No. 23-469

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

JOHN HOLCOMB,

Defendant-Appellant.

On Appeal from the United States District Court
Western District of Washington at Seattle
District Court Case No. 2.21-cr-075-RSL
Hon. Robert S. Lasnik

BRIEF OF FOURTH AMENDMENT SCHOLARS AS *AMICI CURIAE* IN SUPPORT OF DEFENDANT-APPELLANT ON THE GOOD FAITH EXCEPTION ISSUE

David B. Owens, WSBA#53856
Counsel of Record
Rachel Nowlin-Sohl, WSBA#58661
Averill L. Aubrey*
Megan Haygood*
Kayleigh McNiel*
Michael C. Orehek*
CIVIL RIGHTS AND JUSTICE CLINIC
UNIVERSITY OF WASHINGTON
SCHOOL OF LAW P.O. Box 85110
Seattle, Washington 98145-1110
dbowens@uw.edu
*Law Student
Attorneys forAmici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Cases (Cont.) **Page(s)**

Statutes

Statutes (Cont.) **Page(s)**

Other Authorities

Other Authorities (Cont.) **Page(s)**

Other Authorities (Cont.) **Page(s)**

INTEREST OF AMICI CURIAE

Amici curiae are legal scholars who teach and write on Fourth Amendment law. We are the authors of an empirical, historical, and doctrinal study on the good faith exception.

Matthew Tokson is a Professor of Law at the S.J. Quinney College of Law. Professor Tokson graduated cum laude from Dartmouth College and with high honors from the University of Chicago Law School, where he was the Executive Articles Editor of the Law Review. He served as a law clerk to the Honorable Ruth Bader Ginsburg and the Honorable David H. Souter of the United States Supreme Court. Professor Tokson has also served as a fellow at the University of Chicago and as a senior litigation associate in the criminal investigations group of WilmerHale in Washington, D.C. His recent articles have been published or are forthcoming in the Harvard Law Review, the University of Chicago Law Review, the Michigan Law Review, and more. His article *Knowledge and Fourth Amendment Privacy* was discussed at oral argument in the Supreme Court case *Carpenter v. United States*.

Michael Gentithes is Associate Dean of Academic Affairs and Professor at the University of Akron School of Law. Dean Gentithes practiced as an assistant appellate defender in the Illinois Office of the State Appellate Defender, where he represented indigent clients in criminal appeals. Dean Gentithes's teaching and

research focus on criminal procedure, constitutional law, legal theory, and legal research and writing. He has published more than 20 articles in law reviews across the country. Dean Gentithes was elected Chair of the Criminal Procedure Section of the American Association of Law Schools in September of 2022.

We submit this brief in support of Defendant-Appellant because we have a keen interest in preventing the erosion of Fourth Amendment rights through the continued expansion of the good faith exception to the exclusionary rule.[1]

[1] No party, party's counsel, or person—other than *amici* and their counsel—authored any part or contributed money to fund preparation or submission of this brief. Counsel for both parties have provided blanket consent to the filing of briefs by amici curiae.

SUMMARY OF THE ARGUMENT

When the Fourth Amendment is violated by an unconstitutional search, the suppression of wrongfully obtained evidence (the exclusionary rule) is often the only viable remedy that might deter government overreach and provide some redress for the constitutional violation. Though the Supreme Court has long treated remedial mechanisms as separate from their underlying rights, *Wolf v. Colorado*, 338 U.S. 25 (1949), and while limited exceptions to the suppression requirement have existed for years, recent expansion of the "good faith exception" in the digital age imposes unprecedented threats to privacy and security.

A porous or expansive view of the good faith exception threatens to swallow the exclusionary rule entirely, undermining the Fourth Amendment rights of all people—whether guilty, innocent, or never accused of a crime. An ever-expanding version of the good faith exception, like the one endorsed by the district court below, means we are all more likely to have our digital data surveilled and to have no redress when that surveillance is unconstitutional.

This is no idle concern. Instead, as shown by our empirical study concerning its use, expansion of the good faith exception is pervasive and harmful to Fourth Amendment rights. If affirmed, the rationale of the court below would extend application of the good faith exception to the detriment of everyone's constitutional rights. This Court should reject such a rule.

ARGUMENT

I. THE GOOD FAITH EXCEPTION IS BEING INTERPRETED MORE EXPANSIVELY AND APPLIED MORE FREQUENTLY THAN EVER BEFORE, WITH ALARMING RESULTS.

