THE DIGITAL AGE 23

A. A Flexible Test Grounded In Today's Reasonable Expectations Of Privacy Should Govern In The Digital Context 23

B. Transmission To A Service Provider Should Not Automatically Foreclose Protection Of Digital Data 26

TABLE OF CONTENTS—Continued

Page

C. "Non-Content" Digital Data Should Not Automatically Be Excluded From Protection 29

CONCLUSION 32

TABLE OF AUTHORITIES

CASES

Page(s)

Ex parte Jackson, 96 U.S. 727 (1878) 29, 30

In re Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 (3d Cir. 2015) 32

Katz v. *United States*, 389 U.S. 347 (1967) 24

Kyllo v. *United States*, 533 U.S. 27 (2001) 12, 25, 28

Missouri v. *McNeely*, 133 S. Ct. 1552 (2013) 21

NAACP v. *Alabama*, 357 U.S. 449 (1958) 32

Oliver v. *United States*, 466 U.S. 170 (1984) 23

Packingham v. *North Carolina*, 137 S. Ct. 1730 (2017) 12, 15, 17, 26

Riley v. *California*, 134 S. Ct. 2473 (2014) ..... *passim*

Smith v. *Maryland*, 442 U.S. 735 (1979) 12, 26, 27, 28

State v. *Zeller*, 172 Wash. App. 1008 (2012) 21

United States v. *Dotson*, 715 F.3d 576 (6th Cir. 2013) 17

United States v. *Figueroa*, 2008 WL 5423982 (E.D. Wis. Dec. 30, 2008) 14

United States v. *Holm*, 326 F.3d 872 (7th Cir. 2003) 17

United States v. *Jones*, 565 U.S. 400 (2012) 18, 24, 25, 27, 30

TABLE OF AUTHORITIES—Continued

Page(s)

United States v. *Karo*, 468 U.S. 705 (1984) 25, 28

United States v. *LaCoste*, 821 F.3d 1187 (9th Cir. 2016) 14, 17

United States v. *Miller*, 425 U.S. 435 (1976) 12, 26

United States v. *Peterson*, 248 F.3d 79 (2d Cir. 2001) 25

United States v. *Pineda-Moreno*, 617 F.3d 1120 (9th Cir. 2010) 31

United States v. *Sofsky*, 287 F.3d 122 (2d Cir. 2002) 14

United States v. *Voelker*, 489 F.3d 139 (3d Cir. 2007) 25

United States v. *Warshak*, 631 F.3d 266 (6th Cir. 2010) 21, 23, 29, 30

DOCKETED CASES

Microsoft v. *United States*, No. 16-cv-00538 (W.D. Wash.) 22

STATUTES, RULES AND LEGISLATIVE MATERIALS

Stored Communications Act, 18 U.S.C. § 2703 ..... 21, 30

Fed. R. Crim. P. 4.1 21

H.R. Rep. No. 114-528 (2016) 21

TABLE OF AUTHORITIES—Continued

Page(s)

OTHER AUTHORITIES

Anderson, Monica, *6 Facts About Americans and their Smartphones*, Pew Res. Ctr., Apr. 1, 2015, http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/ 14

Apple Inc., *Legal Process Guidelines: Government & Law Enforcement Within the United States*, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (visited Aug. 13, 2017) 22

Apple Inc., *Privacy Policy*, https://www.apple.com/legal/privacy/en-ww/ (visited Aug. 14, 2017) 20

Apple Inc., *Report on Government and Private Party Requests for Customer Information*, https://images.apple.com/legal/privacy/transparency/requests-2016-H2-en.pdf (visited Aug. 13, 2017) 22

Bellovin, Steven M. et al., *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1 (2016) 17, 18

Bowman, Courtney M., *A Way Forward After* Warshak: *Fourth Amendment Protections for E-mail*, 27 Berkeley Tech. L.J. 809 (2012) 15

TABLE OF AUTHORITIES—Continued

Page(s)

CTIA, *Semi-Annual Wireless Industry Survey* (2011), http://files.ctia.org/pdf/CTIA_Survey_MY_2011_Graphics.pdf (visited Aug. 14, 2017) 13

Crist, Ry, *Home Automation Buying Guide*, C|Net (Apr. 28, 2017 9:07 a.m.), https://www.cnet.com/news/smart-home-buying-guide-home-automation/ 16

Colb, Sherry F., *What Is A Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of A Remedy*, 55 Stan. L. Rev. 119 (2002) 29

Dewey, Caitlin, *How Many Hours of Your Life Have You Wasted on Work Email? Try our Depressing Calculator*, Wash. Post, Oct. 3, 2016, https://www.washingtonpost.com/news/the-intersect/wp/2016/10/03/how-many-hours-of-your-life-have-you-wasted-on-work-email-try-our-depressing-calculator/?utm_term=.54666f34830d 14

Dropbox, Inc., *Privacy Policy*, https://www.dropbox.com/privacy (visited Aug. 14, 2017) 20

Dropbox, Inc., *Transparency Overview*, https://www.dropbox.com/transparency (visited Aug. 13, 2017) 22

TABLE OF AUTHORITIES—Continued

Page(s)

Facebook, Inc., *Two Billion People Coming Together on Facebook* (June 27, 2017), https://newsroom.fb.com/news/2017/06/two-billion-people-coming-together-on-facebook/ 15

Google Inc., *Cloud Platform Security*, https://cloud.google.com/security/compliance (visited Aug. 13, 2017) 20

Google Inc., *Privacy, Your Security Comes First in Everything We Do*, https://privacy.google.com/your-security.html (visited Aug. 13, 2017) 20

Madden, Mary & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center, May 20, 2015, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ 19

Madden, Mary, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center (Nov. 14, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ 18

Marya, Radhika, *Cellphones are now essentials for the poor*, USA Today, Sept. 14, 2013, https://www.usatoday.com/story/money/personalfinance/2013/09/14/cellphones-for-poor-people/2805735/ 14

TABLE OF AUTHORITIES—Continued

Page(s)

Mastroianni, Brian, *Survey: More Americans Worried About Data Privacy than Income*, CBS News, Jan. 28, 2016, http://www.cbsnews.com/news/truste-survey-more-americans-concerned-about-data-privacy-than-losing-income/ 19

Meeker, Mary, *2016 Internet Trends Report*, Kleiner Perkins Caufield & Byers (June 1, 2016), http://www.kpcb.com/blog/2016-internet-trends-report 15

Microsoft Trust Center, *Security, Audits, and Certifications*, https://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Security_Audit.htm (visited Aug. 13, 2017) 20

