No. 17-10230

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

BRYAN GILBERT HENDERSON,
Defendant-Appellant.

On Appeal from the United States District Court
for the Northern District of California

BRIEF *AMICI CURIAE* OF THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AND THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF APPELLANT'S PETITION FOR PANEL REHEARING AND REHEARING *EN BANC*

ANDREW CROCKER
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109
(415) 436-9333

Counsel for Amicus EFF

MICHAEL PRICE
Sr. Litigation Counsel, Fourth Amendment Center
National Association of Criminal Defense Lawyers
1660 L St. NW, 12th Floor
Washington, D.C. 20036
(202) 465-7615

DONALD M. FALK
Ninth Circuit Vice-Chair, NACDL Amicus Committee
Mayer Brown LLP
Two Palo Alto Square, Suite 300
Palo Alto, CA 94306
(650) 331-2000
dfalk@mayerbrown.com

Counsel for Amicus NACDL

TABLE OF CONTENTS

Table of Authorities ..... **ERROR! BOOKMARK NOT DEFINED.**

Interest of Amici Curiae 1

Introduction 2

Background 5

Argument 8

A. The Petition Presents A Constitutional Issue Of Exceptional Importance Because The Panel Decision Excuses "Systemic Negligence" In The Digital Age. 8

B. Rehearing Is Warranted To Ensure That Extra-Jurisdictional Warrants Comply with the Laws Where Evidence is Searched or Seized. 12

C. Rehearing Is Warranted To Clarify That The Good-Faith Exception Does Not Apply To Warrants Void For Lack of Jurisdiction Where The Agency Obtaining The Warrant Was Or Should Have Been Aware of The Defect. 15

Conclusion 18

TABLE OF AUTHORITIES

Page(s)

Cases

In re Application of U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone,
849 F. Supp. 2d 526 (D. Md. 2011) 14

Carpenter v. United States,
138 S. Ct. 2206 (2018) 1, 3, 14

Herring v. United States,
555 U.S. 135 (2009) ..... *passim*

Riley v. California,
134 S. Ct. 2473 (2014) 1, 8

In re Sealed Docket Sheet Associated with Malware Warrant Issued on July 22, 2013,
No. 1:16-cv-03029-JKB (D. Md. Aug. 29, 2016) 7, 14

Torres v. Oakland Scavenger Co.,
487 U.S. 312 (1988) 17

Tracey v. State,
152 So. 3d 504 (Fla. 2014) 14

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) (*en banc*) 1

United States v. Cottom,
2015 WL 9308226 (D. Neb. Dec. 22, 2015) 6

United States v. Davis,
564 U.S. 229 (2011) 13

United States v. Jones,
132 S. Ct. 945 (2012) 1

United States v. Krueger,
809 F.3d 1109 (10th Cir. 2015) 16

United States v. Laurita,
2016 WL 4179365 (D. Neb. Aug. 5, 2016) 6

United States v. Leon,
468 U.S. 897 (1984) 9, 11

United States v. Martinez,
696 F. Supp. 2d 1216 (D.N.M. 2010), *aff'd,* 643 F.3d 1292
(10th Cir. 2011) 12

United States v. McLamb,
880 F.3d (4th Cir. 2018) 6

United States v. Pierce,
2014 WL 5173035 6

United States v. Reibert,
2015 WL 366716 (D. Neb. Jan. 27, 2015) 6

United States v. Rios,
830 F.3d 403 (6th Cir. 2016), *cert. denied* 138 S. Ct. 2701 (2018) 14

United States v. Song Ja Cha,
597 F.3d 995 (9th Cir. 2010) 12

United States v. Tippens,
No. 16-05110-RJB (W.D. Wash. Nov. 30, 2016) 5

In re Warrant to Search a Target Computer at Premises Unknown,
958 F. Supp. 2d 753 (S.D. Tex. 2013) 10, 14