The modern exclusionary rule dates to *Weeks v. United States*, 232 U.S. 383 (1914), in which the Court held that the Fourth Amendment barred the use of illegally seized evidence in a federal prosecution. *Mapp v. Ohio*, 367 U.S. 643 (1961), extended the exclusionary rule to state and local prosecutions. Though original understandings of the exclusionary rule suggested it was constituent of the underlying right itself, it is now established that the rule is not a "personal constitutional right" but rather a "judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect." *Calandra v. United States*, 414 U.S. 348, 348 (1974); *see also* David Gray, *A Spectacular Non-Sequitur: The Supreme Court's Contemporary Fourth Amendment Exclusionary Rule Jurisprudence*, 50 AM. CRIM. L. REV. 1, 14-21 (2013) (tracing the evolution of the exclusionary rule from its "principled roots" to the contemporary deterrence rationale).

The good faith exception to the exclusionary rule was first carved out by the Supreme Court in the 1984 case *United States v. Leon*, 468 U.S. 897 (1984). There, the Court admitted evidence obtained when several homes were searched pursuant to a warrant issued without probable cause. Following *Calandra*, the remedy of

exclusion was not required as the Court reasoned deterrence would not be possible when officers believed they were acting in good faith. *Id.* at 908-10. Soon after, the Court extended these rules by applying the good-faith exception to police reliance on statutes permitting administrative searches, even unconstitutional ones, *Illinois v. Krull*, 480 U.S. 340 (1987), and even for hypothetical reliance on later-overruled circuit precedent, *Davis v. United States*, 564 U.S. 229 (2011).

All along, the Court has made it clear it anticipated the good faith exception should apply to a small number of cases and under narrow circumstances. *See Leon*, 468 U.S. at 916 n.14 (doubting that magistrates would erroneously approve search warrants without probable cause very often); *Krull*, 480 U.S. 352 n.8 (predicting passage of surveillance laws of dubious constitutionality would be a rare event).

However, until our study, no empirical research had comprehensively examined how the exception has actually been used or tested whether the Court's expectation has played out in reality. It has not. Instead, the results of our empirical analysis demonstrate that, in practice, courts apply the good faith exception frequently and that frequency is increasing. *See generally* Matthew Tokson & Michael Gentithes, *The Reality of the Good Faith Exception*, University of Utah College of Law Research Paper No. 546, 12, https://ssrn.com/abstract=4414248 (April 10, 2023) ("our study" or "Study").

A. The Good Faith Exception Plays a Major Role in Fourth Amendment Litigation, and Its Use Is Expanding.

Our study reviewed every available judgment, published and unpublished, concerning a Fourth Amendment violation or a motion to suppress unlawfully obtained evidence in July 2015, July 2018, and July 2021. In those months, there were 5,531 cases involving the Fourth Amendment or motions to suppress. *Id.* at 12. Of these, 1,161 substantially addressed a Fourth Amendment suppression motion. *Id.* Our team traced whether the good faith exception was discussed and applied, which authority police had relied upon in each contested search (warrant, statute, precedent, or administrative error), and whether the court made a substantive ruling prior to using the exception. *Id.*

We found that the good faith exception was discussed in 18.4% of suppression cases, or about one out every six cases. *Id.* at 15. In 12.7% of cases—one eighth of all suppression cases, and over two thirds of the cases in which good faith was discussed—courts applied the good faith exception and admitted contested evidence. The exception's use increased overall after July 2015. *Id.* In July 2015, 14.5% of all suppression cases discussed the good faith exception, and 9.6% of cases found that the exception applied. *Id.* at 15. Those numbers rose to 20.9% and 15.8% in July 2018, a statistically significant increase, and remained similar in 2021, at 21.0% and 13.6%, respectively. *Id.* at 15-16.

Across all three years, the good faith exception was applied more in federal courts than state courts; 28.0% of federal suppression cases overall discussed the good faith exception, and 21.7% applied it to allow unlawfully obtained evidence to be used in court. *Id* at 17. In state courts, the good faith exception was discussed in only 9.3% of suppression cases and applied in 4.0%. *Id.*

We found that warrants were by far the most common basis for reliance cited in cases where courts applied the good faith exception, accounting for 78.2% of good faith cases. *Id.* at 19. The remaining searches relied on statutes (10.2%), interpretation of precedents (8.2%), or administrative errors (3.4%). *Id.*

We also found that in 29.9% of the cases where courts applied the good faith exception, they avoided ruling on whether the Fourth Amendment was violated. *Id.* at 20. This fact, and the remarkable prevalence of the good faith exception especially in federal court, raises serious concerns about current law and the incentives it creates, discussed below.

B. Increased Use of The Good Faith Exception Creates Perverse Incentives for Law Enforcement, Potentially Motivating Them to Violate People's Rights.

