No. __-_____

IN THE
SUPREME COURT OF THE UNITED STATES

DAVID MOREL, JR.,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

PETITION FOR A WRIT OF CERTIORARI TO THE U.S. COURT OF APPEALS FOR THE FIRST CIRCUIT

Daniel N. Marx
Counsel of Record
FICK & MARX LLP
24 Federal Street, 4th Floor
Boston, MA 02110
(857) 321-8360
dmarx@fickmarx.com

July 1, 2019

QUESTION PRESENTED

Whether the warrantless search for personal IP address information related to images that Morel privately uploaded to Imgur, an image-hosting website, was unreasonable, because Morel had a reasonable expectation of privacy in that digital information, which law enforcement officials used to track his online activity and to locate his internet-connected computer in his home?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

PETITION FOR A WRIT OF CERTIORARI

Petitioner David Morel, Jr., respectfully petitions this Court for a writ of certiorari to review the judgment of the U.S. Court of Appeals for the First Circuit.

OPINIONS BELOW

The opinion of the Court of Appeals affirming the judgment entered against Morel is reported at 922 F.3d 1 and included in the Appendix at App.1a. The order of the District Court denying the relevant suppression motion is included at App.26a.

JURISDICTION

This Court has jurisdiction under 28 U.S.C. § 1254(1), because the Court of Appeals affirmed the judgment of the District Court on April 19, 2019.

APPOINTMENT OF COUNSEL

Undersigned counsel has been appointed by the Court of Appeals, pursuant to the Criminal Justice Act of 1964, 18 U.S.C. § 3006A, to represent Morel in this case.

CONSTITUTIONAL PROVISIONS INVOLVED

U.S. Constitution, Amendment IV

> 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 person or things to be searched.

STATEMENT OF THE CASE

On November 23, 2013, the National Center for Missing and Exploited Children ("NCMEC"), a quasi-governmental agency that Congress created to assist law enforcement, received an anonymous tip concerning suspected child pornography on the internet. (App.2a-3a). In response, on November 26, 2013, NCMEC contacted Imgur, an image-hosting website, and directed the company to review specific URLs to determine if images posted to an "album" or "gallery" on the website, contained child pornography. (App.4a).

As required by federal law, Imgur reviewed the images, and it filed a report with NCMEC concerning three, recently uploaded images that appeared to contain child pornography. (App.4a). In its report to NCMEC, Imgur provided the IP address from which all three images had been uploaded. (App.4a). On December 6, 2013, Imgur filed another report concerning three additional images that also appeared to contain child pornography and had been uploaded from the same IP address. (App.5a). Using a publicly available search tool, NCMEC looked up the IP address and determined that Comcast had assigned it to a subscriber in Derry, New Hampshire. (App.4a).

Based on the IP address information from Imgur, NCMEC contacted the New Hampshire Internet Crimes Against Children Task Force ("ICAC"), and the ICAC forwarded the reports to a detective in Derry. (App.5a). The detective subpoenaed Comcast; identified the subscriber as Morel's father, and obtained his physical address. When interviewed, Morel's father told the detective, that in November 2013,

his son was living at home and the only person who used the email address associated the Comcast internet account. (App.5a-6a).

After further investigation (which is not relevant to the issues that this petition presents), on April 28, 2014, Morel was arrested at the family home in Derry. (App.8a). Morel was originally charged with attempted possession of child sexual abuse images in violation of New Hampshire law and taken into state custody.

On November 12, 2014, a federal grand jury returned an indictment that charged Morel with one count of possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). D.C. Dkt. #1. On November 20, 2014, Morel appeared in the District Court, was arraigned, and pleaded not guilty. *See* D.C. Entry (Nov. 20, 2014).

On June 9, 2015, Morel filed a motion to suppress evidence, arguing that, at NCMEC's direction, Imgur conducted an unreasonable warrantless search for personal IP address information associated with images that he had privately uploaded to the website. D.C. Dkt. #24. Morel subsequently filed several supplemental motions that addressed related issues, D.C. Dkt. #31, 33, 35, 40, and the District Court considered those papers to constitute a single suppression motion.

On February 24, 2016, following an evidentiary hearing at which a NCMEC representative and an Imgur employee testified, the District Court advised the parties to assume the challenged evidence would not be suppressed and to prepare for trial. After further briefing, D.C. Dkt. #38, 39, on April 4, 2016, the District Court denied Morel's suppression motion with a "[w]ritten order to follow," D.C. Endorsed Order (Apr. 4, 2016).

