No. _____

In The
Supreme Court of the United States

RAYMOND J. LIDDY,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit

PETITION FOR WRIT OF CERTIORARI

DEVIN BURSTEIN
Counsel of Record
WARREN & BURSTEIN
501 W. Broadway, Suite 240
San Diego, California 92101
Telephone: (619) 234-4433
Facsimile: (619) 234-4433
db@wabulaw.com

Attorney for Petitioner

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

QUESTIONS PRESENTED FOR REVIEW

Does Internet subscriber information constitute a digital "paper" or "effect" under the Fourth Amendment? If so, must law enforcement obtain a warrant before searching an individual's Internet subscriber information, which includes private, personal data beyond mere name, IP address, and physical address?

RELATED CASES

United States v. Raymond J. Liddy, No. 19-cr-01685-CAB, U.S. District Court for the Southern District of California. Judgment entered September 2, 2020.

United States v. Raymond J. Liddy, No. 20-50238, U.S. Court of Appeals for the Ninth Circuit. Judgment entered September 28, 2022.

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES – Continued

CONSTITUTIONAL PROVISIONS

STATUTES

In The
Supreme Court of the United States

RAYMOND J. LIDDY,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit

PETITION FOR WRIT OF CERTIORARI

Petitioner Raymond J. Liddy respectfully prays that a writ of certiorari issue to review the judgment of the United States Court of Appeals for the Ninth Circuit.

OPINION BELOW

Relying on prior circuit precedent, the court of appeals rejected petitioner's preserved Fourth Amendment claim and affirmed his conviction. The decision is available at *United States v. Liddy*, No. 19-50177, 2022 U.S. App. LEXIS 27188, 2022 WL 4533991 (9th Cir. 2022).[1]

[1] A copy of the decision is attached as Appendix A.

JURISDICTION

On September 28, 2022, the Ninth Circuit filed its decision. This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const., amend. IV.

STATEMENT OF THE CASE

I.

It is impossible to tell Mr. Liddy's story without first mentioning his infamous father, G. Gordon Liddy. 6-ER-1235.[2] The elder Mr. Liddy was at the center of

[2] The Excerpts of Record (ER) are on file with the Ninth Circuit Court of Appeals.

the Watergate scandal. 6-ER-1235. When the story broke, he became a villain to millions. 6-ER-1235.

The young Mr. Liddy and his family were scorned. 6-ER-1235-36. This fueled his desire to succeed and to serve. 6-ER-1236. In 1986, Mr. Liddy enlisted in the Marine Corps and soon deployed to combat in Panama as part of Operation Just Cause. 6-ER-1236. While there, he was nearly killed in an explosion, suffering burns over 14% of his body. 6-ER-1238. Beyond the physical wounds, the incident ultimately resulted in a severe case of post-traumatic stress disorder, which would manifest later.

Mr. Liddy spent months recovering, but his commitment did not waiver. 6-ER-1238. He continued in the Marine Corps Reserves while attending law school. 6-ER-1240. After being recalled to active combat for Operation Desert Storm, Mr. Liddy completed his degree. 6-ER-1240-41. He eventually worked as a Deputy Attorney General for California in the civil division (he never practiced criminal law). 6-ER-1211, 1243. At the same time, Mr. Liddy also maintained his military service, and was again activated for combat duty during Operation Iraqi Freedom. 6-ER-1241. He was ultimately promoted to full Colonel, his proudest achievement. 6-ER-1241.

As Mr. Liddy approached mandatory Marine Corps retirement, he felt a loss of purpose and grew depressed. 6-ER-1241. This exacerbated his combat-related PTSD. 6-ER-1241. He sought help and was prescribed Ambien for his chronic insomnia. 6-ER-1242.

It did not fix the problem, so he began drinking at night after taking Ambien. 6-ER-1242. Inebriated, depressed, and still unable to sleep, Mr. Liddy turned to the Internet for a sense of connection. 6-ER-1242.

He began frequenting *adult* chatrooms, where sexual topics were discussed, and users posted links to *adult* pornography. 4-ER-566; 5-ER-947-49. The users also frequently chatted on messaging platforms such as Yahoo messenger and Skype. 5-ER-954, 958.