Constitution, Statutes, and Rules

U.S. Const., Am. IV ..... *passim*

28 U.S.C. § 636 16

28 U.S.C. § 2072(a) 16

Fed. R. App. 32(f) 19

Fed. R. App. P. 29(b) 2

Fed. R. Crim. P. 41 ..... *passim*

Fed. R. Crim. P. 41(b)(1) 11

Ninth Circuit Rule 29–2(a).....2

Ninth Circuit Rule 40-1(a) 19

Other Authorities

Nate Anderson, *FBI uses spyware to bust bomb threat hoaxster* Ars Technica, July 18, 2007, http://arstechnica.com/security/2007/07/fbi-uses-virus-to-bust-bomb-threat-hoaxster 6

Joseph Cox, *New Case Suggests the FBI Shared Data from Its Mass Hacking Campaign with the UK*, Motherboard (Feb. 10, 2016), https://motherboard.vice.com/en_us/article/3dabnw/new-case-suggests-the-fbi-shared-data-from-its-mass-hacking-campaign-with-the-uk 6

Joseph Cox. *Unsealed Court Docs Show FBI Used Malware Like 'A Grenade'*, Motherboard, Nov. 7, 2016, http://motherboard.vice.com/read/unsealed-court-docs-show-fbi-used-malware-likea-grenade;.....7

Fed. Bureau of Investigation, News, *'Playpen' Creator Sentenced to 30 Years: Dark Web 'Hidden Service' Case Spawned Hundreds of Child Porn Investigations* (May 5, 2017), *available at* https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years 10

Kay Levine et. al., *Evidence Laundering in A Post-Herring World*, 106 J. Crim. L. & Criminology 627, 640–41 (2016).....9

Memorandum, Department of Justice to Advisory Committee on Criminal Rules (Sept. 18, 2013), *in* Advisory Committee on Criminal Rules, Agenda Book April 7-8, 2014, at 171-175 (2014), *available at* http://www.uscourts.gov/sites/default/files/fr_import/CR2014-04.pdf.....11

Ellen Nakashima, *This is how the government is catching people who use child porn sites*, Wash. Post, Jan. 21, 2016.....7

Kevin Poulsen, *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers For Years*, Wired, April 16, 2009, https://www.wired.com/2009/04/fbi-spyware-pro 6

Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired, Sept. 13, 2013, https://www.wired.com/2013/09/freedom-hosting-fbi 7

Kevin Poulsen, *Visit the Wrong Website, And The FBI Could End Up In Your Computer*, Wired, Aug. 5, 2014, http://www.wired.com/2014/08/operation_torpedo 6

U.S. Dep't. of Justice, Office of Legal Education, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 84-85 (2009), *available at* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf 10-11

INTEREST OF *AMICI CURIAE*

The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct.[1] 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 bar association that encompasses all segments of the criminal defense profession. The Association promotes a fair, rational and humane criminal justice system that upholds fundamental constitutional rights. NACDL has a particular interest in cases that involve surveillance technologies and programs that pose new challenges to personal privacy. The NACDL Fourth Amendment Center offers training and direct assistance to defense lawyers handling such cases in order to help safeguard constitutional rights in the digital age. NACDL has filed numerous amicus briefs in this Court and the Supreme Court on issues involving digital privacy rights, including: *Carpenter v. United States,* 138 S. Ct. 2206 (2018); *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); and *United States v. Cotterman*, 709 F.3d 952, 956 (9th Cir. 2013) (*en banc*).

[1] No party's counsel authored this brief in whole or in part, no party or party's counsel contributed money that was intended to fund preparing or submitting the brief, and no person other than the *amici curiae*, their members, or their counsel, contributed money that was intended to fund preparing or submitting the brief.

The Electronic Frontier Foundation (EFF) is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the digital world since 1990. With over 38,000 active donors, EFF represents technology users' interests in court cases and policy debates involving the Fourth Amendment, technology, and new surveillance techniques.