In the early good-faith-exception cases, like *Leon* and *Krull*, the Supreme Court presented the exception's guiding principle as the law enforcement incentives created (or not created) by particular applications of the exclusionary rule. For example, in *Krull*, officers had acted in direct reliance on a statute that,

while intrusive, was consistent with Supreme Court precedent, and which officers would reasonably believe to be valid. *See* 480 U.S. at 357. Accordingly, there was nothing to deter—police had acted as the Court would want and excluding evidence would not promote deterrence. *See* 468 U.S. at 909. This Court has articulated similar standards. *See, e.g., United States v. Elmore*, 917 F.3d 1068, 1078 (2019) ("[A]pplication of the exclusionary rule . . . would have no 'appreciable deterrent' effect and is thus unwarranted."); *United States v. Korte*, 918 F.3d 750, 759 (9th Cir. 2019) ("[O]ur decision accords with the exclusionary rule's limited purpose to deter future Fourth Amendment violations."); *United States v. Crews*, 502 F.3d 1130, 1136 (9th Cir. 2007) (Suppression "is unwarranted where there can be no deterrent effect.").

That rationale has fallen apart completely with modern applications of the good faith exception. Instead, as our empirical data show, if current Fourth Amendment doctrine provides any incentives to law enforcement, it encourages rather than discourages respect of civilian's constitutional rights. When courts construe what constitutes "good faith" too broadly, admitting evidence that should never have been collected, they not only fail to deter constitutional violations, but encourage law enforcement to err on the side of violation.

1. Allowing "Good Faith" Reliance on Inapplicable or Vague Statutory Law Incentivizes Bad Police Behavior.

One phenomenon examined as part of our study was a cascade of suppression rulings following the Supreme Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). There, the Court found a privacy interest in cell phone location data and required a warrant for its collection due to a person's legitimate expectation of privacy in the record of their physical movements. *Id.* at 2217. In reaching that conclusion, the Court reflected that it "is obligated . . . to ensure that the progress of science does not erode Fourth Amendment protections." *Id.* at 2223 (citation and quotation marks omitted). Indeed, the Supreme Court has emphasized that all courts have an obligation to ensure that constitutional rights are not eroded. *See, e.g.*, *Boyd v. United States*, 116 U.S. 616, 635 (1886) ("It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.").

Nonetheless, in the years since *Carpenter*, courts continued to routinely admit cell phone location evidence in criminal prosecutions, even where unlawfully obtained; the government needed only to cite a legal authority on which police hypothetically relied in collecting the data before *Carpenter* was decided. Study at 22-25; *see generally* Matthew Tokson, *The Aftermath of* Carpenter*: An*

Empirical Study of Fourth Amendment Law 2018–2021, 135 HARV. L. REV. 1790 (2022).

Because some circuits before *Carpenter* had found unwarranted cell phone tracking data to be constitutional, courts allowed good faith reliance on these then-binding precedents under *Davis*, 564 U.S. 229. Study at 27. In other circuits, though, law enforcement pointed to a statute from the early days of the consumer internet which had nothing to do with location tracking or cell phones at all. *Id.*

In 1986—at least a decade before basic cell phones were commonplace and over 20 years before the first iPhone was released in 2007—Congress passed the Stored Communications Act (SCA). *See, e.g.*, John Markoff, *Apple Introduces Innovative Cellphone*, N.Y. TIMES (Jan. 10. 2007). Under the SCA, law enforcement could obtain court orders with less than probable cause for "a record or other information pertaining to . . . a customer" of an electronic service provider. 18 U.S.C. § 2703(c)(1). When the law was passed, such information typically included non-content email metadata: lists of incoming and outgoing email addresses, account usage logs, and email headers without subject lines. Study at 27 (citing Orin S. Kerr, *A User's Guide to the S.C.A.*, 7 GEO. WASH. L. REV. 208 (2004)). After *Carpenter* held this provision unconstitutional as applied to cell phone location data, many circuit courts continued to admit such evidence. *See, e.g.*, *United States v. Korte*, 918 F.3d 750, 759 (9th Cir. 2019); *United States v.*

Castro-Aguirre, 983 F.3d 927, 935 (7th Cir. 2020); *United States v. Herron*, 762 F. App'x 25, 31 (2d Cir. 2019); *United States v. Goldstein*, 914 F.3d 200, 204 (3d Cir. 2019). Police, courts held, had relied on the SCA in good faith, despite legislative history (and common sense) indicating that Congress in 1986 clearly did not intend to weigh in on the constitutionality of cell phone location tracking. Study at 28 (citing M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1472 (2007)).

In the years before *Carpenter*, there were indications from the Supreme Court that this type of surveillance was unconstitutional. Most notable was the Court's decision in *United States v. Jones*, 565 U.S. 400 (2012), holding that police could not install a tracker on a suspect's personal vehicle without a warrant. Far from encouraging caution, however, signs that certain surveillance techniques violate the Fourth Amendment may have incentivized police to use them even more aggressively until the Courts explicitly outlawed them, collecting as much cell tracking evidence as possible under the shield of "good faith" before a warrant requirement was imposed.

