CARPE DATA

A Magistrate Judge's Guide to Electronic-Information Requests in Criminal Cases

Fourth Edition
2025

ANDREW G. SCHOPLER

WENDELL M. ALFORD

MAGISTRATE JUDGES EXECUTIVE BOARD

UNITED STATES COURTS FOR THE NINTH CIRCUIT

TABLE OF CONTENTS

ACKNOWLEDGMENTS i

CHAPTER ONE:
Pen Registers/Trap-and-Trace Devices
[18 U.S.C. §§ 3121–3127] 1

A. Cell-Site Simulators 2

CHAPTER TWO:
Subscriber Records and Stored Communications
[18 U.S.C. §§ 2701–2713] 4

A. Subscriber Information 5
B. Location Data 6
C. Content of Electronic Communications 8

CHAPTER THREE:
Tracking Warrants
[Fed. R. Crim. P. 41] 10

CHAPTER FOUR:
Search and Seizure Warrants
[Fed. R. Crim. P. 41] 16

A. Specificity 18
B. Compelled Biometric Decryption (e.g., "Thumbpulsion") 19
C. Foregone-Conclusion Exception and Compelled Decryption 20
D. Compelled Third-Party Decryption 22
E. Remote-Access Warrants 23
F. Taint Teams/*CDT* Protocols 25

Acknowledgments

Although the fourth edition of *Carpe Data* has been long coming—prior installments were published in 2015, 2016, and 2017—it stands on the shoulders of giants. Magistrate Judge Deborah Smith first conceived the idea of this guide, while Magistrate Judge Mitchell Dembin edited the first three versions, named it *Carpe Data*, and contributed to our lexicon the term "thumbpulsion." This project was born from their trailblazing efforts, as well as from the indispensable contributions of the past *Carpe Data* coauthors:

Stacie F. Beckerman	U.S. Magistrate Judge, D. Or.
Laurel Beeler	U.S. Magistrate Judge, N.D. Cal.
Stanley A. Boone	U.S. Magistrate Judge, E.D. Cal.
Michelle H. Burns	U.S. Magistrate Judge, D. Ariz.
Mark Clarke	U.S. Magistrate Judge, D. Or.
Mitchell D. Dembin	U.S. Magistrate Judge (Ret.), S.D. Cal.
James P. Donohue	U.S. Magistrate Judge (Ret.), W.D. Wash.
Charles R. Pyle	U.S. Magistrate Judge (Ret.), D. Ariz.
Suzanne H. Segal	U.S. Magistrate Judge (Ret.), C.D. Cal.
John T. Rodgers	U.S. Magistrate Judge (Ret.), E.D. Wash.
Deborah M. Smith	U.S. Magistrate Judge (Ret.), D. Alaska
Jennifer L. Thurston	U.S. District Judge, E.D. Cal.

This edition would not have been possible without the unfaltering support of the Ninth Circuit Magistrate Judges Executive Board and the invaluable editorial assistance of U.S. Magistrate Judges James Goeke, Matthew Scoble, and Raymond Patricco as well as law clerks Heather Foe, Allison Jaros, Eitan Peled, Richard Westmoreland, and Sarah Fix. Most of all, this work is lovingly dedicated to our families: Mick's wife Jessica Alford as well as Andy's wife Emma Schopler and children Stephanie and Jeffrey.

ANDREW G. SCHOPLER
U.S. District Judge
(former U.S. Magistrate Judge)
Southern District of California

WENDELL "MICK" ALFORD
Law Clerk
United States District Court
Southern District of California

CHAPTER ONE

Pen Registers/Trap-and-Trace Devices [18 U.S.C. §§ 3121–3127]

***Standard of Review*:** The court must grant a sworn, written application for a pen register or trap-and-trace device that includes the applicant's identity, the identity of "the law enforcement agency conducting the investigation," and the prosecutor's certification that "the information likely to be obtained . . . is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(a)(1) and (b) (application requirements); *id.* § 3123(a)(1) (order issuance requirements).