This brief is submitted under the authority of Federal Rule of Appellate Procedure 29(b) and Ninth Circuit Rule 29–2(a).

All parties have consented to the filing of this brief.

INTRODUCTION

This case should be reheard because it presents a question of exceptional importance to the limits on government intrusion into private matters in the digital age. The panel recognized that the nationwide warrant here exceeded the power of the magistrate judge who issued it. The warrant was part of a nationwide investigatory program which, as implemented here, represented a calculated risk by the government that should be subject to the exclusionary rule.

Yet the panel misapplied the good-faith exception to excuse the government's reliance on a warrant that was not and could not be valid when used against the defendant. That ruling eliminates the government's incentives to comply with the Fourth Amendment's warrant requirement for the broadest investigations, an error with significant repercussions now that almost everyone routinely engages in multi-state electronic communications.

The exclusionary rule cannot adequately deter government overreaching in the digital age if the good-faith doctrine insulates government mistakes of law in cases like this one. The panel decision would permit the government to engage in "systemic negligence" without consequence (*Herring v. United States*, 555 U.S. 135, 144 (2009)), evading the laws of other jurisdictions, and prompting forum-shopping for the weakest application of privacy rights in online investigations.

The Supreme Court has repeatedly stressed that Fourth Amendment rules "must take account of more sophisticated systems" of surveillance and search made possible by cutting-edge technology. *Carpenter v. United States,* 138 S. Ct. 2206, 2218-19 (2018). (quoting *Kyllo v. United States* 533 U.S. 27, 36 (2001)). As the digital age extends the reach of both law enforcement and criminal activity, the temptation to evade jurisdictional and other limits in the name of convenience and efficiency may prove too great for law enforcement to resist, as it did here. Nationwide surveillance initiatives, like the sophisticated digital surveillance tool at issue here, will proliferate as criminal activity continues to migrate to cyberspace. This Court should ensure that the exclusionary rule enforces the limits on government power that protect citizens' constitutional rights to be free of unlawful government intrusion into their homes and affairs.

In addition to the petition's arguments, three considerations underscore the importance of the issue and its suitability for rehearing or rehearing *en banc*.

First, this case involves a coordinated, national investigation using a sophisticated digital surveillance tool called "Network Investigative Techniques" ("NIT"). The violation here does not involve an executing officer's isolated mistake of fact, but a mistake of law, multiplied across jurisdictions throughout the nation. In multi-jurisdictional online investigations, the risk of "systemic negligence" is significant, so that the good-faith inquiry should encompass the government's actions in obtaining a warrant. Focusing solely on the agent responsible for executing the warrant risks nullifying the exclusionary rule in online investigations that begin in a different jurisdiction.

Second, the panel decision allows the government to evade its obligation to comply with the law wherever it operates. Prosecutors could seek authorization for highly invasive surveillance from the nation's most permissive venue, and claim authority for agents even in jurisdictions that might prohibit surveillance of that kind. The good-faith doctrine does not and should not provide such a sweeping safe harbor. Rehearing is warranted to reinforce the government's duty to comply with the rules in every jurisdiction where a warrant is executed. That duty is especially important now that Rule 41 has been amended, at the Justice Department's request, to permit magistrate judges to issue cross-jurisdictional NIT warrants.

Third, the use of warrants that are void for want of jurisdiction is exactly the type of intrusion that should be restrained. A warrant that is void *ab initio* is no warrant at

all. Its execution cannot be a matter of good faith when it was obtained as a matter of policy designed to substitute government convenience for individual liberty.

The case should be reheard and the judgment reversed.

BACKGROUND

This case, like hundreds of others, stems from the FBI's investigation of "Playpen," a website hosting child pornography.[2] The FBI seized the servers hosting Playpen in January 2015 and assumed the role of website administrator.[3] For nearly two weeks , the FBI operated the site and served visitors with malware it termed a "Network Investigative Technique" or NIT, which identified their computers for further investigation and prosecution. Slip Op. 5–6.

