24-2180(L)

24-2182(CON)

United States Court of Appeals

FOR THE SECOND CIRCUIT

UNITED STATES OF AMERICA,

Appellant,

—v.—

BRUCE SILVA, also known as Sealed Defendant 1

Defendant-Appellee,

(*Caption continued on inside cover*)

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

Amicus Brief on behalf of the National Association for Criminal Defense Lawyers and New York State Association of Criminal Defense Lawyers for Defendant-Appellant Bruce Silva

Richard D. Willstatter
Vice Chair, NACDL's *Amicus Curiae* Committee for Second Circuit
Green & Willstatter, Attorneys at Law
200 Mamaroneck Avenue, Suite 605
White Plains, New York 10601
(914) 948-5656

Stephen N. Preziosi
Chair, *Amicus Curiae* Committee
New York State Association of Criminal Defense Lawyers
48 Wall Street, 11th Floor
New York, New York 10005
(212) 960-8267

Adeel Bashir
Amicus Counsel
NACDL *Amicus Curiae Committee*
400 N. Tampa Street
Suite 2660
Tampa, Florida 33609
(703) 835-3929
adeel_bashir@fd.org

Shadell McBride, AKA Sealed Defendant 5, Justin Ballester, AKA Sealed Defendant 6, Alzubair Saleh, AKA Sealed Defendant 7, Giovanni Rodriguez, AKA Sealed Defendant 8, Gabriel Valdez, AKA Sealed Defendant 9, Emmanuel Perez, AKA Sealed Defendant 10, Jordan Bennett, AKA Sealed Defendant 3, Elijah Pough, AKA Sealed Defendant 4, Bruce Melvin, AKA Sealed Defendant 2,

Defendants.

Corporate Disclosure Statement

Amicus curiae is not owned by a parent corporation. No publicly held corporation owns more than ten percent of stock in *amicus*.

TABLE OF CONTENTS

Contents **Page**

Corporate Disclosure Statement i

Table of Contents ii

Table of Citations iv

Interest of *Amicus Curiae* 1

Introduction and Summary of the Argument 3

Argument 5

I. The Founders crafted the Fourth Amendment's particularity requirement to prevent the type of boundless search authority the government seeks here — the power to search any device based on generalized assumptions rather than case-specific evidence 5

A. The Fourth Amendment's nexus requirement 5

B. The Government's limitless theory for establishing probable cause would swallow *Riley*'s protections and render the Fourth Amendment's nexus requirement a mere formality. 10

C. Officer experience cannot substitute for case-specific evidence to establish a Fourth Amendment nexus 17

D. The government's arguments underscore the need to uphold the Fourth Amendment's requirement that a warrant be issued only upon a showing of a case-specific nexus between a cell phone and alleged criminal activity 21

TABLE OF CONTENTS
-continued-

II. The good faith exception cannot excuse reliance on a warrant affidavit that fails to establish any nexus between a cell phone and an alleged crime. 26