National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Emerging Technologies: Strategic Vision Executive Summary* (May 18, 2017), https://www.dhs.gov/sites/default/files/publications/Draft%20NSTAC%20ETSV%20Report%20Executive%20Summary%20508%20Compliant_1.pdf 16

Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 Harv. L. Rev. 1924 (2017) 16, 27

TABLE OF AUTHORITIES—Continued

Page(s)

Organisation for Economic Co-operation Development, *Bridging the Digital Divide*, https://www.oecd.org/site/schoolingfortomorrowknowledgebase/themes/ict/bridgingthedigitaldivide.htm (visited Aug. 13, 2017) 13

Parlante, Nick, *The Internet-TCP/IP, CS101—Introduction to Computing Principles*, CS01, https://web.stanford.edu/class/cs101/network-3-internet.html (visited Aug. 13, 2017) 17

Pesciotta, Daniel T., *I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century*, 63 Case W. Res. L. Rev. 187 (2012) 28

Pew Research Center, *Mobile Fact Sheet* (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ 13

Pew Research Center, *Online Shopping and E-Commerce* (Dec. 19, 2016), http://www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce/ 15

Radicati Group, Inc., *Email Statistic Report, 2017-2021* (Feb. 6, 2017), http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf. 13

Shuler, Rus, *How Does The Internet Work?* (2002), https://www.scribd.com/document/316562293/Rus-Shuler-How-Does-the-Internet-Work 17

TABLE OF AUTHORITIES—Continued

Page(s)

Silliman, Craig, *Musing About the Third Party Doctrine During Network Planning Meetings* (Oct. 10, 2016), https://www.linkedin.com/pulse/musing-third-party-doctrine-during-network-planning-craig-silliman 31

Snap Inc., *Transparency Report*, https://www.snap.com/en-US/privacy/transparency/2015-02-28 (visited Aug. 13, 2017) 22

Twitter Inc., *Transparency Report: United States*, https:// transparency. twitter.com/en/countries/us.html (visited Aug. 13, 2017) 22

United States Government Accountability Office, *Internet of Things: Communities Deploy Projects By Combining Federal Support With Other Funds And Expertise*, GAO-17-570 (July 2017) 16, 17

Warner, Timothy L., *Protect Your Online Privacy by Removing Exif Data from Your Photos*, Que Publishing (May 15, 2014), http://www.quepublishing.com/articles/article.aspx?p=2216446 16

Wasik, Bill, *In the Programmable World, All Our Objects Will Act As One*, Wired, May 14, 2013 6:30 a.m., https://www.wired.com/2013/05/internet-of-things-2/ 16

STATEMENT OF INTEREST[1]

Amici are the world's leading technology companies. Billions of people rely daily on amici's search engines, email services, social networks, smartphones, cloud storage, Internet-based devices and applications, and wireless networks for their businesses and personal lives.

Amici have a substantial interest in the legal standards governing law-enforcement access to data about their customers. Those customers entrust amici with some of their most intimate information, including what they search, where they are, and details of their daily lives. Given the sensitivity of this data, amici work continuously to secure their customers' privacy. And amici agree that Fourth Amendment doctrine should recognize that, in the evolving digital era, where such data is disclosed to or collected by service providers to provide technologies that are increasingly integrated into daily life, people reasonably expect that their data will be stored securely and remain private.

Although amici do not take a position on the outcome of this case, they believe Fourth Amendment protections for digital data should be strong. Rigid rules such as the third-party doctrine and the content/non-content distinction make little sense in the context of digital technologies and should yield to a more nuanced understanding of reasonable expectations of privacy, including consideration of the sensitivity of the data

[1] No counsel for a party authored this brief in whole or in part, and no entity or person other than amici and their counsel made a monetary contribution intended to fund the preparation or submission of this brief. Letters consenting to the filing of amicus briefs are on file with the Clerk.

and the circumstances under which such data is collected by or disclosed to third parties as part of people's participation in today's digital world.

Airbnb is a trusted community marketplace for people to list, discover, and book unique accommodations in more than 65,000 cities and 191 countries. Since its founding in 2008, there have been over 200 million guest arrivals in the over 4 million listings on Airbnb worldwide. While negative incidents are rare, Airbnb works with law enforcement to protect the rights of its Hosts, its Guests, and the community at large. At the same time, Airbnb respects the privacy interests of its community members. Airbnb sets forth in its law-enforcement guidelines how and when it complies with its legal obligations to provide user data to law enforcement. Airbnb publishes a Transparency Report to inform the public of the nature and volume of law-enforcement requests it receives and processes annually.

Apple Inc. offers highly secure hardware, software, and servers to customers worldwide. Apple's business strategy leverages its unique ability to design and develop its own operating systems, hardware, application software, and services to provide customers products and solutions with superior security, ease of use, seamless integration, and innovative design. In addition to the iPhone, iPad, Mac computer, and iPod, Apple offers its users iCloud—a cloud service for storing photos, contacts, calendars, documents, device backups, and more, keeping everything up to date and available to customers on whatever device they are using. Apple is committed its users' privacy and to helping users understand how it handles their personal information. Apple strives to provide straightforward

disclosures when it is compelled to comply with requests for user data from law enforcement.

Box is a cloud-based content-management platform that makes it easier for businesses to securely collaborate, share, and manage their content. Today, more than 74,000 businesses, including 64 percent of the Fortune 500, rely on Box to power how they work. Box respects the privacy rights of its users, collecting only the information necessary to authenticate the authorized user and provide access to the Box Service. Box invests significant resources in maintaining data-protection certifications to support its customers and effectuates personal data transfers from the European Union pursuant to Box's global privacy rules.

Cisco Systems, Inc. is the worldwide leader in providing infrastructure for the Internet. It also offers services including remote data centers, wireless-internet services, internet-security services, and collaboration tools, all managed from data centers operated by Cisco. Cisco is committed to protecting users' personal information. Its privacy statements reflect global principles and standards on handling personal information, including notice and user choice of data use and data security. Cisco regularly publishes information about requests for customer data that it receives from agencies around the world. Cisco believes law-enforcement and national-security agencies should go directly to its customers to obtain information or data regarding those entities, their employees, and users.

Dropbox, Inc. provides file-storage, synchronization, and collaboration services to customers and businesses worldwide. Its services empower people to work the way they want, on any device, wherever they go. Users entrust Dropbox with their most important

files, including documents and photos. When users put their files in Dropbox, they can rest assured that their data is secure and their own. Dropbox has a specialized privacy team dedicated to ensuring that privacy protections are built into Dropbox's products and services from the ground up. Dropbox's Government Request Principles reflect its commitment to protecting user privacy when responding to government requests for user data. Dropbox also publishes regular transparency reports about law-enforcement requests.