The investigation targeted a very large number of suspects. Playpen had at least 150,000 registered users, and the FBI used the NIT to hack into "approximately nine thousand" computers across the country and around the world.[4]

The highly coordinated investigation was national (and international) in scope. "Before applying for the NIT warrant in" the Playpen investigation, "the FBI consulted with attorneys at the Department of Justice's Child Exploitation and Obscenity Section

---

[2] *See* ER II 72–106 (NIT warrant application and affidavit and attachments).

[3] *See* ER II 97-98, ¶¶ 28, 30.

[4] *See* Order on Defendants' Motion to Dismiss Indictment at 5, 12, *United States v. Tippens*, No. 16-05110-RJB (W.D. Wash. Nov. 30, 2016) (ECF No. 106).

as well as the" the FBI's Remote Operations Unit (ROU). *United States v. McLamb*, 880 F.3d, 685, 689 (4th Cir. 2018). After it identified the targeted computers, the FBI apparently shared information with international law enforcement partners.[5]

The government has used remotely installed malware to identify target computers over the Internet since at least 2002.[6] The NIT was developed by the agents and contractors at the FBI's Remote Operations Unit. *United States v. Cottom*, 2015 WL 9308226, at *2-3 (D. Neb. Dec. 22, 2015).

The FBI has repeatedly used NITs to target visitors to "Dark Web" sites. As part of "Operation Torpedo" in November 2012, the FBI seized three Dark Web sites that hosted child pornography, operated the sites for several weeks, and deployed three court-authorized NITs—one per site—to obtain IP addresses for at least 25 visitors.[7] And in the "Freedom Hosting" sting in July 2013, the FBI seized a group of servers

---

[5] Joseph Cox, *New Case Suggests the FBI Shared Data from Its Mass Hacking Campaign with the UK*, Motherboard (Feb. 10, 2016), https://motherboard.vice.com/en_us/article/3dabnw/new-case-suggests-the-fbi-shared-data-from-its-mass-hacking-campaign-with-the-uk.

[6] Nate Anderson, *FBI uses spyware to bust bomb threat hoaxster*, Ars Technica, July 18, 2007, http://arstechnica.com/security/2007/07/fbi-uses-virus-to-bust-bomb-threat-hoaxster; Kevin Poulsen, *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers For Years*, Wired, April 16, 2009, https://www.wired.com/2009/04/fbi-spyware-pro.

[7] Kevin Poulsen, *Visit the Wrong Website, And the FBI Could End Up In Your Computer*, Wired, Aug. 5, 2014, http://www.wired.com/2014/08/operation_torpedo ; *see also United States v. Laurita*, 2016 WL 4179365, at *3 (D. Neb. Aug. 5, 2016); *Cottom*, 2015 WL 9308226, at *8; *United States v. Reibert*, 2015 WL 366716, at *7 (D. Neb. Jan. 27, 2015); *United States v. Pierce*, 2014 WL 5173035, at *6 (D. Neb. Oct. 14, 2014).

that hosted Dark Web sites—including some containing child pornography. Among the targets was an email service known as TorMail, which was "used by a range of people, from criminals to dissidents and journalists."[8] The Freedom Hosting warrant and application revealed that the FBI had sought to hack more than 300 specific users across 23 separate websites.[9]

DOJ surely expected the NIT warrant obtained in Virginia to seed prosecutions around the country. Nearly 100 jurisdictions across the country have felt the fallout of the Playpen investigation, 82 of which also found a violation of Rule 41. *See* Pet. 9, n3. And DOJ surely anticipated those rulings, as it led the government's efforts to amend Rule 41 while it continued to enforce NIT-based warrants. *Id.* at 11-12.