On December 19, 2016, Morel entered a conditional plea agreement that preserved his rights to appeal from the denial of his suppression motion. D.C. Dkt. #72 (confirming the appeal waiver in section 13 of the plea agreement "does not apply to the District Court's April 4, 2016 order"). On the same day, Morel appeared in court to change his plea, and the District Court accepted his guilty plea, confirming the "exceptions" to Morel's waiver of his appellate rights. D.C. Dkt. #100 at 14.

On April 14, 2017, the District Court issued an opinion and order, articulating its reasons for denying the suppression motion. D.C. Dkt. #78. On April 28, 2017, Morel moved for reconsideration of the suppression issues, D.C. Dkt. #80, but on June 26, 2017, the District Court denied that motion, D.C. Dkt. #88.

On June 27, 2017, the District Court sentenced Morel to 70 months in prison to be followed by 120 months of supervised release, and on June 30, 2017, judgment entered against Morel. D.C. Dkt. #91.

On July 5, 2017, Morel filed a timely notice of appeal. D.C. Dkt. #92. On January 22, 2019, the Appeals Court stayed proceedings pending this Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

After this Court's decision in *Carpenter* was issued, the Appeals Court heard Morel's appeal. On April 29, 2019, the Appeals Court affirmed Morel's conviction, rejecting Morel's arguments about the import of *Carpenter* for the warrantless search of his IP address information. (App.1a).

REASONS FOR GRANTING THE PETITION

I. The Question Presented Is of Exceptional Importance and Cannot Be Answered Without This Court's Review.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const., amend. IV. "The amendment grew out of American colonial opposition to British search and seizure practices, most notably the use of writs of assistance, which gave customs officials broad latitude to search houses, shops, cellars, warehouses, and other places for smuggled goods." *United States v. Wurie*, 728 F.3d 1, 3 (1st Cir. 2013), *aff'd sub nom. Riley v. California*, 573 U.S. 373 (2014).

"[A] central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2215 (2018) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). In our digital age, the need for such obstacles has grown significantly, because the power of the government to invade the "'privacies of life'" has increased dramatically. *Riley*, 573 U.S. at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 625 (1886)) (recognizing "a cell phone search," given the quantity and quality of information a typical user stores on the device, "would typically expose to the government far *more* than the most exhaustive search of a house").

In *Carpenter v. United States*, this Court recognized that new digital technologies present novel Fourth Amendment concerns, and it refused to extend the "third-party doctrine" to permit the warrantless collection of cell site location information ("CSLI"), because such digital data provides "a detailed and

comprehensive record of a person's movements" and, thus, "an intimate window into a person's private life." 138 S. Ct. at 2217.

This appeal similarly addresses the novel privacy implications of modern technology: it involves the warrantless search of personal IP address information, which can be used, like CSLI, to accomplish "near perfect surveillance." *Id.* at 2218. In fact, law enforcement officials used Morel's IP address information to track his online activity and to determine where, when, and how Morel used his personal computer in his home.[1] Just as people who use cellphones did not forfeit their Fourth Amendment rights, Morel maintained a reasonable expectation of privacy when he used the internet at his home. Accordingly, the warrantless search of his personal digital information was *per se* unreasonable.

Nevertheless, seizing on this Court's description of *Carpenter* as a "narrow" decision about CSLI (App.16a n.8) (quoting *Carpenter*, 138 S. Ct. at 2220), and disregarding this Court's broadly applicable Fourth Amendment analysis, the First Circuit held that law enforcement may conduct warrantless searches for personal IP address information (App.16a) (citing *United States v. Hood*, 920 F.3d 87 (1st Cir. 2019), and *United States v. Contreras*, 905 F.3d 853 (5th Cir. 2018)). That conclusion misunderstands the revealing nature of IP address information, and it fails to reckon

[1] Law enforcement officials routinely request staggering volumes of data, such as IP address information, from Internet Service Providers ("ISPs"), in connection with criminal investigations. According to publicly available data, in the second half of 2017 alone, Comcast received more than 11,000 requests, and nearly 80 percent of those requests were based on administrative subpoenas rather than search warrants or court orders.

with "the seismic shifts in digital technology" that raise challenging questions about how, if at all, old Fourth Amendment cases apply to the tremendous volume of consumer data constantly generated by modern devices that have become "indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2219-20 (citing *Riley*, 573 U.S. at 385).