***Description*:** In the context of telephone and internet communications, pen registers log *outgoing* phone numbers or email recipients, while trap-and-trace devices document *incoming* phone numbers or email senders. *See* 18 U.S.C. § 3127(3) (defining "pen register"); *id.* § 3127(4) (defining "trap and trace device"). The terms "pen register" and "trap and trace device" once referred only to a physical "device," *see, e.g.*, *id.* § 3127(3), (4) (1986), but now cover any "device or *process*" for obtaining this information, *id.* § 3127(3), (4) (2024) (emphasis added). The data that these tools capture is limited. Pen registers and trap-and-trace devices may not record the "contents of any communication." *Id.* § 3127(3), (4) (2024). And a "telecommunications carrier" cannot provide "call-identifying information" from these devices, which includes "any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)." 47 U.S.C. § 1002(a)(2)(B).

***Procedural Requirements*:** "The installation and use of a pen register" is "not a 'search'" under the Fourth Amendment, and thus "no warrant" is required. *Smith v. Maryland*, 442 U.S. 735, 745–46 (1979). Instead, federal prosecutors must apply for pen registers or trap-and-trace devices "in writing under oath or equivalent affirmation," and

provide the identities of the government attorney making the application and of "the law enforcement agency conducting the investigation" along with a certification that "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(a)(1), (b). If those requirements are met, the court must authorize installation. *Id.* § 3123(a)(1).

***Order's Contents*:** An order allowing a pen register or trap-and-trace device must "specify": (1) "the identity, if known," of the person who leases or owns the target phone or email address; (2) "the identity, if known, of the person who is the subject of the criminal investigation"; (3) "the attributes" "to which the order applies" (typically, the phone "number" or email address and "location of the telephone line or other facility"); and (4) "a statement of the offense" that relates to "the information likely to be obtained" from the device. 18 U.S.C. § 3123(b). The order must also require that it "be sealed until otherwise ordered by the court" and that the "person owning or leasing the line or other facility" to which the order is directed "not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court." *Id.* § 3123(d). An order permitting installation of a pen register or trap-and-trace device cannot exceed 60 days. *Id.* § 3123(c)(1).

***Extensions*:** Extensions of up to 60 days at a time may be granted. 18 U.S.C. § 3123(c)(2). The procedural requirements for an extension are the same as for an original installation. *Id.*

A. Cell-Site Simulators

Some agencies may request to use cell-site simulators—sometimes called "Stingrays"—under the pen register/trap-and-trace statutes. "Cell site simulators are devices that impersonate cell phone towers." *Andrews v. Baltimore City Police Dep't*, 8 F.4th 234, 235 (4th Cir. 2020). "In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive

cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower." *United States v. Sanchez-Jara*, 889 F.3d 418, 419 (7th Cir. 2018) (citing Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015)). "By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices." *Id.* at 420. This includes, at the very least, "identifying number[s]" from the connected phones as well as the "general direction of a subject cellular telephone." *Id.*

In some ways, cell-site simulators can be configured to function like pen register/trap-and-trace devices. As a simulated cell tower, it captures "the sorts of things available from pen registers and trap-and-trace devices," such as the phone numbers for incoming and outgoing communications of nearby mobile telephones. *See Sanchez-Jara*, 889 F.3d at 420. Some can even be calibrated to record only the information concerning a specific phone number rather than capturing information from all phones in the area. *See id.*

But due to its very nature—that is, it simulates a cell tower that covers only a specific geographic area—a cell-site simulator will always provide at least some geographic location data. As a result, some courts have been leery of authorizing cell-site simulators under the pen register/trap-and-trace statutes and have instead required a warrant supported by probable cause (refer to Chapter 4 for a discussion of the search-warrant requirements). *See, e.g.*, *United States v. Ellis*, 270 F. Supp. 3d 1134, 1149 (N.D. Cal. 2017) (holding that "the pen register statute . . . does not authorize obtaining cell phone location information" and that a warrant "is required to use a Stingray to locate a cell phone"). The Ninth Circuit has not yet addressed whether, or in what way, the pen register/trap-and-trace statutes apply to cell-site simulators.

CHAPTER TWO

Subscriber Records and Stored Communications [18 U.S.C. §§ 2701–2713]

***Standard of Review*:** It depends on the type of subscriber records or stored communications sought via 18 U.S.C. § 2703. See discussion below for each relevant category of information.