---

[8] Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired, Sept. 13, 2013, https://www.wired.com/2013/09/freedom-hosting-fbi [hereinafter Poulsen, *FBI Admits*]; *see also* Ellen Nakashima, *This is how the government is catching people who use child porn sites*, Wash. Post, Jan. 21, 2016, http://wpo.st/_lRh1

[9] Poulsen, *FBI Admits*, *supra*; Joseph Cox, *Unsealed Court Docs Show FBI Used Malware Like 'A Grenade'*, Motherboard, Nov. 7, 2016, http://motherboard.vice.com/read/unsealed-court-docs-show-fbi-used-malware-likea-grenade; *see also In re Sealed Docket Sheet Associated with Malware Warrant Issued on July 22, 2013*, No. 1:16-cv-03029-JKB (D. Md. Aug. 29, 2016).

ARGUMENT

A. The Petition Presents A Constitutional Issue Of Exceptional Importance Because The Panel Decision Excuses "Systemic Negligence" In The Digital Age.

The good faith doctrine is not intended to excuse "recurring or systemic negligence." *Herring*, 555 U.S. at 144. But that is what the panel did here, focusing on the last link in the chain—one "executing agent"—rather than the coordinated course of government conduct responsible for the error. Slip Op. 21. In the digital age, this view misses the forest for the trees, insulating the most culpable government actors from accountability by severely limiting the exclusionary rule. The correct resolution of these cutting-edge constitutional issues merits rehearing.

This is not an errant warrant check or other one-off error. *Cf. Herring*, 555 U.S. at 137-38. Rather, this case involves an international digital dragnet run by the FBI and DOJ. The surveillance technology in the NIT deployed purpose-built malware on unknown computers around the world. The calculated use of this invasive new tactic, operating without geographic limits, underscores why the good faith doctrine should not apply. To paraphrase Justice Roberts, comparing a warrant check to a NIT is "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley v. California*, 134 S. Ct. 2473, 2488 (2014). When taken as a whole, the government's actions amount to the "systemic negligence" with respect to warrant requirements that *Herring* called out.

The panel reached its contrary conclusion because it erroneously focused on the behavior of one "executing agent" instead of considering the entire course of the investigation. Slip Op. 21. But the Supreme Court has repeatedly warned against such tunnel vision, explaining that reasonableness is a question of collective knowledge. The panel should have "consider[ed] the objective reasonableness, not only of the officers who eventually executed a warrant, but also of the officers who originally obtained it or who provided information material to the probable-cause determination." *Herring*, 555 U.S. at 140 (quoting *United States v. Leon*, 468 U.S. 897, 923 n.24 (1984)). The *Leon* Court explicitly cautioned against "too narrowly" reading its references to a single "officer," warning that the government could not obtain a void warrant "and then rely on colleagues who are ignorant of the circumstances under which the warrant was obtained to conduct the search." 468 U.S. at 923 n.24; *see also* Kay Levine et. al., *Evidence Laundering in A Post-Herring World*, 106 J. Crim. L. & Criminology 627, 640–41 (2016) (the "conduct of *all* of the police officers involved should come under scrutiny" lest a more cursory approach "permit officers to use their deliberately ignorant colleagues to do what they themselves cannot do.").

Law enforcement efforts to police the internet are collaborative endeavors, and the Playpen operation was no different. The FBI devised a strategy with DOJ to take over a child pornography website in order to install malware on any computer that attempted to log into it. From the outset, the plan was to conduct a global investigation

that would yield multiple prosecutions by local authorities around the country. Indeed, the FBI touts that, as of May 2017, the operation had "sent more than 1,000 leads" to field offices around the country, yielding "at least" 350 domestic arrests.[10] The government reportedly shared "thousands more" leads with law enforcement authorities abroad.[11]

Yet DOJ deliberately chose the Eastern District of Virginia as the launchpad for its multi-jurisdictional investigation. The DOJ did not obtain additional warrants in other jurisdictions, as its own policy required to ensure compliance with Rule 41. *See* U.S. Dep't. of Justice, Office of Legal Education, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 84-85 (2009) ("DOJ Manual").[12] DOJ likely would have failed in its quest. The Southern District of Texas had already found a similar NIT unlawful under Rule 41. *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) ("*Unknown Computer Warrant*"). That court recognized that a NIT search "takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name," and held that, because "the current location of the Target Computer [wa]s unknown[,] … the

[10] Fed. Bureau of Investigation, News, *'Playpen' Creator Sentenced to 30 Years: Dark Web 'Hidden Service' Case Spawned Hundreds of Child Porn Investigations*, (May 5, 2017), *available at* https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years.