Absent clarification from this Court, there is a significant risk that the circuit courts will misread *Carpenter* to have created only a limited "CSLI exception" to the third-party doctrine. In *Morel*, for example, the First Circuit rejected the straw-man contention that *Carpenter* "announced a wholesale abandonment of the third-party doctrine." (App.15a); (App.16a n.8) (noting "*Carpenter* did not eliminate the third-party doctrine"). That is not, and never has been, Morel's argument. More importantly, that dismissive approach misses the core principle of *Carpenter*, in which this Court recognized the need to carefully recalibrate the law of reasonable expectations of privacy for modern technology. On that basis, tis Court "decline[d] to extend" the third-party doctrine due to its inherent limitations as applied to ubiquitous consumer information in the digital age. 138 S. Ct. at 2223.

II. The Decision Below Erroneously Extended the "Third-Party Doctrine" to Reach Personal IP Address Information, Even Though that Revealing Digital Data, Like CSLI, Is Not Voluntarily Disclosed in Any Meaningful Sense by Internet Users But Can Be Used as a Powerful Surveillance Tool by Law Enforcement.

The First Circuit held "Morel's argument fails under *Carpenter*," because IP address information is different from CSLI. (App.15a). Of course, in a sense, that observation is correct. IP address information tracks connections by computers,

smartphones, and other devices to the internet, *see Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 987, n.1 (2005) ("When a device accesses the internet, it uses a unique numerical address called an Internet Protocol ("IP") address to identify itself to other computers."), and CSLI tracks connections from cell phones to cell sites, *see Carpenter*, 138 S. Ct. at 2211 ("Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information."). For Fourth Amendment purposes, however, the comparison is hardly apples to oranges. It is more like McIntoshes to Macouns.

Despite their differences, both types of digital data are "detailed, encyclopedic, and effortlessly compiled," *id.* at 2216, and enable "near perfect surveillance," *id.* at 2218. The First Circuit failed to identify any material distinction for Fourth Amendment purposes. Thus, under the rationale of *Carpenter*, the government should not be allowed to conduct warrantless searches of personal IP address information as part of criminal investigation into people's online activities.

1. Law Enforcement Can Use IP Address Information to Establish Physical Location and to Track Virtual Activity.

Emphasizing that CSLI reveals "information about location" concerning a cellphone (App.17a) (citing *Hood*, 920 F.3d at 91), the First Circuit stated that law enforcement cannot use IP address information to establish a person's physical presence or movement. That assertion is incorrect, and it also misses the larger constitutional problem with warrantless searches of personal digital data concerning online activity.

As in this case, the police routinely use IP address information to pinpoint a person's online activity *in his or her home*, the place "'where privacy expectations are most heightened.'" *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (quoting *Dow Chem. Co. v. United States*, 476 U.S. 227, 237 n.4 (1986)).

> At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of government intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable. Our cases have not deviated from this basic Fourth Amendment principle. Searches and seizures inside a home without a warrant are presumptively unreasonable absent exigent circumstances.

United States v. Karo, 468 U.S. 705, 714-15 (1984) (collecting cases). Thus, whether dealing with beepers (*Karo*), thermal imagers (*Kyllo*), or cellphones (*Carpenter*), the law must constantly assess (and re-assess) the "power of technology to shrink the realm of guaranteed privacy" in the home. *Kyllo*, 533 U.S. at 34.

Both CSLI and IP address information can establish "whether a particular article—or a person, for that matter—is in an individual's home at a particular time." *Karo*, 468 U.S. at 716. Only IP address information can also reveal what the person is doing within the premises—that is, what he or she may be reading, buying, searching for, or saying online. In other words, IP address information can be (and is) used to "reveal a critical fact about the interior of [a] premises," such as Morel's home, that the government is extremely interested in knowing and that *it could not have otherwise obtained without a warrant*." *Id.* (emphasis added).

Courts have "repeatedly recognized the utility of using IP address information to investigate child pornography offenders." *Chism v. Washington*, 661 F.3d 380, 390 (9th Cir. 2011). "Law enforcement officials can generally use an IP address to determine the physical location from which an individual logged into [a specific website]," *United States v. Blake*, 868 F.3d 960, 967 n.1 (11th Cir. 2017), and judges routinely authorize search warrants for physical locations (including private homes) linked to IP addresses that are associated with criminal activity, such as uploading child pornography to, or downloading it from, the internet, *see Chism*, 661 F.3d at 390 (collecting cases).