Evernote Corporation builds technology that enables individuals and teams to capture, organize, find, and share ideas in any form, on any Internet-connected device, forever. The Evernote app is available across platforms on desktop, mobile, or on the web. Users can input, upload, or store text, images, and other data. Evernote has more than 200 million consumer and business users in the United States and around the world. Evernote collects subscriber information, log data, location information, and device information and is committed to the privacy and security of its users' data. Evernote's Privacy Center and Privacy Policy inform users about the data Evernote collects and uses; Evernote's Security Overview describes how Evernote protect users' data. Evernote's Transparency Report reflects the volume of third-party demands Evernote receives for disclosure of user data. Evernote describes its user-notice policy and other practices for responding to such demands on its Information for Authorities website.

Facebook, Inc. provides a free Internet-based social-media service that gives more than two billion people the power to build communities and bring the world closer together. People use Facebook to stay connected with friends and family, to build communities, to

discover what is going on in the world, and to express what matters to them. People provide their names, phone numbers, and/or e-mail addresses when signing up for Facebook. As set forth in its Data Policy, Facebook also collects other information to provide its service, such as IP addresses and device-location data. Facebook is committed to protecting the privacy of the people who use its services. Facebook has robust privacy settings that allow people to control the audience of the information they choose to share. Facebook has also developed a privacy check-up tool to ensure that people's privacy settings reflect their desired level of privacy. Facebook closely reviews all requests for data from law enforcement and notifies people of requests for their information before disclosure unless prohibited by law from doing so or in exceptional circumstances. Facebook regularly produces a Government Requests Report reflecting its responses to government requests for data.

Google Inc. is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of web-based products and services, including Search, Gmail, Maps, YouTube, and Blogger, that are used daily around the world. For example, more than 400 hours of YouTube videos are uploaded to Google every minute, and there are more than a billion monthly active users of Gmail. To use these and other services, users give Google information, including queries for Search, photographs for Photos, documents in Drive, emails in Gmail, videos for YouTube, and location information. Google recognizes and respects the privacy of this information and is transparent with its users about the types of data it stores when users engage with its services. Google's Privacy Policy informs

users about their data, how to keep it safe, and how to take control. And Google regularly publishes transparency reports that reflect the volume of requests for disclosure of user data that Google receives from government entities.

Microsoft Corporation is a worldwide leader in software, services, devices, and solutions, including intelligent cloud-based computing. Since its founding in 1975, Microsoft has developed a wide range of software, services, and hardware products, including the flagship Windows operating system, the Office suite of productivity applications, the Surface tablet computer, and the Xbox gaming system. Microsoft serves more than 90 markets worldwide, delivering more than 200 online services and supporting more than one billion customers from more than 100 datacenters across the globe. Microsoft is committed to its customers' privacy. Microsoft empowers its customers to control and maintain privacy of their personal data. For example, LinkedIn, a professional networking site owned by Microsoft, discloses to members which personal information it collects and gives members choices about the collection, use, and sharing of data—from controlling what data is publicly available to managing who can see when members are active on LinkedIn. Microsoft will not disclose a customer's personal data unless required by law or when necessary to protect the safety and security of its customers and services. Microsoft issues biannual transparency reports regarding requests from law enforcement for user data.

Mozilla is a global, mission-driven organization that works with a worldwide community to create open-source products such as the Firefox browser. Several hundred million users use Firefox to discover, experience, and connect to the Internet. Mozilla also operates

web services such as Firefox Accounts and Firefox Sync, which allow users to synchronize information like bookmarks and browsing history across devices, and Mozilla Location Services, which allows a device to determine their physical location. Mozilla's guiding principles recognize that individuals' security and privacy on the Internet are fundamental and not optional. Mozilla has therefore adopted data-privacy principles that emphasize transparency, user control, limited data collection, and multi-layered security control and practices. For example, Mozilla uses pseudonymous random identifiers, end-to-end encryption, and other tools because users expect their browsing information to remain private.

Nest Labs builds hardware, software, and services for the connected home. The Nest Learning Thermostat, Nest Protect smoke and carbon-monoxide alarm, and Nest Cam security camera can all be controlled remotely by customers, and Nest algorithms use data about customer's devices and activity to automate and optimize device behavior to make users' experience of the product richer and more personal. For example, the Nest Learning Thermostat collects data about users' heating and cooling patterns, as well as household occupancy and patterns. Similarly, Nest Cam can record video and audio of a home and can recognize and record when it sees a familiar person. The data may be collected either actively when the user submits it to Nest, or passively in the everyday use of the product. Nest is transparent about the types of data it stores and commits to sharing personal data only with the user's permission. Nest notifies users about legal demands when appropriate, unless prohibited by law or court order, and if a request is overly broad, Nest will

seek to narrow it. Where possible, Nest will direct government entities to the user rather than to Nest.

Oath, a subsidiary of Verizon, is a values-led company committed to building brands people love. As a global leader in digital and mobile technology, Oath reaches over one billion people around the world with a dynamic house of more than fifty media and technology brands, including Aol, HuffPost, TechCrunch, Tumblr, and Yahoo. Oath may collect IP addresses and device-location data, among other information, from its mobile users. Oath carefully reviews law-enforcement demands for user data as part of its commitment to maintaining strong and meaningful privacy protections.

Snap Inc. operates the mobile application Snapchat. With more than 150 million daily active users, Snapchat is one of the world's leading camera applications. Snapchat empowers its users to create videos and photos that help them tell their stories and talk with their friends. As with any mobile application, users' interactions with these features generate data that may be of interest to law enforcement. Snap is committed to its users' privacy, and releases transparency reports twice a year to show how the company has responded to law-enforcement requests for user data.

Twitter, Inc. operates a global platform for self-expression and communication, with the mission of giving everyone the power to create and share ideas and information instantly, without barriers. Twitter's more than 300 million active monthly users use the platform to connect with others, express ideas, and discover new information. Hundreds of millions of short messages (known as "Tweets") are posted on Twitter every day. One of Twitter's core values is defending and respecting the user's voice through a two-part commitment to

freedom of expression and privacy, including allowing users to speak pseudonymously. Steps Twitter takes to defend and respect its users include notifying users about requests for their information, giving people access to their account data, challenging legal demands to disclose user information or remove content, and having clear guidelines for appropriate uses of Twitter's interface and products. Twitter also releases regular transparency reports detailing government requests for user data.