***Stored Communications Act*:** The Stored Communications Act (sometimes also called the Electronic Communications Privacy Act) permits the government to obtain a stored "record or other information pertaining to a subscriber" of an "electronic communication service or remote computing service." 18 U.S.C. § 2703(c)(1); *see also id.* § 2703(d).

***Jurisdiction*:** The Stored Communications Act gives federal judges broad authority to issue § 2703(d) orders. Any U.S. district court "(including a magistrate judge of such a court)" is authorized to issue these orders, so long as it "has jurisdiction over the offense being investigated," or the "provider" or "information" is in the district, or the court is acting on an 18 U.S.C. § 3512 "request for foreign assistance." *See* 18 U.S.C. § 2711(3); *see also id.* § 2703(d).

***Quashing or Modifying*:** If the service provider "promptly" moves to "quash or modify" a § 2703(d) order, the issuing court may grant relief "if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." 18 U.S.C. § 2703(d).

***Preclusion of Notice to Others*:** The government may seek "an order commanding a provider" "not to notify any other person of the existence of the warrant, subpoena, or court order" for subscriber records or stored communications. 18 U.S.C. § 2705(b). The court must grant such a nondisclosure order "if it determines that there is reason to believe that notification" would have an adverse result—that is,

"endangering the life or physical safety of an individual," "flight from prosecution," "destruction of or tampering with evidence," "intimidation of potential witnesses," or "otherwise seriously jeopardizing an investigation or unduly delaying a trial." *Id.*

A. Subscriber Information

***Standard of Review*:** The court may issue an order for subscriber information if the government "offers specific and articulable facts showing that there are reasonable grounds to believe" that such "records or other information" are "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

***Description*:** Subscriber information is not precisely defined. But it clearly does *not* include the "contents" of communications. *See* 18 U.S.C. § 2703(c). The term "contents" is defined as "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8); *see id.* § 2711(1) (adopting § 2510's definitions). Otherwise, the statute merely provides a "subset" of six categories of subscriber data—known as "basic subscriber information"—that "Congress has deemed less private than other records" and that may be obtained "with a mere subpoena," as well as by § 2703(d) order.[1] *Sams v. Yahoo!, Inc.*, 713 F.3d 1175, 1180 (9th Cir. 2013).

***Procedural Requirements*:** To obtain noncontent subscriber information, the government must offer "specific and articulable facts showing that there are reasonable grounds to believe" that such

---

[1] The subset of "basic" subscriber information includes a customer's "(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number) . . . ." *Sams v. Yahoo!, Inc.*, 713 F.3d 1175, 1180 & n.5 (9th Cir. 2013) (quoting in part 18 U.S.C. § 2703(c)(2)).

information is "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The statute does not place a time limit on how far back those requests can reach. *See generally id.* § 2703. And the government need not provide notice "to a subscriber or customer" of "receiving" such subscriber information. *Id.* § 2703(c)(3).

B. Location Data

***Standard of Review*:** To obtain *historical* or *retrospective* location data, a court must generally issue "a warrant supported by probable cause." *Carpenter v. United States*, 585 U.S. 296, 316 (2018). An "order issued under Section 2703(d) . . . is not a permissible mechanism for accessing historical cell-site records." *Id.* On the other hand, the Ninth Circuit has not yet addressed whether § 2703(d) orders are a proper vehicle for obtaining *real-time* or *prospective* location data.

***Legal Debate on Real-Time Location Data*:** In *Carpenter*, the Supreme Court held that collecting historical cell site location information, or historical CSLI, is "a search within the meaning of the Fourth Amendment," so "the Government must generally obtain a warrant supported by probable cause before acquiring such records." 585 U.S. at 316. But the *Carpenter* Court did not "express a view" on requests for "real-time CSLI" or minute-by-minute tracking of cell phones. *Id.*