Moreover, by narrowly focusing on *physical* movement, the First Circuit overlooked the important parallel to *virtual* activity. IP address information "'leave[s] behind a digital footprint of all the user's internet activity.'" A. Shelton, "A Reasonable Expectation of Privacy Online: 'Do Not Track' Legislation," 45 U. Baltimore L. Forum 39, 40 (Fall 2016); *see Weinstein v. Islamic Repub. of Iran*, 831 F.3d 470, 473 (D.C. Cir. 2016) (citing *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409-10 (2d Cir. 2004) (explaining "[e]very end-user's computer that is connected to the internet is assigned a unique internet protocol number ("IP address") . . . that identifies its location (*i.e.*, a particular computer-to-network connection) and serves as the routing address for email, pictures, requests to view a web page, and other data sent across the internet from other end-users")).

> Every internet action—clicking on a website, sending an email, downloading a song, posting a photo, or instant messaging—leaves a numerical identifying mark from the computer used, allowing the user's activity to be tracked as

> he or she performs any online activity. Every time an individual makes an online purchase, searches for information on a personal health concern, reads a political blog, or sends an intimate message to a friend, that electronic action is identified by his or her Internet Protocol ("IP") address and a record of the activity is captured and stored by the Internet Service Provider ("ISP").

Shelton, *supra*, at 35-36; *see United States v. Tagg*, 886 F.3d 579, 583 (6th Cir. 2018) ("Your online 'face' is known as an 'IP address,' a unique number assigned to every computer connected to the internet."). Such personal data is "all-encompassing" in that it can be "effortlessly compiled" to create a "detailed" historical log of every click on every website. *See Carpenter*, 138 S. Ct. at 2217.

Extending the so-called "third-party doctrine" to IP address information (or other internet traffic data) would allow law enforcement officials to learn, without a search warrant (or probable cause), that an individual regularly visits websites associated with a particular political party, church group, or sexual orientation, and that data would "enable the Government to ascertain, more or less at will, [a person's] political and religious beliefs, sexual habits, and so on." *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring). As a matter of privacy, the fact that a person purchased a specific medication online (which IP address information would help to establish) is arguably more revealing than the fact that he or she drove to the pharmacy (which CSLI would show).

2. Internet Users Do Not Voluntarily Disclose Their Personal IP Address Information in Any Meaningful Sense.

In *Carpenter*, this Court recognized that CSLI is not voluntary disclosed by a cellphone user. 138 S. Ct. at 2220 ("Cell phone location information is not truly

'shared' as one normally understands the term."). Meanwhile, in *Morel*, the First Circuit asserted that, "unlike CSLI, an internet user generates the IP address data. . . only by making the affirmative decision to access a website or application." (App.17a) (quoting *Hood*, 920 F.3d at 92). But that purported distinction between the passive possession of a cellphone and the active use of the internet is illusory.

The choice to go online and visit a website is no more significant for Fourth Amendment purposes, and no more an intentional waiver of constitutional rights against unreasonable searches and seizures, than the choice to use a cellphone or to carry it (while powered on) to a particular location. "[I]n today's technologically based world, it is virtually impossible for an ordinary citizen to avoid creating metadata about himself on a regular basis simply by conducting his ordinary affairs." *ACLU v. Clapper*, 785 F.3d 787, 794 (2d Cir. 2015); *see id.* at 824 (recognizing "individuals can barely function without involuntarily creating metadata that can reveal a great deal of information about them").

The dangerous notion that people forfeit their Fourth Amendment rights by visiting websites or otherwise transmitting information on the internet would "open a veritable Pandora's Box of Internet-related privacy concerns," because "[t]he internet, by its very nature, requires *all* users to transmit their signals to third parties." *United States v. Stanley*, 753 F.3d 114, 124 (3d Cir. 2014), *cert. denied*, 135 S. Ct. 507 (2014).

> Even a person who subscribes to a lawful, legitimate internet connection necessarily transmits her signal to a modem and/or servers owned by third parties. This signal carries with it an abundance of detailed, private

> information about that user's internet activity. A holding that an internet user discloses her "signal" every time it is routed through third-party equipment could, without adequate qualification, unintentionally provide the government unfettered access to this mass of private information without requiring its agents to obtain a warrant. We doubt the wisdom of such a sweeping ruling[.]