As we explain in our study, the SCA can be read to allow many more invasive and likely unconstitutional surveillance practices:

> Imagine that the police encounter a new surveillance technology or practice, the use of which may be unconstitutional. Perhaps they want to obtain a suspect's direct messages on a new social media

> app, for example. Is there a statute that might permit the police to obtain direct messages without a warrant? Indeed there is. An SCA provision, 18 U.S.C. § 2703(a), permits the government to obtain the contents of communications stored for longer than 180 days with a subpoena, which is easy to obtain. Another provision, 18 U.S.C. § 2703(b), likely permits the government to obtain the contents of communications via subpoena even if they have not been stored for 180 days, as long as the communications have already been opened by the recipient and are not kept in "electronic storage" as defined in the Act.

Study at 29.

These loopholes are an obvious result of the obsolescence of a law drafted in the 1980s, unfit for addressing the massive amount of data now held on laptops and computers and even smartphones, watches, and other wearable devices. Yet the good faith exception incentivizes law enforcement to exploit "loopholes" like these. And there are many more to choose from. Numerous general-purpose statutes permit the collection of "records" that today could arguably include sensitive forms of personal data. *See* Study at 32-34. For example, the Pen Register Act permits the government to intercept virtually any form of non-content data transmitted as part of an electronic communication. 18 U.S.C. §§ 3122, 3127. This includes phone and email information but possibly also IP addresses, text message metadata, location data, URLs, and more. *See id.*; Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2120 (2009). Pursuant to 19 U.S.C. § 1509 the Customs Service may examine,

without a warrant, any record "which may be relevant to [a Customs] investigation." 19 U.S.C. § 1509. A provision of the Controlled Substances Act gives the DOJ sweeping authority to subpoena "any records" that are "relevant or material" to a drug investigation. 21 U.S.C. § 876. Notwithstanding the potential for constitutional challenge, in the remedial context law enforcement might also point to state statutes give investigators broad authority to seize records, requiring only that they be "relevant" to an ongoing investigation. Study at 33-34.

As argued in our empirical study, when courts signal that law enforcement can overstep the Constitution in reliance on such statutes, police may see little reason not to—and may instead see every reason to do so swiftly and aggressively. *Id.* at 29. Police are not typically well-versed in case law, Schwartz, *Qualified Immunity's Boldest Lie*, *supra*, at 664, and they can be motivated by an understanding that their actions will generally be immunized even if unlawful.[2] Upon encountering a new surveillance practice that has not yet been examined by courts, the government simply need to find an old statute that could arguably excuse its use, then use that practice to conduct as many searches as possible

[2] This sort of phenomenon has played out in the Fifth Amendment context with deliberate *Miranda* violations. *See, e.g.*, Lee Ross Crain, *The Legality of Deliberate* Miranda *Violations: How Two-Step National Security Interrogations Undermine* Miranda *and Destabilize Fifth Amendment* Protections, 112 MICH. L. REV. 453 (2013).

before courts prohibit it or impose warrant requirements. Retrospective statutory bases are advanced by prosecutors, who may be incentivized to secure convictions by justifying even the most invasive new forms of police surveillance (particularly given the fact that suppression motions only apply where there is *something* to be suppressed). *Id*.

2. Allowing Police to Rely on Vague Precedent Encourages Officers to Push Constitutional Boundaries.

In *Davis*, 564 U.S. at 241, the Supreme Court endorsed police reliance on binding circuit precedent that specifically authorizes a police practice, even one that is later found unconstitutional. *Davis* did not address the possibility that police might rely on ambiguous or vague precedents. However, in the years since *Davis* lower courts have allowed police officers to claim reliance on vague authorities often addressing other forms of surveillance that the ones now being used. *See, e.g., United States v. Asghedom*, 646 Fed. Appx. 830, 834 (11th Cir. 2016) (applying the good faith exception to admit evidence obtained from a GPS tracking device affixed to a vehicle on the basis of appellant precedent involving a different technology); *United States v. Gary*, 790 F.3d 704, 705, 709-10 (7th Cir. 2015) (ruling that police could rely in good faith on general principles from prior cases in conducting a search incident to arrest of a cell phone).

Some courts have gone even farther. Several district courts have suggested police could rely even on a *lack* of precedent to justify an illegal search. *United States v. Leon*, 856 F.Supp.2d 1188, 1193 (D. Hawai'i, Mar. 28, 2012) (citing the silence of most courts on a Fourth Amendment issue as a basis for the good faith exception); *United States v. Luna-Santillanes*, No. 11-20492 at *9 (E.D. Mich. Mar. 26, 2012) (supporting good faith reliance on "a widely-accepted practice in the police community that had not been held unconstitutional" in the jurisdiction). Others have held that police can rely on nonbinding precedents *from other circuits* to justify illegal surveillance techniques. *E.g. United States v. Gordon*, No. 11–CR–20752 (E.D. Mich. Mar. 4, 2013); *United States v. Rose*, No. 11–10062–NMG (D. Mass. Sept. 14, 2012); *United States v. Oladosu*, 887 F.Supp.2d 437, 442–48 (D.R.I. 2012).