[11] *Id.*

[12] *Available at* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

Government's application cannot satisfy the territorial limits of Rule 41(b)(1)." *Id.* So the government tried its luck in Virginia, knowing from prior experience that, once an NIT is approved, rain falls on more than one roof.

DOJ knew its position was shaky. *See* DOJ Manual at 84 ("A territorial limit on searches of computer data poses problems for law enforcement…"). It accordingly proposed a change to Rule 41 more than a year before installing the NIT in this case. *See* Memorandum, Department of Justice to Advisory Committee on Criminal Rules (Sept. 18, 2013), *in* Advisory Committee on Criminal Rules, Agenda Book April 7-8, 2014, at 171-175 (2014).[13]

Had the Virginia court refused the NIT warrant, the government could have worked its way through every state in the Union until it obtained authorization. Under the panel's rationale, that single authorization would shield all derivative prosecutions anywhere in the country from the exclusionary rule, so long as local investigators could claim ignorance of the warrant's invalidity.

But that is the forbidden "rel[iance] on colleagues who are ignorant of the circumstances under which the [initial] warrant was obtained." *Leon*, 468 U.S. at 923 n.24. And this Court has recognized that the exclusionary rule is properly confined to "isolated police negligence," and "does not bar suppression here because the police the

[13] *Available at* http://www.uscourts.gov/sites/default/files/fr_import/CR2014-04.pdf.

police conduct was deliberate, culpable, and systemic." *United States v. Song Ja Cha*, 597 F.3d 995, 1004 (9th Cir. 2010); *United States v. Martinez*, 696 F. Supp. 2d 1216, 1260 (D.N.M. 2010) (finding "systemic negligence" where "misapplication of the exigent-circumstances standard is recurring and not limited to the officers involved in [the] case"), *aff'd,* 643 F.3d 1292 (10th Cir. 2011).

In an age when digital dragnets occur with increasing frequency, courts should not equate expansive government hacking with an errant warrant check. The panel's excessively narrowed analysis would permit the government to commit egregious misconduct in the jurisdiction where it obtains a warrant, yet still use the resulting evidence in every other jurisdiction.

If not reheard, the panel decision's erroneous application of the good-faith doctrine would dilute the constitutional protections of the warrant process in contemporary online investigations by making it practically impossible for criminal defendants to suppress evidence obtained by invalid cross-jurisdictional warrants. DOJ should not be rewarded for forum-shopping, a concern heightened by DOJ's successful effort to amend Rule 41.

B. Rehearing Is Warranted To Ensure That Extra-Jurisdictional Warrants Comply with the Laws Where Evidence is Searched or Seized.

Rehearing is warranted for the additional reason that the panel decision would trigger a race to the bottom on privacy rights. It would reward government forum-shopping for the weakest privacy jurisprudence by imposing that standard on any

affected investigative target nationwide. The good faith exception cannot function within its proper limits unless the government follows the law of each jurisdiction in which it searches or seizes property. "Responsible law-enforcement officers will take care to learn 'what is required of them' under Fourth Amendment precedent and will conform their conduct to these rules." *United States v. Davis,* 564 U.S. 229, 241 (2011) (quoting *United States v. Hudson*, 547 U.S. 586, 599 (2006)). For example, the good-faith exception applies when officers conduct a search in reasonable reliance on binding precedent that is subsequently overruled. Because they have "take[n] care" to learn the laws of their jurisdiction, "all that exclusion would deter … is conscientious police work." *Id.*

But the test for good faith should be more stringent when government agents knowingly seek a warrant that may reach throughout the country, like the NIT warrant here. In that instance, the government must assume the risk that its inherently invasive activity may not be approved by every federal jurisdiction. If agents collectively try to follow the rules of only the issuing jurisdiction, they are not doing "what is required" of them under the Fourth Amendment. Instead, to qualify for the good-faith exception, they must learn and follow the rules of any jurisdiction where they conduct a search.