Id. Only by not using the internet could one "escape this tireless and absolute surveillance." *Carpenter*, 138 S. Ct. at 2218.

> In our time, unless a person is willing to live "off the grid," it is nearly impossible to avoid disclosing the most personal of information to third-party providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling.

United States v. Davis, 785 F.3d 498, 525 (11th Cir. 2015) (*en banc*) (Rosenbaum, J. concurring), *cert. denied*, 136 S. Ct. 479 (2015).

Fortunately, the Constitution does not require citizens to choose between using new technology or maintaining their privacy. Rather, "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo*, 533 U.S. at 34). The same careful balance must be struck regarding personal IP address information. The fact that ISPs generate and assign IP address information for "commercial purposes" does not "negate" a person's "anticipation of privacy" in websites visited, searches conducted, or files viewed (or

shared in a limited way) on the internet from a computer, or other internet-connected device associated with a particular IP address. *Id.* at 2217.

Consistent with the constitutional principles that this Court articulated in *Carpenter*, most people have—and consider reasonable—an expectation of privacy in their online activities. About 90 percent of U.S. adults now use the internet, and 77 percent report that they use it either "several times a day" or "almost constantly." M. Anderson & A. Perrin, "Tech Adoption Climbs Among Older Adults," Pew Research Ctr. (May 17, 2017) at 21. Most people feel it is "very important" to keep private the records of their internet activity, such as "the people to whom they are sending emails, the place where they are when they are online, and the content of the files they download"—all of which are identifiable by aggregating IP address information with other commercially available, consumer data. L. Rainie, "Anonymity, Privacy, and Security Online," Pew Research Ctr. (Sept. 5, 2013) at 3. Similarly, the majority of internet users consider the websites they have visited to be "very sensitive" or "somewhat sensitive" information. M. Madden, "Public Perceptions of Privacy and Security in the Post-Snowden Era," Pew Research Ctr. (Nov. 12, 2014) at 31. Such polling data confirms this Court's view that most people would not "accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year." *Jones*, 565 U.S. at 418 (Sotomayor, J., concurring).

3. IP Address Information Can Be Easily and Cheaply Aggregated with Other Available Data as a Powerful Surveillance Tool.

In an effort to minimize the significance of IP address information, the First Circuit characterized such data as "merely a string of numbers associated with a device that had, at one time, accessed a wireless network," permitting an inference but not independently proving any fact. (App.17a) (quoting *Hood*, 920 F.3d at 92). True, but the same description applies to almost all evidence when viewed in isolation, including CSLI. In *Carpenter*, this Court explained the police were able to "deduce a detailed log of Carpenter's movements" by aggregating location data from his cell phone and analyzing it "*in combination with other information*." 138 S. Ct. at 2218 (emphasis added).

"Rules that permit the government to obtain records and other information that consumers have shared with businesses without a warrant seem much more threatening as the extent of such information grows." *ACLU*, 785 F.3d at 822-23. As with cellphone service providers that collect "increasingly vast amounts of increasingly precise CSLI" concerning all their subscribers. *Carpenter*, 138 S. Ct. at 2212. ISPs routinely log the date, time, duration, and access device associated with every internet session for all IP addresses. Modern surveillance techniques depend on collecting, aggregating, and analyzing these vast stores of information. *See, e.g.*, *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *see also* S. Friedland, "Of Clouds and Clocks: Police Location Tracking in the Digital Age," 48 Tex. Tech. L. Rev. 165, 177 (2015) (explaining how government agencies and private companies "aggregate

and crunch information through Big Data, sifting through vast buckets of seemingly unrelated bits of information to develop clues about people's habits and propensities"). "Bits and pieces of data" can have significant privacy implications, because they "may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself," *CIA v. Sims*, 471 U.S. 159, 178 (1985), and people have reasonable expectations of privacy in the "mosaic of information," *Clapper*, 785 F.3d at 823.

Moreover, as with GPS tracking information, IP address information is not subject to the sort of "practical" constraints that, "[i]n the precomputer age," limited the ability of law enforcement officials to conduct extensive, long-term surveillance of a suspect. *Jones*, 556 U.S. at 429 (Alito, J., concurring). "Traditional surveillance for any extended period of time was difficult and costly," and as a result, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not secretly monitor and catalogue" a person's movements or activities "for a very long period." *Id.* at 430. In contrast, however, modern technologies "make long-term monitoring relatively easy and cheap." *Id.* at 429.