The chatrooms functioned like a tickertape. 4-ER-566. Messages continuously scrolled by with text, thumbnail images,[3] or links. 4-ER-566. Mr. Liddy generally had numerous windows open, holding multiple conversations. 4-ER-566. It was too much to digest in real-time. 4-ER-566; 5-ER-961.

As a result, Mr. Liddy would often right-click a thumbnail or a link and save the file *without* first viewing it or knowing what it depicted. 4-ER-566. Sometimes the links would result in mass-downloads of image files. 4-ER-566. Often Mr. Liddy would simply delete the downloaded files without reviewing them, feeling ashamed of his drunken conversations. 4-ER-566. Other times, he would open the files to see the pictures before deleting them. 4-ER-566. Almost always, it was adult pornography. 4-ER-566.

---

[3] A thumbnail is a small, low-resolution file; the details of the image are generally not discernable. 5-ER-917; *see Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 818-19 (9th Cir. 2003); *United States v. Battershell*, 457 F.3d 1048, 1049 (9th Cir. 2006).

Occasionally, however, an image would reveal what appeared to be child pornography. 4-ER-566; 5-ER-969. He always deleted any such images. 4-ER-566; 5-ER-969. Moreover, as the forensic evidence would establish – and the district court found – Mr. Liddy never sought this contraband. 4-ER-566; 5-ER-965, 970; 6-ER-1340-41. One of the unique factors of this case is that there were *no* Internet searches for child pornography and *no* discussion of child pornography in the numerous chat messages recovered by the government. 6-ER-1340-41.

But algorithms do not differentiate between intentionality and inadvertence. Internet companies like Yahoo and Skype use special software to search their systems for contraband images. When the software encounters such a file, the company must report the incident to the CyberTipline of the National Center for Missing and Exploited Children (NCMEC). *See* 18 U.S.C. § 2258A(a). Typically, the electronic report contains basic information about the user account and the suspect files. NCMEC then forwards the reports to law enforcement. 2-ER-100.

II.

In early 2017, Yahoo and Microsoft (Skype) reported to NCMEC that their software encountered several images of child pornography on their systems.[4]

[4] The companies intercepted the files and then uploaded them to NCMEC from their servers. 6-ER-1205, 1220. Mr. Liddy did not upload the files from his computer.

2-ER-72-92. The IP address associated with both reports was 76.88.66.25, and the associated account was "cahubby." 2-ER-74.

Several months later, Department of Justice Administrative Subpoenas were served on Time Warner Cable seeking subscriber information for the customer utilizing the IP address 76.88.66.25. 2-ER-100, 179-83.

- With no judicial oversight, the subpoenas "commanded and required" Time Warner Cable to disclose a broad list of personal information:
- "Customer or subscriber name, address of service, and billing address;"
- "Length of service (including start date and end date);"
- "Local and long distance telephone connection records (examples include: incoming and outgoing calls, push-to-talk, and SMS/MMS connection records);"
- "Means and source of payment (including any credit card or bank account number);"
- "Records of session times and duration for Internet connectivity; Telephone or **Instrument number (including IMEI, IMSI, UFMI, and ESN)** and/or other customer/subscriber number(s) used to identify customer/subscriber, including any temporarily assigned network

address (including Internet Protocol addresses);"[5] and,

- "Types of service used (e.g. push-to-talk, text, three-way calling, email services, cloud computing, gaming services, etc.)."

2-ER-179. None of this information was public.

In response, Time Warner provided the name, home address, dates of service, several personal email addresses, and three personal phone numbers for Mr. Liddy and his wife. 2-ER-186, 189. The government then used this information to obtain search warrants for Mr. Liddy's home. 2-ER-136.

Several hours after executing the warrant, agents told Mr. Liddy that, using special forensic software, they found a few (deleted and otherwise inaccessible) files containing child pornography on his devices and arrested him. 3-ER-325-26. The agents then seized all the digital media from the Liddy home for further forensic examination.