Conclusion 31

Certificate of Compliance 33

TABLE OF CITATIONS

Caselaw and Constitutional Authorities **Page(s)**

Boyd v. United States, 116 U.S. 616 (1886) 6

Commonwealth v. Broom, 52 N.E.3d 81 (Mass. 2016) 18

Commonwealth v. White, 59 N.E.3d 369 (Mass. 2016) 18

Coolidge v. New Hampshire, 403 U.S. 443 (1971) 6

Diaz v. United States, 144 S. Ct. 1727 (2024) 19

Illinois v. Gates, 462 U.S. 213 (1983) 6

In re 650 Fifth Ave. & Related Props.,
830 F.3d 66 (2d Cir. 2016) 5

Maryland v. Garrison, 480 U.S. 79 (1987) 5

Maryland v. Pringle, 540 U.S. 366 (2003) 7

Riley v. California, 573 U.S. 373 (2014) 3, 8, 9, 10, 16, 21, 24, 26, 29, 30, 31

Stanford v. Texas, 379 U.S. 476 (1965) 5, 6

State v. Baldwin, 664 S.W.3d 122 (Tex. Crim. App. 2022) 18, 19

State v. Thein, 138 Wash. 2d 133 (1999) 18

Steagald v. United States, 451 U.S. 204 (1981) 7

United States v. Boles, 914 F.3d 95 (2d Cir. 2019) 7

United States v. Brown, 828 F.3d 375 (6th Cir. 2016) 8

United States v. Brown, 676 F. Supp. 2d 220 (S.D.N.Y. 2009) 23

TABLE OF CITATIONS
-continued-

United States v. Donald, 417 F. App'x 41 (2d Cir. 2011) 24

United States v. Falso, 544 F.3d 110 (2d Cir. 2008) 6

United States v. Galpin, 720 F.3d 436 (2d Cir. 2013) 8

United States v. Ganias, 824 F.3d 199 (2d Cir. 2016) 8

United States v. Gatto, 313 F. Supp. 3d 551 (S.D.N.Y. 2018) 23

United States v. Gomez, 652 F. Supp. 461 (E.D.N.Y. 1987) 18

United States v. Griffith, 867 F.3d 1265 (D.C. Cir. 2017) 8

United States v. Hoey, 2016 WL 270871 (S.D.N.Y. 2016) 23

United States v. Lauria, 70 F.4th 106 (2d Cir. 2023) 6, 7

United States v. Leon, 468 U.S. 897 (1984) 27, 28, 31

United States v. Pabon, 871 F.3d 164 (2d Cir. 2017) 7

United States v. Pinto-Thomaz, 352 F. Supp. 3d 287 (S.D.N.Y. 2018) 23

United States v. Purcell, 967 F.3d 159 (2d Cir. 2020) 5

United States v. Robinson, 2018 WL 5928120 (E.D.N.Y. 2018) 23

United States v. Rosa, 626 F.3d 56 (2d Cir. 2010) 16

United States v. Singh, 390 F.3d 168 (2d Cir. 2004) 7

United States v. Watson, 2023 WL 7300618 (E.D.N.Y. 2023) 23

TABLE OF CITATIONS
-continued-

U.S. Const. amend. IV 3, 4, 5, 6, 9, 10, 13, 15, 16, 17, 18, 19, 20, 21, 22, 24, 25, 26, 27, 28, 29, 30, 31, 32

Velardi v. Walsh, 40 F.3d 569 (2d Cir. 1994) 24

Other Authorities

Brian Walsh & Tiffany Joslyn, The Heritage Foundation and NACDL, Without Intent: How Congress is Eroding the Criminal Intent Requirement in Federal Law 2-4, 6 (Apr. 2010) 13

Consumer Affairs, Cell Phone Statistics: How We Use Our Phones in 2023 20

Gabrielle Fonrouge & Ben Feuerherd, *Inside the FBI Cell Phone Scheme That Took Down Gangs Across Globe*, N.Y. Post (June 8, 2021) 20

GianCarlo Canaparo et al., The Heritage Foundation, *Count the Code: Quantifying Federalization of Criminal Statutes* 5 (Jan. 7, 2022) 13

Matthew Tokson & Michael Gentithes, *The Reality of the Good Faith Exception*, University of Utah College of Law Research Paper No. 546, 12 (April 10, 2023) 27

Neil Gorsuch, "Over Ruled: The Human Toll of Too Much Law," PBS (Nov. 25, 2024) 14

Pew Research Center, Mobile Fact Sheet, Pew Research Center: Internet & Technology (Nov. 2024) 10, 11

Togher, L., *Strategies to Improve Research Outcomes in the Field of Acquired Brain Injury: The Kevin Bacon Effect, Networking and Other Stories.* Brain Impairment, 13(2), 271-280 (Cambridge Uni. Press 2012) 12, 13

World Economic Forum, Charted: There Are More Phones Than People in the World (April 2023) 11

INTEREST OF *AMICUS CURIAE*[1]

Amicus curiae, the National Association of Criminal Defense Lawyers (NACDL), is a non-profit, voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crimes or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous amicus briefs each year in the U.S. Supreme Court and other federal and state courts, in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal legal system as a whole.

---

[1] Undersigned counsel hereby certifies that counsel for both appellant and appellee were notified of the intent to file this brief. All parties have consented to the filing of this brief. Additionally, opposing counsel has indicated that the United States does not intend to file a response to this brief.

The New York State Association of Criminal Defense Lawyers (NYSACDL) is a not-for-profit corporation with a subscribed membership of more than 1,700 attorneys, including private practitioners, public defenders, and law professors, and is the largest private criminal bar in the State of New York. It is a recognized state affiliate of the NACDL and, like that organization, works on behalf of the criminal defense bar to ensure justice and due process for those accused and convicted of crimes.[2]

[2] No party or its counsel authored this brief in whole or part. No party or its counsel, nor any other person, contributed money to fund its preparation or submission.

Introduction and Summary of Argument

The Fourth Amendment's warrant requirement stands as a bulwark against general, exploratory searches of the kind the Founders sought to prohibit. Yet the government here asks this Court to adopt a rule that would effectively nullify this protection in the digital age: the mere presence of a cell phone, combined with suspicion of any crime, automatically creates probable cause to search that device. Amici urge this Court to reject this dangerous proposition and affirm the district court's suppression ruling.

The government's position would transform *Riley v. California*'s warrant requirement into an empty formality. Under its theory, law enforcement could obtain a warrant to search any cell phone based solely on generalized assumptions about how people use phones in modern life, disguised as specialized observations based on an officer's training and experience. This approach contradicts *Riley* and threatens to eviscerate the Fourth Amendment's core protection against general warrants and writs of assistance.

Riley recognized that cell phones contain "the privacies of life" and deserve heightened constitutional protection. 573 U.S. 373, 403 (2014). Allowing warrants based on boilerplate assertions about cell phone use

without requiring case-specific evidence linking the device to alleged criminal activity would be like allowing general warrants for the digital age. That result is even more alarming when considering the ubiquity of phones in modern life and the vast amount of personal information they contain.

The district court properly suppressed the search warrant issued by the Magistrate Judge and correctly declined to apply the good faith exception, recognizing that the warrant's complete failure to establish any nexus between the phone and the alleged crime rendered reliance on it unreasonable. This Court should affirm those sound decisions to preserve meaningful Fourth Amendment protections in the digital age.

Argument

I. The Founders crafted the Fourth Amendment's particularity requirement to prevent the type of boundless search authority the government seeks here — the power to search any device based on generalized assumptions rather than case-specific evidence.