All of this is problematic, given that police do not actually pay much attention to, and are not generally trained in, case-by-case updates in their own jurisdictions, let alone others. *See generally* Joanna Schwartz, *Qualified Immunity's Boldest Lie*, 88 U. CHI. L. REV. 605 (2021).

Like reliance on outdated statutes, reliance on vague precedent creates perverse incentives. Confidently protected behind a fictional shield of "good faith"—which does not rely on officer's *actual* good faith or absence thereof—police are permitted or arguably encouraged to aggressively employ dubious

surveillance techniques, then accelerate their use when signs suggest they may be unconstitutional.

3. "Good faith" Reliance on Erroneous Warrants Poses Its Own Perils.

The application of the good faith exceptions discussed so far illustrate the dangers of excusing aggressive reliance on outdated statutes and precedent. Failing to exclude evidence obtained based on faulty warrants is problematic as well. As our study found, warrants are the most common basis for invoking the good faith exception. Study at 19. Compared to statutes and precedent, the individualized nature of warrants could lead to arbitrary and inequitable correction of errors, to the detriment of marginalized communities. *See* Aziz Z. Huq, Judicial Independence and the Rationing of Constitutional Remedies, 65 DUKE L.J. 1, 20 (2015) (explaining the equity impacts of contemporary remedies doctrine that "makes it easier to challenge concentrated, top-down forms of lawmaking [than] dispersed, localized exercises of delegated authority").

The district court's decision in this case exemplifies overapplication of the good faith exception in the warrant context. When the officers aggressively interpreted a clearly overbroad warrant, they did exactly what the most extreme versions of the good faith exception encourage: they searched well beyond constitutional boundaries. Admitting evidence obtained under these circumstances

encourages officers to prepare *intentionally* broad warrants and contains no limiting principle to protect sensitive personal information. The district court's decision demonstrates that the good faith exception, applied loosely in a digital world, can effectively create general warrants, the odious "exploratory rummaging through a person's belongings" that inspired the Fourth Amendment in the first place. *Coolidge v. N.H.*, 403 U.S. 443 (1971).

The decision below also shows, once again, just how far the good faith exception has come since its creation. In *Leon*, the trial court had "recognize[d] the case was a close one, but . . . concluded the affidavit was [narrowly] insufficient to establish probable cause." 468 U.S. at 903. Here, the trial court conceded that police acted on what was essentially a general warrant ("in practice, the dominion and control clause superseded the limitations contained in the other warrant clauses and allowed officers to search defendant's entire computer") yet applied the good faith exception regardless. 1ER-14.

C. Expanded Use of the Good Faith Exception Stunts the Development of Constitutional Law

Another issue examined in our study is the threat the good faith exception poses to the elaboration of Fourth Amendment law. When courts admit contested evidence based on good faith, they sometimes do so without addressing the

constitutional validity of the search.[3] This risks a self-perpetuating cycle where constitutional rights around the most pressing issues concerning privacy in the technological age remain unclear simply because they have not been adjudicated.

The avoidance effect is not merely hypothetical. Our data show that in roughly 30% of cases applying the good faith exception, the court declined to resolve the underlying substantive Fourth Amendment issue. Study at 43. That is, in those cases, the court declined to create precedent to guide law enforcement to reduce future Fourth Amendment violations. Federal courts of appeals were nearly twice as likely as district courts to avoid substantive Fourth Amendment issues in cases where they applied the good faith exception. *Id.* at 22.

Overall, federal courts of appeals avoided substantive Fourth Amendment issues in 52.4% of cases applying the good faith exception. *Id.* at 43. This trend is troubling, and "[i]f every court confronted with a novel Fourth Amendment question were to skip directly to good faith, the government would be given carte blanche to violate constitutionally protected privacy rights, provided, of course, that a statute supposedly permits them to do so." *United States v. Warshak*, 631 F.3d 266, 282 n.13 (6th Cir. 2010). When courts of appeals decline to clarify the

[3] *United States v. Needham*, a case on which the district court relied heavily in its ruling, is one such case. 718 F.3d 1190, 1193 (9th Cir. 2013).

contours of Fourth Amendment rights, they are likely to remain ambiguous and prone to misinterpretation or abuse.

II. THE GOOD FAITH EXCEPTION IN THE CONTEXT OF DIGITAL DATA SEARCHES IS PARTICULARLY CORROSIVE TO CONSTITUTIONAL RIGHTS.

A. Reining in the Good Faith Exception in Digital Data Searches Is Uniquely Crucial Due to the Vast Private Information Accessible Through Digital Devices.