In the context of CSLI, this Court explained the problem as follows:

> In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound

> tracking capacity runs against everyone. Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when.
>
> Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment.

Carpenter, 138 S. Ct. 2218. Law enforcement officials use historical IP address information in the same way to achieve "near perfect surveillance" concerning the online activity of persons who turn out to be suspects in criminal investigations. *Id.*

Notably, in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), this Court initially applied the "third-party doctrine" in a limited fashion to "short-term, forward-looking (as opposed to historical), and highly-limited data collection." *Klayman v. Obama*, 957 F. Supp. 2d 1, 32 (D.D.C. 2013), *vacated on other grounds*, 800 F.3d 559 (D.C. Cir. 2015). But this case, like *Carpenter*, involves long-term, historical data that "presents even greater privacy concerns" than real-time surveillance, such as GPS tracking or beeper monitoring. *Carpenter*, 138 S. Ct. at 2218 (explaining the "retrospective quality" of such data "gives police access to a category of information otherwise unknowable").

III. This Case Is an Ideal Vehicle to Clarify the Implications of *Carpenter* Because the Good-Faith Exception Does Not Apply.

Morel's petition gives this Court an important opportunity to clarify how *Carpenter* and the third-party doctrine apply to IP address information. Moreover, the resolution of these issues is critical to the outcome of Morel's case, because the

good-faith exception of *United States v. Leon*, 468 U.S. 897 (1984), does not apply here and, thus, cannot excuse the warrantless search that law enforcement conducted.

When the warrantless search of Morel's IP address information was conducted in or about January 2014, no "binding appellate precedent" from this Court or the First Circuit "specifically *authorize[d]* that particular police practice." *Davis v. United States*, 564 U.S. 229, 241 (2011) (emphasis in original; alteration added). In fact, a reasonable investigator would have known that, in *Jones*, this Court refused to extend the third-party doctrine to warrantless GPS tracking and, by implication, raised important questions about warrantless searches of modern consumer data, including CSLI and IP address information.

The good-faith exception is "not a license for law enforcement to forge ahead with new investigative methods in the face of uncertainty as to their constitutionality." *United States v. Sparks*, 711 F.3d 58, 67 (1st Cir. 2013). Rather "[w]hen confronting new concerns wrought by digital technology," the police, like the courts, must be "careful not to uncritically extend existing precedents" that appear to authorize warrantless searches of private information. *Carpenter*, 138 S. Ct. at 2222. And "where judicial precedent does not clearly authorize a particular practice, suppression has deterrent value because it creates an 'incentive to err on the side of constitutional behavior.'" *Sparks*, 711 F.3d at 64 (quoting *Davis*, 598 F.3d at 1266-67 (quoting *United States v. Johnson*, 457 U.S. 537, 561 (1982))). In this case, suppression would have "deterrent value," because law enforcement improperly erred on the side of crime detection, not "constitutional behavior." *Id.*

Finally, "[w]hether the exclusionary sanction is appropriately imposed in a particular case" depends on whether the benefit of "deter[ring] future Fourth Amendment violations" outweighs "the 'substantial social costs'" of suppressing evidence in a particular case, *Davis*, 564 U.S. at 236-37 (quoting *Leon*, 468 U.S. at 907), because "its bottom-line effect, in many cases, is to . . . set the criminal loose in the community without punishment," *id.* Here, there is no risk that Morel will "go free because the constable blundered." *Id.* (quoting *People v. Defore*, 242 N.Y. 13, 21 (1926) (Cardozo, J.)). Even if Morel prevails, he will have already served his severe punishment, a 70-month sentence in federal prison. Because society will pay no cost, the deterrent benefit of encouraging the police to tread carefully with warrantless searches of IP address information tips the balance in favor of suppression.

CONCLUSION

For the foregoing reasons, Petitioner David Morel, Jr., respectfully requests that this Court grant his petition for a writ of certiorari, vacate the decision of the Court of Appeals, and remand to the District Court for further proceedings.

Respectfully submitted,

DAVID MOREL, JR.

By his attorney,

/s/ Daniel N. Marx

Daniel N. Marx
Counsel of Record
FICK & MARX LLP
24 Federal Street, 4th Floor
Boston, MA 02110
(857) 321-8360
dmarx@fickmarx.com

Dated: July 1, 2019

APPENDIX