A. The Fourth Amendment's nexus requirement.

The Fourth Amendment guarantees that "[t]he 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 [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. By its text, the Fourth Amendment demands both probable cause and particularity, with these requirements working in tandem to ensure searches are "carefully tailored to their justifications" and do not become exploratory fishing expeditions. *In re 650 Fifth Ave. & Related Props.*, 830 F.3d 66, 98 (2d Cir. 2016); *see also Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *United States v. Purcell*, 967 F.3d 159, 178 (2d Cir. 2020).

This nexus requirement emerged from the Founders' experience with general warrants that allowed Crown officials "to search where they pleased." *Stanford v. Texas*, 379 U.S. 476, 481 (1965). This

historical context underscores how general warrants contributed to the Revolution and shaped the Fourth Amendment's core protections. *See Boyd v. United States*, 116 U.S. 616, 624–30 (1886).

So, at its heart, the warrant requirement combats one of the most significant privacy concerns raised by forensic searches of digital devices—their potential to become open-ended fishing expeditions into the most private aspects of our lives. As the Supreme Court has emphasized, "[t]he specific evil is the general warrant abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

Building on this foundation, courts examine whether the issuing judge had a "substantial basis" for concluding that "a search would uncover evidence of wrongdoing." *Illinois v. Gates*, 462 U.S. 213, 236 (1983). While probable cause is a "fluid concept" that resists reduction to rigid rules, *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (citing *Gates*, 462 U.S. at 232), it consistently requires more than speculation or hunches, *United States v. Lauria*, 70 F.4th 106, 128 (2d Cir. 2023).

Determining probable cause thus requires evaluating the totality of circumstances in each case to find a fair probability that evidence will be found in a particular location. *See United States v. Boles*, 914 F.3d 95, 102 (2d Cir. 2019). Moreover, this "fair probability" must be grounded in concrete facts that connect the alleged crime to the location rather than generalized assumptions about what might typically be found in similar situations. *Lauria*, 70 F.4th at 128.

The analysis becomes even more exacting when distinguishing between probable cause to search and probable cause to arrest. *See United States v. Pabon*, 871 F.3d 164, 181 (2d Cir. 2017); *Steagald v. United States*, 451 U.S. 204, 212–13 (1981)). Search warrants specifically require "a sufficient nexus between the criminal activities alleged" and the location or items to be searched. *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004); *Warden, Md. Penitentiary v. Hayden*, 387 US 294, 307 (1967) (providing that there must "be a nexus…between the item to be seized and criminal behavior."). This nexus depends on case-specific facts evaluated under the totality of circumstances. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003).

The nexus requirement takes on heightened importance in the context of digital devices. For instance, this Court has emphasized that

the particularity requirement assumes even greater significance when searching computer hard drives. *See United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013). Digital searches give the government access to "a vast trove of personal information," much of which may be irrelevant to the investigation. *United States v. Ganias*, 824 F.3d 199, 217 (2d Cir. 2016) (en banc). The potential for privacy violations in such searches is "enormous," compounded by the vast storage capacity of digital devices. *Galpin*, 720 F.3d at 447.[3]

Riley v. California, 573 U.S. 373 (2014), underscores these principles, rejecting attempts to analogize cell phone searches to

---

[3] The importance of case-specific evidence in digital searches is well-illustrated by key circuit decisions. For instance, in *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017), the D.C. Circuit rejected an affidavit that relied solely on an officer's experience-based assertion that gang members maintain regular contact with each other and often stay advised and share intelligence about their activities through cell phones. *See id.* at 1273-74. The court found this reasoning insufficient to establish probable cause, noting that cell phones are typically carried on a person, unlike physical evidence that might reasonably be stored at home, requiring more specific evidence to justify their search. *See id.* Analogously, in *United States v. Brown*, 828 F.3d 375 (6th Cir. 2016), the Sixth Circuit suppressed evidence because the affidavit 'failed to establish the required nexus between the alleged drug trafficking and Brown's residence. *See id.* at 382. The court emphasized that if an affidavit lacks facts directly connecting the location with suspected criminal activity, it cannot be inferred that drugs will be found in the defendant's home—even if the defendant is a known drug dealer. *See id.* at 384.

physical searches given their qualitative and quantitative differences. The Court likened such comparisons to "saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* at 393. Cell phones, containing "the privacies of life," demand even greater protection than searches of homes. *Id.* at 403.

Together, the longstanding nexus requirement and the extraordinary privacy implications of cell phones compel a robust Fourth Amendment rule that demands case-specific evidence to justify a warrant for a cell phone search. Without a concrete nexus, the potential for abuse and overreach is magnified, transforming the particularity requirement into an empty gesture and permitting the very general searches the Fourth Amendment was designed to prohibit. The unique nature of cell phones, as recognized in *Riley*, only heightens the need for vigilance. Given their ubiquity in modern society, immense storage capacity, and their ability to reveal "the privacies of life," cell phones cannot be treated as mere containers subject to broad assumptions and speculative reasoning. Upholding the nexus requirement for cell phones is thus essential to preserving the balance between privacy and law enforcement authority that the Fourth Amendment strikes.

B. The Government's limitless theory for establishing probable cause would swallow *Riley*'s protections and render the Fourth Amendment's nexus requirement a mere formality.