In the absence of Supreme Court (and Ninth Circuit) guidance, most courts have rejected attempts to use § 2703(d) orders to obtain real-time location data and have instead required a warrant supported by probable cause. Some courts hold as a matter of statutory construction that § 2703(d)—and the Stored Communications Act generally—do not authorize real-time or prospective data. *See United States v. Cooper*, No. 13-CR-00693-SI-1, 2015 WL 881578, at *5 (N.D. Cal. Mar. 2, 2015) ("[A]s its name might suggest, the Stored Communications Act's entire focus . . . is to describe the circumstances under which the government can compel disclosure of existing

communications and transaction records . . . . Nothing in the SCA contemplates a new form of ongoing surveillance."); *United States v. Espudo*, 954 F. Supp. 2d 1029, 1037, 1043 (S.D. Cal. 2013) (rejecting the "theory that real-time cell site location data are business records under the SCA" as well as the "hybrid theory" that such information is available under the SCA when "combined with the Pen/Trap Statute"). Other courts focus on the constitutional argument, concluding that *Carpenter*'s privacy-related reasoning about historical CSLI also "applies to real-time CSLI." *See United States v. Broderick*, No. 5:22-CR-00251-EJD-1, 2024 WL 295293, at *6 (N.D. Cal. Jan. 25, 2024) (collecting cases).

The Seventh Circuit has taken another tack. In *United States v. Hammond*, 996 F.3d 374 (7th Cir. 2021), the Court held that "the collection of [defendant's] real-time CSLI did not constitute a search under the particular circumstances of this case." *Id*. at 387. That case arose under a different provision, which does not require a court order at all in the case of certain emergencies, but the Court later extended its holding to § 2703(d) requests. *See United States v. Lewis*, 38 F.4th 527, 538 (7th Cir. 2022), *cert. denied*, 143 S. Ct. 2499 (2023). Regardless, the Seventh Circuit concluded that there was no reasonable expectation of privacy when "the officers only collected real-time CSLI for a matter of hours while the suspect travelled on public roadways." *Hammond*, 996 F.3d at 392. It was critical to the court's analysis, like it often was in pre-*Carpenter* surveillance cases, that the real-time location data was gathered for only a short time and only in public spaces. *Id.*

Until the Supreme Court or Ninth Circuit weighs in on this debate, the suitability (and proper breadth) of § 2703(d) orders for real-time location data will remain unclear.

C. Content of Electronic Communications

***Standard of Review*:** The Stored Communications Act sets different standards depending on the age of the content records. To obtain the "contents of a wire or electronic communication" that has been "in electronic storage in an electronic communications system" for up to 180 days, the government must seek "a warrant" supported by probable cause. 18 U.S.C. § 2703(a). If it has been "in electronic storage" for *more* than 180 days, however, the Act authorizes warrantless disclosure by § 2703(d) order. *Id.* § 2703(a). Specifically, under the Act, a court may order production of such older records if the government offers "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).

***Constitutionality*:** The Sixth Circuit holds that a warrant is required—and a § 2703(d) order is insufficient—to procure *any* content records. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). The Ninth Circuit has not yet addressed this issue, but judges should tread carefully regarding § 2703 applications for content records.

***Prior Notice to Subscriber*:** Putting aside constitutional concerns about seeking content records by § 2703(d) order (see above), the government generally cannot obtain content records in this fashion until it gives "prior notice . . . to the subscriber." 18 U.S.C. § 2703(b)(1), (b)(1)(B). If the government obtains a warrant for this information, however, no such notice is required. *Id.* § 2703(b)(1)(A).

***Delayed Notice to Subscriber*:** If notice is required, the court must grant a request "for an order delaying the notification" for up to "90 days" if the court finds that "there is reason to believe that notification of the existence of the [§ 2703(d)] order may have an adverse result." 18 U.S.C. § 2705(a)(1)(A). An "adverse result" is defined as: "endangering the life or physical safety of an individual," "flight

from prosecution," "destruction of or tampering with evidence," "intimidation of potential witnesses," or "otherwise seriously jeopardizing an investigation or unduly delaying a trial." *Id.* § 2705(a)(2)(A)–(E).

***Extensions of Delayed Notice*:** Upon further applications for delayed notice, the court may extend the original delayed-notice period for up to 90 days each, with a renewed showing that notification may have an adverse result. 18 U.S.C. § 2705(a)(4).