There were no readily accessible contraband files found on any of the devices. 6-ER-1249. Instead, the government's subsequent examination with forensic

[5] Instrument numbers are unique identifiers of a particular device equivalent to a serial number. Specifically, IMEI is the International Mobile Equipment Identity, a unique number used to identify a particular mobile device. IMSI is the International Mobile Subscriber Identity, a unique number used to identify a mobile subscriber. UFMI is the Universal Fleet Member Identifier, a unique number assigned to a telecommunications subscriber. ESN is the Electronic Serial Number, a unique number assigned to a specific mobile phone.

software revealed several deleted and/or inaccessible files depicting child pornography. 6-ER-1249.

III.

Despite the lack of active contraband files or any evidence that Mr. Liddy had searched for such content on the Internet, the government charged him with knowingly possessing child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). 2-ER-67; 3-ER-439.

Mr. Liddy moved to suppress the fruits of the warrantless search of his subscriber information. 2-ER-68; 3-ER-320. The district court denied the motion. 1-ER-2-12. Following a bench trial, the district court found Mr. Liddy guilty of possessing a few deleted and inaccessible images and sentenced him to probation.

On appeal, Mr. Liddy argued that the warrantless search of his subscriber information violated the Fourth Amendment, and that the third-party doctrine did not apply. Thus, he asserted that the district court erred in denying his motion to suppress the evidence stemming from the subscriber search.

The court of appeals affirmed, finding Mr. Liddy's "argument is foreclosed by *United States v. Rosenow*, 33 F.4th 529 (9th Cir. 2022), in which we held that 'a defendant 'ha[s] no expectation of privacy in . . . IP addresses' or basic subscriber information because internet users 'should know that this information is provided to and used by Internet service providers for

the specific purpose of directing the routing of information.'" APP:A at 9.

This petition for a writ of certiorari follows.

REASON FOR GRANTING THE PETITION

I.

The government is currently allowed to trespass on our digital papers and effects without a warrant. In cases such as *Rosenow*, 33 F.4th at 547; *United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017); and *United States v. Caira*, 833 F.3d 803, 806 (7th Cir. 2016), the circuit courts have determined that an individual's Internet subscriber information deserves no Fourth Amendment protection. These courts reason that, under the third-party doctrine, there is no expectation of privacy in such data because the user shares the information with an Internet service provider. *See id*.

This conclusion is worthy of the Court's review because it suffers from two fatal flaws and has significant consequences for hundreds of millions of Americans. First, the circuits fail to consider traditional property-based Fourth Amendment protections. Second, they misunderstand this Court's recent precedent clarifying that, when it comes to digital data, courts can no longer uncritically apply judicially created exceptions to the warrant requirement.

As a result of these errors, under current circuit-level jurisprudence, law enforcement can obtain by

administrative subpoena – without judicial review or notice to the impacted individual – substantial private information regarding internet usage, including information that could otherwise only be learned by *physically entering the home*, such as a modem's unique identifying number. *See Arizona v. Hicks*, 480 U.S. 321, 325 (1987) (turning over a record player to reveal its serial number is a search requiring a warrant).

This is a big deal. Internet use in the United States is ubiquitous. But it is impossible to do so without a service provider like a cable company or mobile phone carrier. All such carriers maintain subscriber information about their customers, which the government can now obtain without a warrant. This means that the personal information of nearly the entire United States population – every household with an Internet connection and every person with a mobile phone – is implicated. Plainly, this is an issue of national significance.

Nor does it matter that Internet subscriber information does not reveal the content of any communications. As this Court has made clear, "it matters not that [a] search uncovered nothing of any great personal value. . . . A search is a search, even if it happens to disclose nothing but the bottom of a turntable." *Id.* at 325. The same is true as applied to Internet subscriber information.

The Court, therefore, should take this case to determine whether the government's use of

administrative subpoenas to obtain such information is consistent with the Fourth Amendment.

II.

The process by which the government currently obtains Internet subscriber information is analogous to the process this Court held unconstitutional in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). Thus, *Carpenter* is a good place to begin.

This Court considered whether the government could use a court order under the Stored Communications Act (SCA) – as opposed to a warrant – to obtain cell-site location information (CSLI). *See id.* at 2215. In concluding it could not, the Court needed to reconcile "a person's expectation of privacy in his physical location," *id.*, with the "third-party doctrine," under which, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 2216.

The solution was straightforward. The Court simply declined to extend the third-party doctrine to CSLI records: "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology . . . *or leverages the technology of a wireless carrier*, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Id.* at 2217.