The probable cause standard the government advocates for would undermine the core privacy protections that motivated *Riley*'s warrant requirement. Under the government's theory, the very ubiquity of cell phones in modern life—the same characteristic that led the *Riley* Court to demand heightened Fourth Amendment protection—would paradoxically justify more expansive government searches. This reasoning misunderstands the probable cause nexus requirement.

Rather than providing specific evidence linking a particular device to criminal activity, the government attempts to substitute generalized assumptions about how people use cell phones. This approach would transform *Riley*'s careful balance between privacy and law enforcement needs into an empty formality, permitting the government to search any cell phone based on little more than speculation about typical patterns of use.

Cell phones have become essential tools of modern life. According to the Pew Research Center, 98% of Americans own a cell phone, and

mobile subscriptions now exceed the global population.[4] Phones serve as the primary means for everything from communication and navigation to personal documentation. Globally, mobile subscriptions exceed the number of people on the planet.[5] This prevalence, while reflecting their utility, makes cell phones unreliable indicators of criminal activity without a case-specific nexus.

Silva's case demonstrates the fatal flaw in the government's reasoning. The government's warrant application—filed two weeks after Silva's arrest on felon-in-possession charges but nearly a year before any racketeering charges—attempts to transform an unremarkable fact of modern life into probable cause: Silva, like most Americans, had a cell phone; and he happened to have it on him when he was arrested.

The government recites various allegations about Silva: his alleged gang membership since the late 2000s; a shooting incident from 2019; his status as a fugitive in late 2021; and supposed participation in financial scams. While these allegations might establish probable cause

---

[4] Pew Research Center, Mobile Fact Sheet, Pew Research Center: Internet & Technology (Nov. 2024), https://tinyurl.com/5c8r2v8p.

[5] World Economic Forum, Charted: There Are More Phones Than People in the World (April 2023), https://tinyurl.com/56sdf47u.

that Silva was involved in criminal activity (and thus establish probable cause for his arrest), they say nothing about probable cause to search his phone. The warrant affidavit simply generalizes that because Silva had a phone, and because phones can be used to communicate, his phone must contain evidence of crime.

This generalization becomes even more tenuous when examining what the affidavit lacks. For example, the warrant affidavit contains:

- No evidence of communications between Silva and other gang members linked to prior investigations.
- No photos, videos, or social media posts tied to Silva's phone and connected to the alleged gang activity.
- No witness statements or co-conspirator testimony identifying Silva's phone as being used in the crimes.
- No specific details about the Dub City gang's use of cell phones, or Silva's particular use of his device.

Rather than providing this kind of case-specific evidence, the government offers only boilerplate assertions about how gang members "often use cellular telephones" and "frequently" store photos of their activities. This circular logic would apply equally to any person carrying a phone who is suspected of any crime. The government argues that because phones are tools of modern life, and because criminals (like everyone else) use them for pretty much everything, phones must contain evidence of crime. This approach creates what some may call

the "Kevin Bacon effect"[6] of probable cause: the government's logic would allow any crime to be connected to a cell phone through increasingly attenuated links. But the Fourth Amendment demands more than these theoretical connections - it requires direct, case-specific evidence linking the device to criminal activity.

The government's approach becomes even more troubling when viewed against the backdrop of modern overcriminalization. On just the federal level, "Congress has spread crimes throughout the Code, resulting in what scholars have described as an incomprehensible, random and incoherent, duplicative, ambiguous, incomplete, and organizationally nonsensical mass of federal legislation that carries criminal penalties."[7] In a world where, as Justice Gorsuch notes, the

---

[6] The "Kevin Bacon" effect refers to how any actor in Hollywood can be connected to Kevin Bacon through a chain of movies they've appeared in together, typically within six steps or fewer, and, more generally, how any two people on Earth can be connected through acquittances in six or fewer degrees. *See generally*, Togher, L., *Strategies to Improve Research Outcomes in the Field of Acquired Brain Injury: The Kevin Bacon Effect, Networking and Other Stories*. Brain Impairment, 13(2), 271-280 (Cambridge Uni. Press 2012).

[7] GianCarlo Canaparo et al., The Heritage Foundation, *Count the Code: Quantifying Federalization of Criminal Statutes* 5 (Jan. 7, 2022) (citations and quotations omitted); *see also* Brian Walsh & Tiffany Joslyn, The Heritage Foundation and NACDL, Without Intent: How

average American unwittingly commits multiple crimes daily, the government's logic would transform every routine inspection and minor violation into grounds for invasive cell phone searches.[8]

Cell phones have become our photo album, calendar, personal guide, communication hub, and diary all in one. Under the government's reasoning, this essential device becomes vulnerable to search whenever someone runs afoul of even the most minor regulation.

Consider a restaurant owner cited for a minor health code violation—perhaps an improperly calibrated refrigerator or incorrect food storage temperatures. Under the government's probable cause logic, this commonplace citation would justify searching the owner's entire phone. After all, the cell phone inevitably contains text messages with employees about food handling procedures, calendar entries for equipment maintenance, emails about health inspections, and

---

Congress is Eroding the Criminal Intent Requirement in Federal Law 2-4, 6 (Apr. 2010).