Verizon is a global leader delivering innovative communications and technology solutions. In the United States, Verizon's award-winning wireless network affords our more than 100 million connected devices a fast, reliable network to make phone calls and consume ever-increasing amounts of data and video. When a customer uses her phone for a call or data session, the specific cell sites with which the customer's device communicates are recorded in Verizon's network records. Last year, law enforcement obtained approximately 40,000 warrants or court orders to require Verizon to provide such cell-site location information to aid them in identifying the location of a device and, presumably, its user. Verizon believes that such demands present important questions about the proper balance between security and privacy. Verizon is committed to maintaining strong and meaningful privacy protections for its customers. Verizon thus carefully reviews law-enforcement requests for user data and publishes biannual transparency reports to disclose how it has responded to those requests.

SUMMARY OF ARGUMENT

The Internet and Internet-connected devices have revolutionized nearly every facet of our lives.

Americans rely daily on services made possible by networked technologies—from email, smartphones, and web-based social media the Court has already encountered to new and evolving products and applications in the "Internet of Things," such as smart-home devices that can be used to control room temperature and lighting, order groceries, and perform a multitude of other tasks. These devices and services not only confer immense value on users and society, but in many instances are considered practical necessities of modern life.

Using these technologies often involves transmitting highly personal information through the networks and applications of digital service providers. That includes transmission of metadata—*i.e.*, data about data—generated by automated processes that are part of the background operation of digital devices and applications. Such transmissions are inherent features of how the Internet and networked devices work. Short of forgoing all use of digital technologies, they are unavoidable. And this transmission of data will only grow as digital technologies continue to develop and become more integrated into our lives. Because the data that is transmitted can reveal a wealth of detail about people's personal lives, however, users of digital technologies reasonably expect to retain significant privacy in that data, notwithstanding that technology companies may use or share the data in various ways to provide and improve their services for their customers.

Fourth Amendment doctrine must adapt to this new reality. Although amici do not take a position on the outcome of this case, they believe the Court should refine the application of certain Fourth Amendment doctrines to ensure that the law realistically engages with Internet-based technologies and with people's expectations of privacy in their digital data. Doing so

would reflect this Court's consistent recognition that Fourth Amendment protections, governed as they are by reasonable expectations of privacy, must respond to changes in technology that implicate privacy. Indeed, in declining to extend the search-incident-to-arrest exception to searches of cell phones in *Riley* v. *California*, 134 S. Ct. 2473 (2014), this Court has already signaled that digital information deserves special consideration, largely because Internet-connected devices such as smartphones "are not just another technological convenience," but are necessary to participate in the modern world, and "hold for many Americans 'the privacies of life.'" *Id.* at 2494-2495.

In the digital context, inflexible doctrines that categorically foreclose any protection for data automatically generated by ordinary digital activity—or that will be generated by the yet-to-be-conceived technologies of tomorrow—are not sustainable. In particular, the analog-era notion that transmission of data to a third party is necessarily "voluntary" conduct that precludes Fourth Amendment protection should not apply in a world where devices and applications constantly transmit data to third parties by dint of their mere operation. No constitutional doctrine should presume that consumers assume the risk of warrantless government surveillance simply by using technologies that are beneficial and increasingly integrated into modern life. Similarly, the fact that certain digitally transmitted information might have been traditionally classified as "non-content" should not unconditionally bar Fourth Amendment protection, as this data can often be highly revealing of the intimate details of a user's life.

Rather than adhere to rigid Fourth Amendment "on/off" switches developed in the analog context,

courts should take a more flexible approach that realistically reflects the privacy people expect in today's digital environment. Consistent with the general reasonable-expectation-of-privacy inquiry, courts should focus on the sensitivity of the data at issue and the circumstances of its transmission to third parties. That approach would better reflect the realities of today's digital technologies and accommodate the technologies of the future.

ARGUMENT

I. FOURTH AMENDMENT DOCTRINE MUST ADAPT TO THE CHANGING REALITIES OF THE DIGITAL ERA

"It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo* v. *United States*, 533 U.S. 27, 33-34 (2001). "The forces and directions of the Internet are so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow." *Packingham* v. *North Carolina*, 137 S. Ct. 1730, 1736 (2017). This Court has therefore repudiated "mechanical interpretation of the Fourth Amendment"—woodenly applying doctrines developed in one context to materially different contexts—because doing so would leave reasonable expectations of privacy "at the mercy of advancing technology." *Kyllo*, 533 U.S. at 35. Fourth Amendment law, influenced as it is by societal expectations, must account for new technology that affects those expectations.

Digital interconnectedness defines modern society. When this Court decided the cases that form the basis of the third-party doctrine—*United States* v. *Miller*, 425 U.S. 435 (1976), and *Smith* v. *Maryland*, 442 U.S.

735 (1979)—the Internet did not exist, people made calls from shared public payphones, and third-party disclosure was rarely necessary for conducting daily activities. And when Congress enacted the Stored Communications Act (SCA) in 1986, few people used the Internet, almost none had portable computers, and only around 500,000 Americans subscribed to basic cell-phone service. *See, e.g.*, CTIA, *Semi-Annual Wireless Industry Survey* 2 (2011). Today, in contrast, the vast majority of Americans—over 95% of adults—own cell phones, and 77% own smartphones. Pew Res. Ctr., *Mobile Fact Sheet* (Jan. 12, 2017). "[A] growing share of Americans now use smartphones as their primary means of online access at home." *Id.* These phones regularly transmit more data in a span of minutes than could fit on an entire hard drive in 1986. People send and receive 269 billion emails each day worldwide. Radicati Group, *Email Statistic Report, 2017-2021* (2017). Unlike the era of payphones or the early days of the SCA, many people now use the Internet and Internet-connected devices and applications to facilitate all aspects of their lives—from personal communications to shopping to tracking their health and managing their homes.

Amid these changes, as discussed below, expectations of privacy in one's personal information vis-à-vis the government have not diminished. Transmitting personal data to the companies that provide digital products and services is an unavoidable condition of using technologies that people find beneficial and useful, and forgoing the use of those technologies for many is not an option. *See, e.g.*, OECD, *Bridging the Digital Divide* (collecting articles on "[t]he risks] … of being disconnected" due to "gaps in access to information and communication technology"). But that data can often

reveal details about the user's personal life and activities and therefore can require Fourth Amendment protection.