Carpenter also rejected the government's "primary contention" that, under the third-party doctrine, "cell-site records are fair game because they are 'business records' created and maintained by the wireless carriers." *Id.* at 2219. This position, "fail[ed] to contend with the seismic shifts in digital technology[.]" *Id.*

Moreover, "[c]ell phone location information is not truly 'shared' as one normally understands the term. In the first place, cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.* at 2220. Given the Fourth Amendment implications, the Court "found that the acquisition of [ ] CSLI was a search," and "conclude[d] that the Government must generally obtain a warrant supported by probable cause before acquiring such records." *Id.* at 2221.

On this point, the Court further explained it had "*never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy*." *Id*. (emphasis added). "If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement." *Id.* at 2222. Instead, a warrant is required "where the suspect has a legitimate privacy interest in records held by a third party." *Id.*

This reasoning should also apply to administrative subpoenas for Internet subscriber information.

III.

The Fourth Amendment protects the People against unreasonable searches or seizures in our persons, houses, papers, and effects. These protections are triggered in two circumstances. *See id*. at 2213.

First, a "search" occurs when a government agent infringes on an "expectation of privacy [] that society is prepared to consider reasonable[.]" *Id*. Second, there is a "search" within the meaning of the Fourth Amendment when the government intrudes upon "'a constitutionally protected area'" – persons, houses, papers, or effects – to "'obtain[] information.'" *Id.* (quoting *United States v. Jones*, 565 U.S. 400, 407 (2012)).[6] Here, the Court should evaluate whether the government's use of administrative subpoenas infringes on either or both protected interests.

To be clear, this is not simply a matter of obtaining basic information like a user's IP and physical address. Rather, the subpoenas at issue include, *as to every inhabitant of the home*, the instrument numbers of communication devices, payment records, personal telephone numbers, local and long-distance telephone connection records, times and duration of internet

[6] This original Fourth Amendment understanding is often referred to as the property or trespassory theory. *See Jones*, 565 U.S. at 409 (the "reasonable-expectation-of-privacy test has been added to, not *substituted for*, the common-law trespassory test.") (emphasis in original).

access sessions, the types of internet services used and email addresses.[7]

Under this Court's controlling precedent and common sense, this should be private information protected by the Fourth Amendment. Indeed, as noted, it "could not otherwise have been obtained without physical intrusion into a constitutionally protected area" – e.g., entering Mr. Liddy's home to physically examine his devices and monitor his usage. *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (internal quotations and citation omitted). And in the home, "[t]he Fourth Amendment's protection . . . has never been tied to measurement of the quality or quantity of information obtained. . . . In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes." *Id.* at 37 (emphasis in original).

As such, the expectation of privacy is manifest. *See id.* at 34-37. And the courts of appeals' decisions to the contrary should hold no weight.

Independently, the type of administrative subpoena at issue also directly impacts the individuals' *property* rights in the requested data. As Justice Gorsuch has explained, "the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them."

---

[7] That fact distinguishes this case from those where the government uses a subpoena solely to obtain the residential address and/or the subscriber's name associated with a particular IP address.

Carpenter, 138 S. Ct. at 2268 (Gorsuch, J., dissenting). "Just because you entrust your data – in some cases, your modern-day papers and effects – to a third party may not mean you lose any Fourth Amendment interest in its contents." *Id.* at 2269.

Applying this principle here, the subpoenas effectuate a digital trespass. They allow the government to gain access to the subscriber's property (data) without a warrant. *Jones*, 565 U.S. at 419 n.2 ("At common law, a suit for trespass to chattels could be maintained if there was a violation of the *dignitary interest* in the inviolability of chattels") (Alito, J., concurring, internal quotations and citation omitted).[8] Indeed, the intrusion here was in many ways more egregious than in *Carpenter*. There, the location information obtained by the government involved activities conducted by the defendant in public, where he could be observed by numerous third parties. The information sought in this case would divulge facts and events occurring *within the home*.