[8] The problem of overcriminalization is recognized at the highest levels of our judiciary. Justice Neil Gorsuch, for instance, recently noted, while discussing his book "Over Ruled: The Human Toll of Too Much Law" on PBS's Frontline, that "according to many scholars, there are now so many federal laws on the books—crimes—that every American over the age of 18 commits one felony a day." Neil Gorsuch, PBS (Nov. 25, 2024), https://tinyurl.com/4js7mtd3.

communications with suppliers about deliveries. What began as a simple regulatory matter would become a gateway to examine years of private communications, photos, and business records.

This problem extends well beyond food service. A street vendor operating without proper permits would face not just a fine but potential exposure to their entire digital life. Because vendors naturally use phones to coordinate locations, manage inventory, advertise their services on social media, and communicate with customers, the government could claim probable cause to search any vendor's phone based on a simple licensing violation.

The same intrusive logic would apply to a weekend fisherman caught without a proper license. Because modern anglers use their phones to check weather conditions, mark GPS coordinates, photograph their catches, and coordinate trips with friends, the government could argue that evidence of the licensing violation must exist on the device.

These examples show how the government's flawed syllogism supporting probable cause would effectively nullify the Fourth Amendment's particularity requirement. When nearly every minor violation involves some phone use, and every phone contains vast

personal data, the government's approach creates exactly what *Riley* sought to prevent—a general warrant for the digital age.

Riley, in fact, rejected this exact line of reasoning where the government argued that cell phone searches should be allowed whenever it was "reasonable to believe" the phone contained evidence of the crime of arrest. The Court emphasized that such a standard "would prove no practical limit at all," as "it would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone." 573 U.S. at 399.

The government's reliance on generalized assertions about cell phone use contradicts established Fourth Amendment principles. *See United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010) (finding a warrant defective for failing to link the items to be searched with the alleged criminal activity). The Fourth Amendment's protections become mere formalities without a concrete and particularized nexus between the phone and alleged criminal activity, supported by specific evidence rather than general assumptions. The government's proposed approach would thus render Fourth Amendment protections hollow, transforming the Fourth Amendment's particularity requirement into a simple box-

checking exercise. But this is exactly the type of general warrant that the Fourth Amendment was designed to prevent.

C. Officer experience cannot substitute for case-specific evidence to establish a Fourth Amendment nexus.

The government's reliance on officer training and experience is as troubling as it is flawed; it would replace the Fourth Amendment's demand for particularized suspicion with a categorical rule that experienced officers can search any gang member's phone based solely on general knowledge about how phones can be used in criminal enterprises.

Here, the government points to Detective Boyer's assertions, supposedly gleaned from his training and experience, that "gang members use cell phones." But what is couched as specialized knowledge is little more than a truism—akin to saying water is wet.

Everyone uses cell phones, including for a wide range of lawful and unlawful activities. While such statements reflect general human behavior, they offer no case-specific evidence tying Silva's phone to the alleged gang activity.

Allowing "training and experience" alone to substitute for specific, case-based evidence creates a dangerous loophole in Fourth

Amendment protections. Courts have consistently rejected attempts to substitute officer experience for specific, case-based evidence. (*See, e.g.*, *United States v. Gomez*, 652 F. Supp. 461, 463 (E.D.N.Y. 1987) (holding that while an agent's specialized knowledge can be considered, it cannot alone establish probable cause without specific evidence connecting illegal activity to the place searched); *State v. Thein*, 138 Wash. 2d 133, 147–48 (1999) (rejecting generalizations that drug dealers often store drugs at home as insufficient for probable cause); *Commonwealth v. Broom*, 52 N.E.3d 81, 89 (Mass. 2016) (requiring a "substantial, particularized basis" connecting phone files to the crime under investigation)).

This principle applies with particular force to cell phone searches. Courts have consistently rejected boilerplate assertions about how criminals use phones as a basis for probable cause. *See Commonwealth v. White*, 59 N.E.3d 369 (Mass. 2016) (rejecting argument that defendants in group crimes often use phones to communicate); *State v. Baldwin*, 664 S.W.3d 122, 134 (Tex. Crim. App. 2022) (holding that

boilerplate language about criminal phone use must include specific facts connecting the phone to the alleged offense).[9]

The government's "training and experience" argument suffers from an additional flaw; it overlooks the realities of how people—especially criminals—use and replace their phones. Cell phones are not static objects uniquely tied to an individual. They are dynamic, often replaced, and often disconnected from the prolonged activities law enforcement seeks to investigate. For many people, upgrading phones is routine: nearly 12% of individuals purchase new phones every year, 4%

---

[9] The government's reliance on training and experience also reveals a troubling inconsistency in its approach to group-based inferences. For example, as Justice Gorsuch recently observed when addressing expert testimony about a defendant's mental state based on generalizations about group behavior, there is an inherent logical gap between evidence about what "most" people in a group think and proof of what any specific individual actually thought. *See Diaz v. United States*, 144 S. Ct. 1727, 1738, 1744 (2024) (Gorsuch, J., dissenting) (noting the difficulty in seeing how the government can simultaneously maintain that expert opinions about "most" people are not directly "about" the defendant's mental state while still claiming such opinions are relevant to proving that mental state). Yet here, the government asks courts to accept an even more attenuated inference—that probable cause exists to search a specific phone based solely on generalizations about how, in the detective's view, gang members typically use phones. If such group-based reasoning is questionable even under the more rigorous standards for expert testimony at trial, it makes sense that such inferences cannot satisfy the Fourth Amendment's requirement for particularized probable cause to conduct invasive digital searches.

upgrade every six months, and the majority—55%—replace their phones every two to three years.[10] This rapid turnover makes it unreliable to assume that a specific device will contain meaningful evidence of long-past events.