The panel decision lets the government off the hook with no evidentiary consequences. The panel ignored evidence that, when they sought the NIT warrant, the FBI and DOJ were aware that the Southern District of Texas had held a similar warrant

invalid. *See* Pet. 12 (citing *Unknown Computer Warrant*, 958 F. Supp. 2d 753). And because not all courts—only an overwhelming majority—subsequently found that the warrant violated Rule 41, the panel concluded that the government could not have known the warrant was invalid. Slip Op. 20.

The application of the good-faith exception to national, roving warrants based on the law of just one jurisdiction warrants this Court's close attention. The different jurisdictions affected by cross-jurisdictional warrants often have different privacy rules.

For example, NITs can be programmed to calculate the device's location in real time. *See Unknown Computer Warrant*, 958 F. Supp. 2d at 755 (denying warrant application to use NIT to do this). Although the Supreme Court recently held that *historical* location tracking is a search, it declined to rule on *real-time* location tracking. *See Carpenter,* 138 S. Ct. at 2220. And the lower courts are divided on that issue. *Compare Tracey v. State*, 152 So. 3d 504, 526 (Fla. 2014) (Fourth Amendment requires warrant for real-time tracking), and *In re Application of U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone*, 849 F. Supp. 2d 526, 583 (D. Md. 2011) (same), *with United States v. Rios*, 830 F.3d 403, 428 (6th Cir. 2016), *cert. denied* 138 S. Ct. 2701 (2018) (no warrant required for real-time cell tracking). Under the panel's rule, the good faith exception could prevent exclusion of real-time tracking evidence gained from a NIT warrant issued in the Sixth Circuit (where *Rios* might authorize its use) even if devices

were tracked without an additional warrant in Florida or Maryland, where that use of a NIT might well be prohibited.

The Court should not stretch the good-faith doctrine so that a single nationwide warrant may effectively override the Fourth Amendment jurisprudence of the jurisdictions where evidence is actually seized. That rule could result in a *de facto* national domestic surveillance court with the most permissive Fourth Amendment requirements, the actions of which could insulate the government from the consequences of Fourth Amendment violations occurring in other jurisdictions and used to bolster prosecutions there.

C. Rehearing Is Warranted To Clarify That The Good-Faith Exception Does Not Apply To Warrants Void For Lack of Jurisdiction Where The Agency Obtaining The Warrant Was Or Should Have Been Aware of The Defect.

Rehearing is warranted for the additional reason that the good faith exception does not apply to a warrant that is void *ab initio*—one that wasn't and never could have been valid. The exception's purpose is to ensure that the exclusionary rule applies only where "police conduct [is] sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid to the justice system." *Herring*, 555 U.S. at 144.

The government took on a calculated risk by seeking a nationwide warrant that it knew likely exceeded the magistrate judge's jurisdiction. It is axiomatic that a judicial act taken without jurisdiction is a nullity. As the panel recognized, "[f]ederal magistrate

judges are creatures of statute." Slip Op. 12 (internal quotation marks omitted). They accordingly have no power beyond that granted by 28 U.S.C. § 636. And the territorial limits on their power to issue warrants are "obvious[]" on the face of the statute and of Rule 41 as it then existed. *United States v. Krueger*, 809 F.3d 1109, 1113 (10th Cir. 2015). Magistrate judges may act only within their own district, at other places "where that court may function, and elsewhere as authorized by law." 28 U.S.C. § 636(a).