A. Digital Data And Devices Are Pervasive, Personal, And Often Necessary To Modern Life

Digital technologies have become a necessary aspect of life today. As many courts have recognized, the "[u]se of the Internet is vital for a wide range of routine activities in today's world—finding and applying for work, obtaining government services, engaging in commerce, communicating with friends and family, and gathering information on just about anything, to take but a few examples." *United States* v. *LaCoste*, 821 F.3d 1187, 1191 (9th Cir. 2016); *see also*, *e.g.*, *United States* v. *Sofsky*, 287 F.3d 122, 126 (2d Cir. 2002) ("'[C]omputers and Internet access have become virtually indispensable in the modern world.'"). Many people own cell phones simply to access the Internet and use online services. Anderson, *6 Facts About Americans and their Smartphones*, Apr. 1, 2015; *see also Riley*, 134 S. Ct. at 2489.

The Internet and Internet-connected devices have become fundamental tools for participating in many forms of modern-day activity. People now communicate by emails, text messages, and instant messaging. In the workplace, digital access has become a basic prerequisite of many jobs. *E.g.*, Dewey, *How Many Hours of Your Life Have You Wasted on Work Email?*, Wash. Post, Oct. 3, 2016 (average American white-collar worker spends 4.1 hours daily checking email); *United States* v. *Figueroa*, 2008 WL 5423982, at *2 (E.D. Wis. Dec. 30, 2008) ("Computers, internet access, and email have become indispensable parts of the functioning of this court."); Marya, *Cellphones are now essentials for*

the poor, USA Today, Sept. 14, 2013 (describing use of cell phones "to follow up on job and housing leads, and to keep in touch with public assistance agencies"). In the marketplace, digital technology offers enormous freedom for consumers in many areas of economic life. *See* Pew Res. Ctr., *Online Shopping and E-Commerce* (Dec. 16, 2016).

Digitally based activity is increasingly and quintessentially personal. Whereas in 1986 digital technologies were primarily used for business purposes, Bowman, *A Way Forward After* Warshak, 27 Berkeley Tech. L.J. 809, 809 (2012), today personal data, relationships, and intimate interactions predominate. Using digital platforms, people communicate with family and friends about their own and their children's whereabouts and activities. They share updates and exchange messages with old friends. They use cloud storage to archive notes and photos. And they network with peers, organize events, and engage in civic activity. Billions of people use social media and the Internet to "connect with one another" and "contribute to their local communities." Facebook, *Two Billion People Coming Together on Facebook*. "Seven in ten American adults use at least one Internet social networking service," *Packingham*, 137 S. Ct. at 1735, and more than 3.5 billion photos are shared daily over social media, Meeker, *2016 Internet Trends Report* 90, Kleiner Perkins Caufield & Byers (June 1, 2016).[2]

---

[2] Although using social media may sometimes involve broadcasting certain information to the public, most platforms also allow private posts or communications. Moreover, social media can implicate metadata—the result of automatic data processing that occurs "under the hood" of digital technology—that people can be unaware of or otherwise expect to remain private. *See, e.g.*,

Digital devices are also increasingly used for home-automation technology. Examples include voice assistants, such as Google Home and Apple's HomeKit and Siri, that can control room lighting and temperature, play music, or order groceries, among other functionalities, as well as cloud-based security systems and cameras, such as Nest Cam. *See* Crist, *Home Automation Buying Guide*, C|Net (Apr. 28, 2017 9:07 a.m.); Wasik, *In the Programmable World, All Our Objects Will Act As One*, May 14, 2013; *see also* Note, *If These Walls Could Talk*, 130 Harv. L. Rev. 1924, 1939-1945 (2017).

Such technologies exemplify the growing "Internet of Things" (IoT): an interconnected network of "smart" devices "used to communicate and process information to an extent that was not possible before." GAO, *Internet of Things* 1 (2017) (*GAO IoT Report*). IoT devices include wearable technology such as fitness trackers and smartwatches, medical equipment and transportation infrastructure, and items in the home including coffee makers, washing machines, headphones, and lamps. This network of "rapidly proliferating … sensors and control devices … leverage higher capacity and higher quality wireless technology and meshed networks to add unimaginable amounts of data and ubiquitous connectivity." *NSTAC Report to the President on Emerging Technologies: Strategic Vision Executive Summary* (May 18, 2017). A "smart" thermostat, for example, can allow homeowners "not only to remotely adjust the home's temperature, but also gather data on motion, temperature, and light, and analyze those data to

---

Warner, *Protect Your Online Privacy by Removing Exif Data from Your Photos*, Que Publ'g (May 15, 2014); *see also infra* pp. 17-19.

automate the thermostat to respond to changes in the home's environment and use." *GAO IoT Report* 1.

As all these examples suggest, to withdraw from the digital arena would be to deny oneself participation in "a revolution of historic proportions," giving up access to "full dimensions and vast potential to alter how we think, express ourselves, and define who we want to be." *Packingham*, 137 S. Ct. at 1736. Forgoing the use of networked devices would "render[] modern life … exceptionally difficult." *United States* v. *Holm*, 326 F.3d 872, 878 (7th Cir. 2003); *see also*, *e.g.*, *United States* v. *Dotson*, 715 F.3d 576, 586 (6th Cir. 2013). And it would "constrain[] … freedom in ways that make it difficult to participate fully in society and the economy." *LaCoste*, 821 F.3d at 1191.

B. Users Of Digital Technologies Cannot Avoid Transmitting Sensitive Data To Service Providers, But They Expect That Data To Remain Private

"The Internet is essentially made of a big web of routers talking to each other." Parlante, *The Internet-TCP/IP*, *CS101—Introduction to Computing Principles*. It operates through varied and complicated forms of communication and information exchange between different parties and devices. *Id.*; *see also* Bellovin, *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1, 5, 32-92 (2016). Using the Internet to make a call, send a message, or retrieve information means "talk[ing]" to other computers by sending packets of data and interacting with various layers of system protocols and architecture. Shuler, *How Does The Internet Work?* "[E]ven within a single device, different layers

may be operated by different parties." Bellovin, 30 Harv. J.L. & Tech. at 33.

By virtue of that architecture and the way the Internet and wireless networks operate, all digital technology transmits user information to various service providers. Those transmissions are an unavoidable condition of using digital technology. But in this digital era, users may not expect or intend that, by relying on service providers to administer everything from their email content and address book to their health and fitness data, they assume the risk that the government could amass and monitor their data without a warrant. *See, e.g.*, Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era* 34 (Nov. 14, 2014) (most study respondents thought of their location information as private).