This disconnect is even more pronounced for criminals, who often use "burner phones"—prepaid, disposable devices designed specifically to avoid detection. The prevalence of burner phones in criminal enterprises (demonstrated by the FBI's successful use of compromised burner phones to infiltrate major criminal organizations) highlights the speculative nature of assuming Silva's personal phone would contain evidence of criminal activity.[11]

This is all to say that even if Silva had used a phone during the alleged crimes, it could have been a burner phone, long since discarded. The government's boilerplate reasoning fails to consider these realities,

---

[10] *See* Consumer Affairs, Cell Phone Statistics: How We Use Our Phones in 2023, https://tinyurl.com/yckcwtt4.

[11] *See* Gabrielle Fonrouge & Ben Feuerherd, *Inside the FBI Cell Phone Scheme That Took Down Gangs Across Globe*, N.Y. Post (June 8, 2021), https://tinyurl.com/y6vukjkj (reporting how the FBI duped criminals across the globe into buying cellphones that had pre-loaded FBI software on them — and exposed Asian Triad gangs, Middle Eastern organized crime outfits, Latin American drug cartels, and even biker crews to police investigators).

instead relying on a simplistic narrative that presumes a consistent and meaningful connection between individuals and their phones. Such assumptions fail to meet the Fourth Amendment's demand for particularity, making the government's case for probable cause constitutionally insufficient.

D. The government's arguments underscore the need to uphold the Fourth Amendment's requirement that a warrant be issued only upon a showing of a case-specific nexus between a cell phone and alleged criminal activity.

The government's attempts to defend the warrant rest on misunderstandings of the legal standard and overly broad generalizations that would transform *Riley*'s warrant requirement into a mere formality - one satisfied whenever law enforcement asserts that criminals commonly use phones.

First, the government incorrectly claims that the district court "improperly required a standard higher than probable cause for cell phone search warrants" (GB 29). This assertion misrepresents the applicable legal framework. Both the Supreme Court and the Second Circuit, in decisions predating *Riley*, have consistently required a factual nexus between the place to be searched and the alleged criminal activity. Far from imposing a heightened standard, the district court

adhered to this long-standing principle, ensuring that the Fourth Amendment's protections remained meaningful.

By requiring evidence connecting Silva's cell phone to the alleged criminal activity, the district court did not create a new standard but instead upheld the Fourth Amendment's demand for particularity. This approach was not only appropriate but necessary to prevent the constitutional protections of the Fourth Amendment from being reduced to a mere formality.

Next, the government wrongly contends that there was a "common-sense inference" of probable cause because this case involves a long-running criminal conspiracy, and cell phones often contain communications, photographs, and other evidence of crime (GB 31). This argument, however, amounts to little more than a recognition about how people communicate in the modern era. The mere fact that cell phones are indispensable part of our daily lives does not create a particularized basis for searching any individual's device.

The Fourth Amendment requires more than generalizations about how technology might be used in criminal activity; it demands specific facts linking the phone to the alleged crime. The government's reliance on a "common-sense inference" disregards this principle, offering broad

assumptions about cell phone use in place of the particularized evidence required to establish probable cause.[12]

The government further analogizes this case to the search of a home, asserting that a home may be searched for evidence of drug

---

[12] The government argues that the inferences drawn here by the Magistrate Judge are precisely the type of common-sense and experience-based conclusions that the Supreme Court and other courts have long routinely relied upon. (GB 24 & n.3). But every case the government cites involves a case-specific nexus. *See, e.g.*, *United States v. Watson*, 2023 WL 7300618, at *5 (E.D.N.Y. Nov. 6, 2023) (finding a case-specific nexus where the agent had knowledge of both the nature of the defendant's alleged criminal conduct and the use of electronic communications in furtherance of that conduct); *United States v. Pinto-Thomaz*, 352 F. Supp. 3d 287, 305 (S.D.N.Y. 2018) (holding probable cause existed where the affidavit detailed specific connections between email and iCloud accounts and the alleged crimes, including evidence of trading notifications and text message exchanges tied to the criminal scheme); *United States v. Gatto*, 313 F. Supp. 3d 551, 554 (S.D.N.Y. 2018) (upholding probable cause where FBI wiretaps recorded the defendant using the recovered cell phones for calls and messages directly related to the charged schemes); *United States v. Robinson*, 2018 WL 5928120, at *16 (E.D.N.Y. Nov. 13, 2018) (noting a case-specific nexus in cases where cell phones were discovered at or near the scene of the crime, suggesting their relevance to the investigation); *United States v. Hoey*, 2016 WL 270871, at *7 (S.D.N.Y. Jan. 21, 2016) (finding probable cause where the defendant was observed using a cell phone immediately before arrest, witnesses attested to the defendant's frequent use of cell phones for drug trafficking, and the defendant attempted to use the phone during his arrest); *United States v. Brown*, 676 F. Supp. 2d 220, 228 (S.D.N.Y. 2009) (finding a case-specific nexus where cell phones were located in the residence of the alleged criminal activity, supporting the "common sense notion" that evidence of the conspiracy, including contact information, could be found on the phones).

trafficking even absent direct evidence of drug transactions occurring there. GB 27. Yet this analogy is flawed for two key reasons.