Section 636 unquestionably does not give magistrate judges jurisdiction to issue warrants that reach as far as the NIT warrant did here. Nor did Rule 41 purport to provide that jurisdiction.[14] As applied to Henderson in California, the warrant here was "no warrant at all when looking to the statutes of the United States." *Krueger*, 809 F.3d at 1118 (Gorsuch, J., concurring in the judgment). The panel wondered "how an executing agent ought to have known that the NIT warrant was void," Slip Op. 21, but the better question is what authority—what source of positive law—would have led an agent reasonably to believe that a national warrant could be valid. Surely it was not Section 636.

When a warrant is void *ab* initio, especially for lack of jurisdiction, the conduct to be evaluated is that of the officer or agency that procured the warrant, not the officer

[14] Whether a Federal Rule *could* provide jurisdiction beyond that enumerated in Section 636—whether a Rule satisfies the statute's "authorized by law" provision—in light of the Rules Enabling Act's prohibition on using the Rules to alter substantive rights (28 U.S.C. § 2072(a)) is a live question, but not presented here. *See Krueger*, 809 F.3d at 1120-21 (Gorsuch, J., concurring in the judgment).

in another jurisdiction who ultimately enforced it. Otherwise, even blatantly unlawful conduct at the highest levels of government may leave citizens unprotected by the Fourth Amendment.

The conduct of the DOJ and FBI here in obtaining a warrant beyond the power of the issuing judicial officer meets the criteria of deliberateness and culpability reiterated in *Herring*, 555 U.S. at 144. The calculated effort to obtain what effectively is a nationwide warrant from a territorially limited magistrate judge was no innocent mistake. As explained above (at pp. 5-6; 9-10), the NIT program is approved and run by high-ranking officials at the federal agencies. And those agencies were aware that, under current law, the program could not turn on what are effectively nationwide warrants when the issuing officers are magistrate judges. As soon as they began to implement the program, DOJ sought, and ultimately obtained, an amendment to Rule 41 that purported to give magistrate judges this power.

Culpability is equally clear. What amount to knowingly fake warrants render the warrant protections of the Fourth Amendment a nullity. There is no question that the agencies here could have sought valid warrants. But they treated constitutional and statutory limits as an inconvenience, and jurisdictional limits as irrelevant. Violations of a jurisdictional limitation are never harmless. *See Torres v. Oakland Scavenger Co.*, 487 U.S. 312, 317 n.3 (1988). The extra-jurisdictional warrant here, and others like it, undermine core protections against unlawful searches and seizures.

CONCLUSION

The petition should be granted and the judgment reversed.

Respectfully submitted.

December 17, 2018

s/Donald M. Falk

Donald M. Falk

ANDREW CROCKER
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109
(415) 436-9333

Counsel for Amicus EFF

MICHAEL PRICE
Sr. Litigation Counsel, Fourth Amendment Center
National Association of Criminal Defense Lawyers
1660 L St. NW, 12th Floor
Washington, D.C. 20036
(202) 465-7615

DONALD M. FALK
Ninth Circuit Vice-Chair, NACDL Amicus Committee
Mayer Brown LLP
Two Palo Alto Square, Suite 300
Palo Alto, CA 94306
(650) 331-2000
dfalk@mayerbrown.com

Counsel for Amicus NACDL

CERTIFICATE OF COMPLIANCE

Pursuant to Federal Rule of Appellate Procedure 32(g)(1), I certify as follows:

1. This brief complies with the type-volume limitation in Ninth Circuit Rule 40-1(a) because this brief contains 4,163 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it was prepared in a proportionally spaced typeface in Microsoft Word 2016 with 14 point Garamond font.

December 17, 2018

Respectfully submitted.

s/Donald M. Falk

Donald M. Falk

CERTIFICATE OF SERVICE

I certify that I electronically filed this brief with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on December 17, 2018.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Respectfully submitted,

December 17, 2018 s/