The data transmitted may be highly sensitive. As this Court has observed with respect to established technologies, "[a]n Internet search and browsing history … [can] reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD." *Riley*, 134 S. Ct. at 2490. Similarly, "[h]istoric location information"—something not unique to cell phones—"can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* (citing *United States* v. *Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.")). The same is true of other new and evolving technologies. To improve energy efficiency, a smart thermostat detects and transmits not just a home's temperature, but information

about the homeowner's habits—whether and when the occupants are home, and where they are in the home. And to improve home security, smart security cameras can develop the ability to recognize individuals and record and transmit information about their comings and goings.

Whether email, cloud computing, location-based tracking, or any other digital functionality is at issue, users consider many types of collected electronic data to be private—particularly given the personal details that information can reveal—regardless of whether transmission to a third party has occurred behind the scenes in the creation or processing of that data. *See* Mastroianni, *Survey: More Americans Worried About Data Privacy than Income*, CBS News, Jan. 28, 2016. User and market research, including extensive review of user feedback and complaints, confirms this expectation.[3]

Even on social-media platforms such as Facebook and Twitter, privacy settings allow users to control whether their posts will be disclosed publicly, only to specified friends and family, or not at all. And even

---

[3] According to a poll by the Pew Research Center, "93% of adults say that being in control of who can get information about them is important: 74% feel this is 'very important'; 19% say it is 'somewhat important.' 90% say that controlling what information is collected about them is important—65% think it is 'very important' and 25% say it is 'somewhat important.'" Madden, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Res. Ctr., May 20, 2015. Additionally, "Americans say they do not wish to be observed without their approval; 88% say it is important that they not have someone watch or listen to them without their permission (67% feel this is 'very important' and 20% say it is 'somewhat important')." *Id.*

when posting publicly, users may not expect metadata encoded within those posts to be available to the government without a warrant. *Supra* p. 15-16 n.2. Indeed, for some platforms, privacy controls are at the heart of the service provided. For example, the Snapchat app, from its very beginning, was designed to give individuals a way of expressing themselves and communicating with others without creating a permanent record of the expression. In this way, the app protects individuals' privacy by deleting many communications and content by default once they have been viewed by the recipient. Snap further protects its users' privacy by encrypting the most sensitive data while it is stored, including location data, "Snaps," and "Stories."

Because amici recognize the sensitivity of the data their users entrust to them, they work diligently to protect customer information and take substantial measures to honor and reinforce their customers' expectation of privacy. These measures include offering user-controlled privacy settings, providing robust data encryption, and employing teams of data-security specialists to protect their systems from unauthorized access.[4] Many amici subject themselves to external audits of their infrastructure, applications, and operations to ensure the highest levels of protection of user data.[5] The reason for these measures is simple: While amici's customers understand that data is collected by service providers as part of providing digital technologies,

---

[4] *See, e.g.*, Google, *Privacy*; Apple, *Privacy Policy*; *Dropbox Privacy Policy*.

[5] *See, e.g.*, Google, *Cloud Platform Security*; Microsoft Trust Center, *Security, Audits, and Certifications*.

customers still expect privacy with respect to other parties, including the government.

C. Amici's Compliance With Law-Enforcement Requests Respects User Privacy

When law-enforcement agencies seek user data pursuant to a warrant—which, for example, has been routine with regard to email for some time—amici work to ensure that investigative needs are met without subjecting users to undue intrusion.[6] Where appropriate, amici voluntarily challenge overbroad or unsupported requests; but they also regularly turn digital information over to law enforcement in response to valid warrants. For example, Apple "carefully reviews all requests from government, law enforcement, and private parties to ensure that there's a valid legal basis for

---

[6] The SCA, 18 U.S.C. § 2703(a), generally requires law enforcement to obtain a warrant based on probable cause to access the "contents" (but not "records," *see id.* § 2703(c); *infra* p. 30 n.8) of electronic communications. Although Section 2703(b) of the Act allows law enforcement to use lesser legal process for certain types of communications under certain conditions, that subsection has been held unconstitutional, *see United States* v. *Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), and the Department of Justice has followed that holding as a matter of policy since 2013 by using only warrants to obtain stored content, H.R. Rep. No. 114-528, at 9 (2016). As this Court has noted, digital technologies make it easier for law-enforcement officers to secure warrants. *See Missouri* v. *McNeely*, 133 S. Ct. 1552, 1562 (2013); *see also Riley*, 134 S. Ct. at 2493. Federal Rule of Criminal Procedure 4.1 and "a majority of States" allow law-enforcement officials "to apply for search warrants remotely through various means, including telephonic or radio communication, electronic communication such as e-mail, and video conferencing." *McNeely*, 133 S. Ct. at 1562. Telephonic or email warrants can be obtained within the time of the average traffic stop. *See, e.g.*, *State* v. *Zeller*, 172 Wash. App. 1008 (2012).

each request." Apple, *Legal Process Guidelines: Government & Law Enforcement Within the United States*. Should it "determine[] that there is no valid legal basis or … [that the] request is … unclear, inappropriate or over-broad[,] Apple will challenge or reject the request." *Id.*

All amici practice and support this approach. *See, e.g.*, Dropbox, *Transparency Overview* ("Government data requests should be limited in the information they seek and narrowly tailored to specific people and legitimate investigations. We'll resist blanket and overly broad requests."); Apple, Lithium Techs., Mozilla, and Twilio Amicus Br. 11-12, Dkt. 66-1, *Microsoft* v. *United States*, No. 16-cv-00538 (W.D. Wash. Sept. 2, 2016) (discussing service providers' standing and practices to "challenge various forms of legal process served upon [companies] seeking customer data").

Amici also strive to be fully transparent about their interactions with law enforcement. *Supra* pp. 2-9. For instance, most amici notify users about requests for their data unless legally prohibited from doing so, and most amici publish transparency reports that detail the number and types of requests amici have received from government agencies and how they have responded to those requests.[7] These steps require an investment of time, energy, and resources. Yet amici take them because their users care about the privacy of their data and have made clear their "societal understanding that certain areas"—including in the digital realm—"deserve the most scrupulous protection from govern-

[7] *See, e.g.*, Apple, *Report on Government and Private Party Requests for Customer Information*; Snap, *Transparency Report*; Twitter, *Transparency Report: United States*.

ment invasion." *Oliver* v. *United States*, 466 U.S. 170, 178 (1984).