The immense amount of personal information stored on our devices can reveal nearly every detail about our lives. Access to our digital data means knowing where we go, what we buy, what entertainment we consume, and which news articles we read. The breadth of information readily available on a person's cell phone or computer far surpasses what could be garnered from a search of their home, car, or office. *Riley v. California*, 573 U.S. 373, 394 (2014); *United States v. Wilson*, 13 F.4th 961, 977 (9th Cir. 2021) (acknowledging the need to confine searches of digital material due to the "immense storage capacity" of modern technology); *United States v. Cano*, 934 F.3d 1002, 1015 (9th Cir. 2019) (explaining that a significant expectation of privacy exists regarding the vast and sensitive information on electronic devices). Social media and internet-based "cloud storage" accounts are even more extensive, often containing decades of emails, photos, videos, financial records, internet search history, and location data.

With the advent of smart speakers and virtual assistants, police can even listen to private conversations within our homes.[4]

Because of the sheer volume of information accessed on or through our personal devices, digital searches are far more invasive than traditional physical searches. *See United States v. Korte*, 918 F.3d 750, 756 (9th Cir. 2019) (explaining that cell phone searches are more invasive than placing a GPS device on a vehicle due to the "vast quantities of personal information" a cell phone holds); *United States v. Johnson*, 875 F.3d 1274 (9th Cir. 2017) (noting the acute privacy interests implicated in cell phone searches); *United States v. Payton*, 573 F.3d 859, 861–62 (9th Cir. 2009) (stating that computer searches are more intrusive than physical searches because of the vast and detailed private information they contain).

As investigators increasingly seek recordings from new "smart" technologies like Ring doorbells and Amazon's Alexa, the Fourth Amendment implications are only beginning to be realized. In the months after Amazon acquired Ring, it partnered with more than 1,300 law enforcement agencies to use footage from its home security cameras in criminal investigations.[5] And, until a

---

[4] *See e.g.* Mark Osborne, *Judge orders Amazon to hand over Echo recordings in double murder case*, ABC News (Nov. 9, 2018, 11:29 PM), https://abcnews.go.com/US/judge-orders-amazon-hand-echo-recordings-double-murder/story?id=59100572.

[5] Karen Hao, *The two-year fight to stop Amazon from selling face recognition to the police*, MIT Tech. Rev. (June 12, 2020),

court rules otherwise, police can gain access to recordings from private home security systems without a warrant or the owner's consent. Amazon handed over Ring doorbell video to police at least eleven times last year based only on "emergency requests" from law enforcement, providing the footage without permission from the owner or an order signed by a judge. [6]

This can be particularly problematic for those who live in or visit shared housing where multiple people might use or be recorded by the same devices. Customers at an Airbnb who sync their devices via Wi-Fi or are recorded on a Nest camera may have their private data or intimate moments snared in a later investigation.

Additionally, due to the interconnected nature of social media and the expansiveness of metadata, overly broad digital searches can capture the personal information of completely innocent third parties merely because of their

---

https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/. Amazon also partnered with police to pilot its "Rekognition" facial recognition technology, which presents its own universe of privacy concerns. Amazon paused police use of Rekognition in 2020 following pressure from shareholders and civil rights groups; however, the company could, at its discretion, move forward with keen law enforcement interest and little or no limitation under federal law. *Id.*

[6] Alfred Ng, *Amazon gave Ring videos to police without owners' permission*, Politico (Jul. 13, 2022, 6:00 AM), https://www.politico.com/news/2022/07/13/amazon-gave-ring-videos-to-police-without-owners-permission-00045513.

interactions with those who are the subject of a digital search. This concerning reality was highlighted in 2013 by Edward Snowden's revelation of the National Security Agency's ("NSA") warrantless dragnet that secretly collected the phone records of millions Americans as part of a global surveillance program.[7]

Though Snowden's disclosure of this information was unlawful, and we do not endorse his tactics, they did shed light on the staggering nature of government surveillance that occurs beyond court supervision (either under the Fourth Amendment or the Foreign Intelligence Surveillance Act (FISA)). Under the NSA program, telephone metadata including the phone numbers, timing, and location of all communications within the United States and between domestic and foreign callers was placed into a database that NSA officials could then search. *See United States v. Moalin*, 973 F.3d 977, 989 (9th Cir. 2020). In *Moalin*, this court found the bulk collection of metadata was illegal under FISA and likely violated the Fourth Amendment, noting that a large enough volume of metadata "absolutely tells you everything about somebody's life" even without the content of the communications. *Id* at 989-91 (citation omitted).

[7] Raphael Satter, *U.S. court: Mass surveillance program exposed by Snowden was illegal*, Reuters (Sep. 2, 2020, 10:21 PM), https://www.reuters.com/article/us-usa-nsa-spying-idUSKBN25T3CK/.

While *Moalin* made it clear that the NSA's bulk collection of Americans' phone records violated the Constitution, that does not necessarily mean such evidence cannot be used by the government, given a broad interpretation of the good-faith exception. Overbroad warrants raise the same concerns. As technology becomes more and more ubiquitous and covers an ever-increasing quantity of personal data, such searches are a growing threat to Fourth Amendment principles.