Then, too, the subpoena in *Carpenter* was subject to judicial supervision, having been issued "[u]pon approval by a neutral magistrate, and based on the Government's duty to show reasonable necessity," 138 S. Ct. at 2224 (Kennedy, J., dissenting), whereas the administrative subpoena in this case was subject to *no* judicial supervision and no requirement that the

[8] While Mr. Liddy acknowledges that the government had statutory authority to issue the subpoenas at issue, *see* 18 U.S.C. § 2703(c)(2), as in *Carpenter*, the statute must yield to the Fourth Amendment. *See* 138 S. Ct. at 2221.

government show "reasonable necessity" or even that "that the records sought are relevant and material to an ongoing criminal investigation." *Id.* at 2212 (majority opinion). Prosecutors simply wrote their own ticket without having to justify the necessity or breadth of the search to anyone.

Nor does it matter that the government may have had probable cause to obtain some of the information it requested in the subpoena. Probable cause alone is not sufficient to obtain evidence protected by the Fourth Amendment. "It is a basic principle of Fourth Amendment law that searches and seizures inside a home without a warrant are presumptively unreasonable." *Payton v. New York*, 445 U.S. 573, 586 (1980) (internal quotation and citation omitted). Absent an exception, such as exigency or plain view, none of which apply here, the "answer to the question of what police must do before [obtaining subscriber data] is accordingly simple – get a warrant." *Riley v. California*, 573 U.S. 373, 403 (2014).

Doing so, moreover, is far from onerous. In fact, in at least some jurisdictions, law enforcement does seek a warrant before searching subscriber information. *See United States v. Bryant*, 2022 U.S. App. LEXIS 9091 at *2 (6th Cir. 2022) ("the La Habra officer obtained a warrant compelling an internet service provider to turn over the subscriber information for the identified IP address."). If it can be done by local police in La Habra, California, it can be done by officers and agents around the country. Thus, bringing uniformity to the

law is yet another reason the Court should grant review in this case. There is another.

IV.

Along with the significant Fourth Amendment implications, this case also provides a vehicle to further examine the third-party doctrine in the context of modern technology.

On this issue, *Carpenter* specifically held that the doctrine does not apply to all information shared with, or generated by, a third party: "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere." 138 S. Ct. at 2217. Rather, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id*. (internal quotations and citation omitted). Even more so where the information is not "accessible to the public" but maintained in the most private place in the world – one's own home. *Id.* "[A]ny other conclusion would leave homeowners 'at the mercy of advancing technology[.]'" *Id.* at 2214 (quoting *Kyllo*, 533 U.S. at 35).

Indeed, in ruling for individual privacy in the face of technological innovations, *Carpenter* became the third piece of an unmistakable trifecta that includes *Riley* and *Kyllo.* These cases collectively stand for the proposition that "Court[s] [are] obligated – as [s]ubtler and more far-reaching means of invading privacy have become available to the Government – to ensure that the progress of science does not erode

Fourth Amendment protections." *Id*. at 2223 (internal quotations and citation omitted).

This warning is particularly apt here. The information "commanded and required" by the government's subpoena formed a chronicle of private communication activity conducted from and within the home. Knowing a household's local and long distance telephone records, means and source of payment (including any credit card or bank account number), records of session times and duration for Internet connectivity, telephone or instrument number and/or other customer/subscriber number(s) and types of service used (e.g., push-to-talk, text, three-way calling, email services, cloud computing, gaming services, etc.), is every bit as intrusive – arguably *more* intrusive – than tracking a single individual's location while in public.

Not only does such data provide far more detailed information as to personal life experiences, but it also necessarily covers *everyone* living in the home, including those as to whom there is *no* suspicion. If the government can obtain such information without making a showing of probable cause and obtaining a warrant for Mr. Liddy's home, it can constitutionally obtain such information, on its own and without judicial supervision, for any home with an Internet connection.

This Court, therefore, should grant the petition to further decide the how the Fourth Amendment will apply in a world relying more and more on technology controlled by private companies.

CONCLUSION

The Court should grant the petition for a writ of certiorari.

Dated: December 13, 2022

Respectfully submitted,

DEVIN BURSTEIN
Counsel of Record
WARREN & BURSTEIN
501 W. Broadway, Suite 240
San Diego, California 92101
Telephone: (619) 234-4433
Facsimile: (619) 234-4433
db@wabulaw.com

Attorney for Petitioner