II. RIGID ANALOG-ERA RULES SHOULD YIELD TO CONSIDERATION OF REASONABLE EXPECTATIONS OF PRIVACY IN THE DIGITAL AGE

A. A Flexible Test Grounded In Today's Reasonable Expectations Of Privacy Should Govern In The Digital Context

As the foregoing discussion illustrates, when customers transmit personal data to technology companies in the course of using digital products and services, they reasonably expect that data and the metadata generated alongside it to be securely stored and remain private as to the rest of the world. They should not be forced to relinquish Fourth Amendment protections against government intrusion simply by choosing to use those technologies. To resolve this case, the Court should forgo reliance on outmoded rules that make little sense when applied in the digital context. In particular, the third-party doctrine and the content/non-content distinction should not operate to categorically foreclose Fourth Amendment protection; instead, Fourth Amendment law should favor a more flexible approach that assesses reasonable expectations of privacy in light of new and evolving technologies and the highly sensitive data they implicate.

"[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish," *Warshak*, 631 F.3d at 285—a point this Court has recognized and applied on more than one occasion. For example, where previously the Fourth Amendment's protections applied only to common-law trespass and physical seizure, this

Court held half a century ago that the widespread adoption of telephones "so eroded" that approach that it "c[ould] no longer be regarded as controlling." *Katz* v. *United States*, 389 U.S. 347, 351-353 (1967); *see also id.* at 361-362 (Harlan, J., concurring); *Jones*, 565 U.S. at 404-411. As the Court recognized, "[t]o read the Constitution more narrowly"—and allow law enforcement to eavesdrop unfettered on a caller "surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world"—would impermissibly "ignore the vital role that the public telephone has come to play in private communication." *Katz*, 389 U.S. at 352.

The Court should take similar account of the effects of the Internet and other digital technologies. Just as the widespread adoption of the telephone in the twentieth century required the Court to cabin obsolete Fourth Amendment doctrine in *Katz*, in the twenty-first century, Fourth Amendment doctrine must accommodate a historic shift in the use of digital technology. This Court has already taken a large step in that direction. In *Riley*, 134 S. Ct. 2473, the Court recognized the all-encompassing and private nature of digital data in holding that "officers must generally secure a warrant" before conducting a search for data on a cell phone. *Id.* at 2485. The Court reasoned that while the general rule allowing warrantless searches incident to arrest "strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones." *Id.* at 2484. Consequently, the Court declined to extend that rule to "searches of data on cell phones," instead requiring a warrant. *Id.* at 2485.

Fundamental to the Court's decision in *Riley* were two factors that apply as well to other digital technolo-

gies. First, the Court observed that "[m]odern cell phones are not just another technological convenience," but rather have become "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley*, 134 S. Ct. at 2484, 2494. Second, the Court recognized that cell phones "hold for many Americans 'the privacies of life.'" *Id.* at 2494-2495; *see also id.* at 2488-2491.

As discussed above, those considerations apply with equal or greater force to other digital technologies. As to the first, Internet-based services and devices are ubiquitous and "virtually indispensable in the modern world of communications and information gathering." *United States* v. *Peterson*, 248 F.3d 79, 83 (2d Cir. 2001) (per curiam); *see United States* v. *Voelker*, 489 F.3d 139, 145 (3d Cir. 2007); *supra* Part I.A. And as to the second, digital devices and services produce and record data that, alone or in the aggregate, has the potential to reveal highly sensitive information about all aspects of our private lives. *Supra* Part I.B. Accordingly, rather than automatically disqualifying digital data from Fourth Amendment protection based on rigid analog-era rules, courts should focus on the fundamental Fourth Amendment question: whether an individual has a reasonable expectation of privacy in a given set of digital data. In answering that question, courts should consider among other things the degree to which the data has the potential to reveal intimate details about the user, *see, e.g.*, *Riley*, 134 S. Ct. at 2490; *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 34-36 & n.4, 40; *United States* v. *Karo*, 468 U.S. 705, 715 (1984), and the extent to which the service or device is used by the average person, *cf. Riley*, 134 S. Ct. at 2484.

This approach has the virtues of assessing digital data on its own terms and realistically engaging with the reasonable expectations of privacy of modern Americans. And it affords courts an adaptable method of analysis that will remain workable even as digital technology evolves. *Packingham*, 137 S. Ct. at 1736.

B. Transmission To A Service Provider Should Not Automatically Foreclose Protection Of Digital Data

The third-party doctrine is the notion that Fourth Amendment protection does not extend to information voluntarily disclosed to a third party. In *Smith*, 442 U.S. 735, for example, the Court rejected Fourth Amendment protection for telephone numbers recorded by pen register, which had "limited capabilities"—indeed, "'[n]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed [could be] disclosed.'" *Id.* at 741. The decision rested on the caller's conveyance of the numbers to his telephone company through early switchboard equipment, which the Court analogized to giving information to a live operator. *Id.* at 745. Similarly, in *Miller*, 425 U.S. at 442, the Court declined to extend Fourth Amendment protection to "negotiable instruments to be used in commercial transactions" when those instruments had been given to a bank. The Court explained that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party," "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443. Courts have extrapolated from these decisions a "binary" inquiry "in which any information dis-

closed to a third party for any reason is public and does not merit Fourth Amendment protection." Note, *If These Walls Could Talk*, 130 Harv. L. Rev. at 1931.

This rigid interpretation is unworkable when applied to the Internet and digital technologies, which operate through varied and complicated forms of information exchange between different parties and devices. *See Jones*, 565 U.S. at 417-418 (Sotomayor, J., concurring); Note, *If These Walls Could Talk*, 130 Harv. L. Rev. at 1933-1937. Unlike the "limited capabilities" of pen-register data, *Smith*, 442 U.S. at 742, the data transmitted by users of digital devices and applications can often reveal intimate details of people's lives, especially when viewed in the aggregate. Cell-tower records that reveal a person's general location are but the tip of the iceberg. People search online for all manner of information, including medical advice, and rely on the Internet for their jobs, schooling, and interpersonal communications. They reveal their habits, views, and preferences by interacting with apps used to navigate almost every facet of their lives. They store photos and emails in the cloud, rely on data-collecting devices such as fitness trackers to manage their health, and use smart appliances to provide home security and efficiency. For many of these activities, there is no analog-era analogy; in the past, for instance, a user did not have to tell a company when and how he wanted to adjust his thermostat, thereby risking losing all privacy protection in that information.

The incongruity between the third-party doctrine and reasonable expectations of privacy is only amplified in the context of home-automation devices and other smart-home technology, which bring connectedness into private spaces. *See supra* pp. 7, 10, 13, 16-17, 18-19. "'At the very core' of the Fourth Amendment

'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" *Kyllo*, 533 U.S. at 31; *see also*, *e.g.*, *Karo*, 468 U.S. at 714 ("[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."); Pesciotta, *I'm Not Dead Yet:* Katz, Jones, *and the Fourth Amendment in the 21st Century*, 63 Case W. Res. L. Rev. 187, 217-219 (2012) ("the Court has always been steadfast in its protection of privacy in the home—an area in which all citizens undoubtedly expect the utmost level of privacy").