B. The Perverse Incentives of an Expansive Good Faith Exception Interact with Technological Advancement in Harmful Ways.

Under its broadest interpretation, because the good faith exclusion does not rely on a particular officer's actual good (or bad) faith, the doctrine motivates police to aggressively exploit loopholes and "[k]eep pushing until they tell you to stop, and then push somewhere else." Study at 36 (quoting Caleb Mason, *New Police Surveillance Technologies and the Good-Faith Exception: Warrantless GPS Tracker Evidence After* United States v. Jones, 13 NEV. L.J. 60, 71 (2012)).

Warrants for digital data are a particularly concerning place for courts to give police broad latitude, as these are far more prone to abuse than warrants for physical searches. For example, say the police have a warrant to search a garage for stolen property. The walls of the garage create an obvious boundary beyond which they may not search. They may not wander beyond the garage to seize old home videos stashed in the back of a bedroom closet or dig through photo albums

in the attic. In a digital search, however, as happened in this case, police may effectively do what they cannot in the real world, overstepping the bounds of their permitted search with just a few taps or clicks, because various types of sensitive information are stored in a single device or account.

While the Fourth Amendment promises the same protections in digital and physical searches, oversearching in violation of the Fourth Amendment is both easier and potentially much more consequential in the digital context. Searches of cell phones, for example, "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Riley*, 573 U.S. at 393. To ensure the same protections guaranteed in physical searches, law enforcement must use—and courts must require—additional care.

Without such safeguards, police can continue to apply archaic authorities—written before our modern, online lives could be imagined—to fundamentally novel circumstances. Expansive interpretations of general-purpose statutes, like overbroad interpretations of warrants, are likely to violate the Constitution, and genuine good faith on the part of law enforcement would mean employing them with caution. In *Jones*, *Carpenter*, and *Riley*, the Supreme Court recognized the need for additional protections regarding GPS trackers and cell phone data. *See Jones*, 565 U.S. at 411; *Carpenter*, 138 S. Ct. at 2221; *Riley*, 573 U.S. at 401 (2014). Over time, it will likely resolve more surveillance questions by requiring

warrants to search personal digital data. However, by virtue of the structure of our judicial system, each of these questions will be presented to lower courts first. Keeping the good faith exception narrow is one thing courts can and should do to ensure that the Fourth Amendment's safeguards remain faithful to its principles, regardless of technological advances.

III. THIS COURT CAN AND MUST REJECT EXPANSION OF THE GOOD FAITH EXCEPTION TO PRESERVE THE VALUE OF FOURTH AMENDMENT RIGHTS.

A. The Exclusionary Rule Is Often the Only Remedy Available for Fourth Amendment Violations,

The good faith exception, and the exclusionary rule it limits, are part of a remedial structure for Fourth Amendment violations that has been significantly weakened over the past four decades. Study at 40-42. The Fourth Amendment protects the "right of the people to be secure . . . against unreasonable searches and seizures"; one of its central motivating concerns was to prevent the government from using the fruits of an unreasonable search or seizure to support criminal charges. *Id.*

As a general matter, there are two primary remedies for Fourth Amendment violations: (1) the exclusion of evidence, and (2) a potential civil suit pursuant to 42 U.S.C. § 1983. As other commentators have pointed out, the availability of these remedies determines, as a practical matter, the actual value of the constitutional right beyond mere theory. *See* Pamela S. Karlan, *The Paradoxical*

Structure of Constitutional Litigation, 75 FORDHAM L. REV. 1913 (2007); David B. Owens, *Fourth Amendment Remedial Equilibration: A Comment on* Herring v. United States *and* Pearson v. Callahan, 62 STAN. L. REV. 563, 564 (2010).

Against this backdrop, criminal decisions addressing whether a suppression remedy should apply often point to the potential availability of a § 1983 remedy in a civil case as a justification for limiting that remedy. Pamela S. Karlan, *What's a Right Without a Remedy?,* Bos. Rev. (Mar. 1, 2012), https://www.bostonreview.net /articles/pamela-karlan-supreme-court-rights-legal-remedies; *see generally* Owens, *supra*. But in civil cases, the increasingly robust doctrine of qualified immunity serves to limit remedies for known constitutional violations unless they violate "clearly established law," even where Courts have no problem concluding the Constitution was violated. *See, e.g.*, *Safford Unified School Dist. No. 1 v. Redding*, 557 U.S. 364 (2009) (school officials' strip-search of middle schooler violated Fourth Amendment, but qualified immunity applied as law on strip-searches was not clearly established); *Wilson v. Layne*, 526 U.S. 603 (1999) (Fourth Amendment was violated when police brought media into arrestee's home, but qualified immunity applied as law was clearly established); *Anderson v. Creighton*, 483 U.S. 635 (1987) (search violated Fourth Amendment, but qualified immunity was warranted if a reasonable officer could have believed it did not); *Manriquez v. Ensley*, 46 F.4th 1124 (9th Cir. 2022) (officers conducted unconstitutional search

based on warrant that did not list place to be searched, but were entitled to qualified immunity as law was not clearly established). Part of the justification for this rule is the availability of a suppression remedy—the one already separately limited. *See, e.g.*, *Vega v. Tekoh*, 597 U.S. 134, 151 (2022).