First, the government overlooks *Riley*'s recognition that searching a cell phone often implicates greater privacy concerns than searching a home. Second, the government ignores that the cases it cites involve case-specific facts that establish a clear nexus between the home (or location) and the alleged drug trafficking activities.[13] Once again, the Fourth Amendment doctrine establishes that warrants may be issued only where case-specific facts are tied to the location of the criminal conduct.

The government also argues that the district court improperly applied a heightened standard of protection for cell phones, causing it to "eschew reasonable inferences" about whether Silva's phone might contain evidence of criminal conduct (GB 33). This claim

---

[13] *See, e.g.*, *United States v. Donald*, 417 F. App'x 41, 43 (2d Cir. 2011) (finding a case-specific nexus where officers observed the defendant's wife traveling from his residence to complete a narcotics transaction, combined with the scale of the defendant's drug distribution activities); *Velardi v. Walsh*, 40 F.3d 569, 574 (2d Cir. 1994) (upholding probable cause where evidence specifically linked the narcotics supplier to the residence described in the warrant, establishing a connection between the location and the drug trafficking activities).

misunderstands the district court's reasoning. The court did not impose a heightened standard; again, it applied the well-established Fourth Amendment requirement of a nexus between the item to be searched and the alleged crime.

The district court correctly noted that the warrant application lacked case-specific facts tying Silva's phone to his alleged criminal activity. Without evidence demonstrating such a connection—such as communications, location data, or observed use of the phone during the crime—the court rightly concluded that the warrant was unsupported by probable cause. This decision aligns with established precedent and underscores the constitutional requirement of particularity.

Finally, the government argues that an agent's training and experience provided a permissible basis for probable cause (GB 34). True enough, training and experience can inform probable cause determinations. Training and experience, however, cannot substitute for specific evidence about a particular case. Here, for instance, the warrant affidavit relied on boilerplate language about how cell phones are generally used to communicate, without offering any case-specific facts about how Silva or the Dub City gang used their phones in connection with the alleged crimes. By relying solely on generic

assertions, the government ignored the Fourth Amendment's requirement for individualized evidence—a requirement that does not ask too much to give license to search "the privacies of life." Thus, without case-specific evidence establishing a nexus, probable cause cannot rest solely on an agent's experience or generalized assumptions about cell phone use.

At bottom, the government's arguments fail to address the central constitutional deficiency in this case: the lack of a factual nexus between Silva's cell phone and the alleged criminal activity. The district court anchored its decision in established Fourth Amendment principles and appropriately rejected speculative inferences and boilerplate assertions. Upholding these constitutional protections is particularly critical in the digital age, where cell phones hold vast amounts of private information. Without a case-specific basis for probable cause, the warrant to search Silva's phone cannot be justified.

II. The good faith exception cannot excuse reliance on a warrant affidavit that fails to establish any nexus between a cell phone and an alleged crime.

The government's good faith argument suffers from the same fatal flaw as its probable cause analysis—it seeks to establish a principle so broad that it would render *Riley*'s warrant requirement a mere

formality in cases involving cell phones. Far from remaining the narrow exception originally intended in *United States v. Leon*, 468 U.S. 897 (1984), the good faith doctrine has become law enforcement's reflexive fallback whenever a warrant falls short of probable cause.[14]

This routine invocation of good faith threatens to swallow the exclusionary rule entirely, particularly in digital search cases where privacy interests are most acute and where, as here, the warrant application lacks any particularized showing of probable cause. When courts consistently excuse warrants based on generic assertions rather than specific facts, they risk transforming *Leon*'s limited exception into an automatic safety valve that undermines Fourth Amendment protections.

Leon acknowledged that the good faith doctrine is not a shield for every Fourth Amendment violation. It declined to excuse reliance on warrants "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." This is precisely the situation here. The affidavit fails to connect Silva's cell phone to the

---

[14] *See generally* Matthew Tokson & Michael Gentithes, *The Reality of the Good Faith Exception*, University of Utah College of Law Research Paper No. 546, 12 (April 10, 2023), https://ssrn.com/abstract=4414248.

crime and instead relies on a generic assumption that people use phones. While this might be true in the abstract, it does nothing to establish probable cause for searching this phone. *Leon*'s framework cannot support good faith reliance on a warrant, which, as here, lacks any connection to the facts of the case.

Thus, as the district court concluded, the warrant affidavit here relies on a boilerplate claim that people commonly use cell phones, without any case-specific facts establishing a nexus between the alleged criminal activity and the particular phone to be searched. This conclusory reasoning fails to satisfy the Fourth Amendment's requirement for particularity and falls outside the *Leon* exception.

Beyond falling outside of *Leon*, practical considerations and sound policy further counsel against extending the good faith exception to such conclusory warrants. For instance, when, as here, an officer presents a conclusory affidavit devoid of case-specific facts, the officer denies a magistrate judge the ability to exercise meaningful independent judgment, which is a key safeguard the Fourth Amendment requires. As NACDL and NYSACDL members—practicing defense attorneys on the front lines—we understand that judicial oversight is especially crucial for digital searches, where a single

warrant can authorize access to vast troves of intimate personal data. Allowing boilerplate language about cell phone use to substitute for actual probable cause reduces the magistrate's role to a rubber stamp, undermining the very purpose of the Fourth Amendment's warrant requirement.