Moreover, the premise of the third-party doctrine—that what one voluntarily and knowingly exposes to another is no longer private—bears little relevance to many modern technologies. As discussed, many devices and applications transmit data automatically with no prompting by the user. *See supra* pp. 10, 15-16 n.2, 17-19. In addition, digital data, whether passively or actively conveyed, often is not really "exposed" to others or directly observed by another human being, but is instead automatically transmitted and processed by different computer software and servers. And as discussed, these transmissions are a necessary condition of participating in the digital world.

Finally, treating such disclosures as a voluntary relinquishment of privacy for all purposes is misconceived because it allows no possibility for degrees of privacy. In the digital era, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all." *Smith*, 442 U.S. at 749 (Marshall, J., dissenting). Engaging in activities that expose personal information to one audience does not diminish the reasonable expectation that one's personal information should otherwise remain private.

That users rely on technology companies to process their data for limited purposes does not mean that they expect their intimate data to be monitored by the government without a warrant. As one court aptly observed, "[h]otel guests, for example, have a reasonable expectation of privacy in their rooms … even though maids routinely enter hotel rooms to replace the towels and tidy the furniture," and "tenants have a legitimate expectation of privacy in their apartments … regardless of the incursions of handymen to fix leaky faucets." *Warshak*, 631 F.3d at 287; *see also* Colb, *What Is A Search?*, 55 Stan. L. Rev. 119, 122-123 (2002). In using digital technologies, too, people can and do reasonably expect certain information to be kept private with regard to one audience or purpose but not with regard to another—particularly when that data is highly revealing of intimate details and cannot be kept entirely from others without forgoing the use of digital technologies.

C. "Non-Content" Digital Data Should Not Automatically Be Excluded From Protection

The content/non-content distinction is the idea that, although the content of communications themselves, such as the text of a letter, is considered private and subject to Fourth Amendment protections, the "non-content" information necessary to process the communication or route it from one point to another—*e.g.*, the address on the outside of the envelope—is not. Thus, in *Ex parte Jackson*, 96 U.S. 727 (1878), the Court held that postal inspectors needed a search warrant to open letters and packages, but that the "outward form and weight" of those mailings were not constitutionally protected. *Id.* at 773. This distinction rests on the notion that non-content routing information is limited in what

it reveals about a person and is visible in plain view. *See id.*

Amici agree that content, digital or otherwise, should receive strong protection under the Fourth Amendment. *See Warshak*, 631 F.3d at 285-286. An email is no less personal and revealing, and no more out in the open, than the contents of a physical letter or telephone call. "Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection." *Id.* But the notion that "non-content" information should automatically be relegated to a less-protected status ignores the realities of digital data.[8]

The cell-site location data at issue here can reconstruct the user's movements, revealing significant information about the user's associations and activities. *Riley*, 134 S. Ct. at 2490; *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). Indeed, the detail revealed by such data is even greater today than it was just six years ago when law enforcement sought access to information from Mr. Carpenter's device. Since then, as the number of smartphones and the volume of data usage have dramatically increased, Verizon has expanded its network and added smaller cell sites, which have narrower ranges than larger, traditional cell towers

[8] The SCA—enacted more than thirty years ago—distinguishes between contents of communications and records concerning communications by requiring the full protections of a warrant only for the former. *See* 18 U.S.C. § 2703. But that statute was not written with today's digital landscape in mind, and it is not dispositive of the constitutional question whether there is a reasonable expectation of privacy in digital data.

and "fill in coverage gaps between larger towers." Silliman, *Musing About the Third Party Doctrine During Network Planning Meetings* (Oct. 10, 2016). As a result, Verizon's network now collects even more voluminous and much more precise location information capable of providing a wealth of detail. *Cf. United States* v. *Pineda-Moreno*, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, J., dissenting) ("Are Winston and Julia's cell phones together near a hotel a bit too often? Was Syme's OnStar near an STD clinic? Were Jones, Aaronson and Rutherford at that protest outside the White House?").

That said, the sensitivity of digital data is hardly limited to location information. Some types of data that digital devices generate may reveal with considerable precision granular details about the materials people read, the precise actions they take on their devices, and much more. *Riley*, 134 S. Ct. at 2490. Moreover, digitally encoded information is hardly in plain view. It requires special equipment and software to piece together.

For example, when an Internet user opens a news story, views a photograph, or sends a message to a friend, the user's smartphone often makes a record of that action, and those records are often transmitted to third parties such as the operator of the Internet platform or mobile application. Arguably, these records are not "content" in the analog sense; they do not contain communications in sentence or paragraph form. But they have the potential to reveal highly private and personal information about the user.[9] A law-

[9] Given the content/non-content distinction's analog pedigree, courts have struggled to classify certain types of data. URLs are

enforcement agent who accesses such records about John Smith would know what news stories Smith read, what photographs he viewed, and when and from where he sent those messages. Government agencies could try to use log data from a search engine that would show a user's pattern of accessing websites about anorexia, mental health, or substance-abuse treatments. Data from a connected security systems or other smart-home devices could reveal when the user is out of town. Even the metadata recording the delivery information of a single email message could expose the membership of an entire political organization. *Cf. NAACP* v. *Alabama*, 357 U.S. 449 (1958).

Even if it could be considered "non-content," this data can be as revealing about the intimate details of one's life as the actual content of a message. It makes little sense to subject such sensitive data, which is both quantitatively and qualitatively "different" from any analog notion of routing information for telephones or snail mail, *Riley*, 134 S. Ct. at 2490, to a rule developed in the pre-digital context, where the risks of revealing deeply personal information were indisputably lower.

CONCLUSION

The Court should afford strong Fourth Amendment protection to digital data and reject mechanical application of the third-party doctrine and content/non-content distinction in favor of a more flexible analysis

---

a good example: "Though some district courts have held that a URL is never content," other courts have found that certain types of URLs could be content depending on the information they reveal. *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 138 (3d Cir. 2015).

that takes account of people's reasonable expectations of privacy in the digital era.

Respectfully submitted.

SETH P. WAXMAN
Counsel of Record
JONATHAN G. CEDARBAUM
CATHERINE M.A. CARROLL
ROBBIE MANHAS
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Ave., NW
Washington, DC 20006
(202) 663-6000
seth.waxman@wilmerhale.com

AUGUST 2017