As both suppression and § 1983 remedies are continually whittled down, there will often be no remedy whatsoever for a constitutional violation in either the criminal or civil context. Without any effective remedy for its violation, the Fourth Amendment itself becomes weakened, even if courts are only issuing a decision about remedy. Owens, *supra*, at 570-71. And, as we found, the lack of remedy can make citizens reluctant to even assert their rights. For example, criminal defendants are less inclined to litigate even flagrant Fourth Amendment violations when the probability of obtaining relief is slim. Study at 13.[8]

Most subjects of an unlawful search will never have the possibility of a § 1983 suit if their Fourth Amendment rights have been violated. Even putting aside qualified immunity, such claims frequently cannot proceed due to the criminal proceedings or a criminal conviction, *Heck v. Humphrey*, 512 U.S. 477

[8] As we tallied suppression cases for our study, we also noted one impact of the good faith exception that could not be reflected in the data: "the innumerable suppression motions that the exception discourages defendants from filing in the first place." Study at 2-3.

(1994), and any damages remedy would be so minimal (given a conviction) no attorney is likely to pursue it. *See generally* JOANNA SCHWARTZ, SHIELDED: HOW THE POLICE BECAME UNTOUCHABLE CH. 6 (2022) (describing obstacles to bringing § 1983 suits).

B. For the Exclusionary Rule to Be Meaningful, the Court Must Narrowly Construe Exceptions.

For law enforcement to truly act in good faith in its use of search and surveillance technologies, courts must give it a reason to do so. This means narrowly construing exceptions to protect a robust exclusionary rule.

In the area of warrants, the case at bar gives the Court a choice between maintaining the contours of the exclusionary rule and diminishing it substantially. It is critical that the Court not further erode Fourth Amendment rights by extending the good faith exception beyond its present limits in the Circuit.

Here, the district court misinterpreted binding caselaw to admit evidence from a clearly overbroad warrant because it was not "so lacking in indicia of probable cause as to render official belief in its existence unreasonable." ER18-19, quoting *Needham*, 718 F.3d at 1194. This was not the proper test. While a warrant's complete lack of probable cause is *sufficient* to justify suppression, it is not *necessary*: there are other ways a warrant can be (obviously) invalid. *See Leon*, 468 U.S. at 898-99 (listing a lack of "indicia of probable cause" as one of several

things that could make reliance on a warrant unreasonable).[9] Requiring an obvious lack of probable cause as the *sine qua non* for suppression of evidence obtained with a warrant would greatly expand the good faith exception. If the district court's reasoning on reconsideration is allowed to stand, it is hard to see how evidence obtained with an overbroad warrant could *ever* be suppressed. This could end exclusion for any overbroad or otherwise unconstitutional warrant, so long as it was not clearly "lacking indicia of probable cause." And with no consequences for overbreadth, law enforcement would have little reason to tailor warrants narrowly as the Constitution requires.

CONCLUSION

For the foregoing reasons, the Court should reverse the district court and decline to apply—and greatly expand—the good faith exception.

Dated this 20th day of November 2023.

/s/ David B. Owens
Counsel of Record for Amici Curiae

David B. Owens
Rachel Nowlin-Sohl
Averill L. Aubrey*
Megan Haygood*

[9] Even here, the district court originally suppressed evidence not because the warrant lacked probable cause but because it lacked particularity and was overbroad. 1ER35-40.

Kayleigh McNiel*
Michael C. Orehek*
CIVIL RIGHTS AND JUSTICE CLINIC
UNIVERSITY OF WASHINGTON
SCHOOL OF LAW P.O. Box 85110
Seattle, Washington 98145-1110
nowsohl@uw.edu
*Law Student
Attorneys for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on November 20, 2023, I electronically filed the foregoing with the Clerk of Court using the ECF system, which will electronically send notice to all counsel of record.

/s/ David B. Owens
Counsel of Record for Amici Curiae

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 23-469

I am the attorney or self-represented party.

This brief contains 6,469 **words,** including 0 words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - ☐ it is a joint brief submitted by separately represented parties.
  - ☐ a party or parties are filing a single brief in response to multiple briefs.
  - ☐ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated ____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature /s/David B. Owens **Date** 11/20/2023
*(use "*s/[typed name]*" to sign electronically-filed documents)*