The exclusionary rule's deterrent purpose also counsels against applying the good faith exception where, as here, an affidavit fails to establish even a minimal case-specific nexus to justify the search. This deficiency becomes particularly concerning in the digital age, where a single device contains "the privacies of life" in ways the Founders could never have imagined. Unlike physical searches constrained by walls and tangible boundaries, digital searches enable law enforcement to access vast personal data repositories with minimal effort. Officers who execute general warrants for digital searches can examine intimate details of a person's life far beyond any legitimate investigative scope. Given this unprecedented reach into personal privacy, Fourth Amendment protections demand more vigorous enforcement, not erosion through expansive good faith applications.

Excusing such a warrant would set a dangerous precedent that undermines the critical privacy protections recognized in *Riley*. *Riley*

emphasized that cell phones are unlike traditional objects of search because they contain an unparalleled breadth and depth of personal information. A warrant to search a phone must therefore meet the Fourth Amendment's exacting standards for particularity and probable cause. Allowing the government to justify a warrant based on vague, generic reasoning about cell phone use would gut *Riley*'s protections, transforming the warrant requirement into a hollow formality and opening the door to unchecked invasions of digital privacy.

Furthermore, excusing warrants based on mere generalizations about cell phone use would create perverse incentives for law enforcement. Officers would have little reason to develop actual probable cause when they can rely on boilerplate language about how "criminals use phones." This is particularly dangerous in the digital age, where a single overbroad warrant can give access to years of private communications, photos, location data, and intimate details of daily life.

Finally, the deficiencies in this case highlight why the good faith exception cannot apply to affidavits that reflect neglect rather than reasonable investigative effort. The good faith doctrine presupposes that officers have acted with diligence and care in preparing a warrant

affidavit. Here, however, Detective Boyer failed to articulate even the most basic connection between the cell phone and Silva's alleged crimes. Permitting reliance on such a warrant would normalize inattention and lower the constitutional standards for future searches, creating a cascading erosion of Fourth Amendment rights.

By declining to extend the good faith exception here, this Court can establish clear guardrails that protect both Fourth Amendment rights and legitimate law enforcement needs. Officers must understand that digital searches require actual probable cause, not mere assumptions about cell phone use. As the defenders of constitutional rights, NACDL and NYSACDL urge this Court to ensure that *Leon*'s good faith doctrine does not become a vehicle for gutting Fourth Amendment protections in the digital age.

CONCLUSION

As courts continue to grapple with applying Fourth Amendment doctrine to digital age searches, this case presents a clear choice: the Court can maintain meaningful constitutional protections by requiring case-specific probable cause for digital searches, or it can accept the government's invitation to reduce *Riley*'s warrant requirement to a mere formality. The Fourth Amendment's framers knew the dangers of

general warrants. Today, when a single cell phone can reveal more about a person's private life than the most exhaustive physical search of a home, those dangers are exponentially greater.

By affirming the district court's ruling, this Court will send an essential message: in our digital age, the Fourth Amendment's protections against general searches matter more, not less. Accordingly, and for the reasons argued, amici urge this Court to affirm the district court's decision to suppress the blue iPhone and its contents.

Dated: December 9, 2024

Respectfully submitted,

/s/*Adeel Bashir*

Adeel Bashir
Amicus Counsel
NACDL Amicus Curiae Committee
400 N. Tampa Street, Suite 2660
Tampa, FL 33609
(703) 835-3929
adeel_bashir@fd.org

Richard D. Willstatter
Vice Chair, NACDL's *Amicus Curiae* Committee for Second Circuit
Green & Willstatter, Attorneys at Law
200 Mamaroneck Avenue, Suite 605
White Plains, New York 10601
(914) 948-5656

Stephen N. Preziosi
Chair, *Amicus Curiae* Committee
New York State Association of Criminal Defense Lawyers
48 Wall Street, 11th Floor
New York, New York 10005
(212) 960-8267

CERTIFICATE OF COMPLIANCE

Under Fed. R. App. P. 32(g)(1), the undersigned hereby certifies that this brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and 32(a)(7)(B), exclusive of the exempted portions of the brief, as provided in Fed. R. App. P. 32(f), the brief contains 5,030 words.

Dated: December 9, 2024

Respectfully submitted,

/s/*Adeel Bashir*

Adeel Bashir
Amicus Counsel
NACDL Amicus Curiae Committee
400 N. Tampa Street, Suite 2660
Tampa, FL 33609
(703) 835-3929
adeel_bashir@fd.org

Richard D. Willstatter
Vice Chair, NACDL's *Amicus Curiae* Committee for Second Circuit
Green & Willstatter, Attorneys at Law
200 Mamaroneck Avenue, Suite 605
White Plains, New York 10601
(914) 948-5656

Stephen N. Preziosi
Chair, *Amicus Curiae* Committee
New York State Association of Criminal Defense Lawyers
48 Wall Street, 11th Floor
New York, New York 10005
(212) 960-8267