***Taint Teams*/CDT *Protocols*:** When authorizing seizure of the content of electronic communications, judges may wish to consider whether a taint team or the so-called *CDT* protocols may be necessary. That topic is discussed in Chapter 4.

CHAPTER THREE

Tracking Warrants
[Fed. R. Crim. P. 41]

***Standard of Review*:** "After receiving an affidavit or other information, a magistrate judge . . . must issue the [tracking] warrant if there is probable cause . . . to install and use a tracking device." Fed. R. Crim. P. 41(d)(1).

***"Tracking Device" Defined*:** A "tracking device" is "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b); *see also* Fed. R. Crim. P. 41(a)(2)(E) (same).

***Are Cell Phones "Tracking Devices"?*:** Because tracking-device warrants authorize—and draw their venue limitations from—"install[ation]" of a device, it's unclear whether mobile phones with built-in GPS receivers qualify as tracking devices. *See* Fed. R. Crim. P. 41(b)(4) ("[A] magistrate judge . . . has authority to issue a warrant to *install* within the district a tracking device." (emphasis added)); 18 U.S.C. § 3117(a) ("If a court is empowered to issue a warrant or other order for the *installation* of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is *installed* in that jurisdiction." (emphasis added)). The Ninth Circuit has not yet resolved this ambiguity, and courts have come to differing conclusions. *Compare United States v. Ackies*, 918 F.3d 190, 199 (1st Cir. 2019) (holding that "a cell phone used for obtaining precise location information does not fit within the definition of a 'tracking device,'" because the jurisdictional provision—18 U.S.C. § 3117(a)—"refers to the 'installation of a mobile tracking device'"), *with In re Search Warrant Application for Location Information*, 754 F. Supp. 3d 1099, 1110, 1134–35 (D.N.M. 2024) (disagreeing with *Ackies*, holding that "a cell phone used to track a person's location on a real-time, rolling basis is a tracking device," and

concluding that Congress's use of "conditional words" like "*if* and *may*" in § 3117(a) "make clear that this section does not apply in all circumstances"—that is, "if a device is not installed, its designation as a tracking device" is unaffected).

These conflicting interpretations have practical consequences. If mobile phones are tracking devices, requests for real-time cell-phone location data are then subject to the more specific jurisdictional limitations and notification requirements set out below. If not, then jurisdiction may be based on the investigated offense, rather than the phone's location, and investigators would avoid Rule 41's tracking-specific requirements. Although in many cases the jurisdictional prerequisites will be met under either theory, judges will be well served to adopt a standard approach until the Ninth Circuit or Supreme Court provides more guidance.

For judges who treat cell phones as tracking devices, the Administrative Office's standard Tracking Warrant form accommodates this approach. The form does not require that the tracking device be "installed." It instead offers checkboxes for either (i) "using the object . . . to monitor the location of the person, property, or object" or (ii) "installing and using a tracking device." *See* AO Form 104 (attached at page 15).

***Procedural Requirements*:** To issue a tracking warrant, a magistrate judge must find that: (1) venue is proper for the warrant application and (2) there is probable cause to believe that installing and using a tracking device will satisfy one of the appropriate investigative purposes set out in Rule 41(c). *See* Fed. R. Crim. P. 41(b), (c), (d)(1).

(1) *Venue*: Magistrate judges have "authority to issue a warrant to install" a tracking device "within the district" in which they sit if a warrant application from "a federal law enforcement officer or an attorney for the government" establishes that the person,

property, or object to be tracked is "within the district" or will be in the district at installation.[2] *See* Fed. R. Crim. P. 41(b), (b)(4).

(2) *Probable Cause*: Probable cause exists when "the totality of the circumstances indicates a fair probability" that "evidence of a crime," or one of the other Rule 41(c) purposes, "would be found" by tracking the target's location. *See United States v. Elmore*, 917 F.3d 1068, 1074–75 (9th Cir. 2019) (cleaned up). The affidavit need not establish that a tracking device "is more likely than not" to reveal the evidence, but merely that "it would be reasonable to seek the evidence" with the requested tracking device. *See id.* at 1074.

***Tracking Warrant's Contents*:** A tracking warrant must "identify the person or property to be tracked, designate the magistrate

---

[2] The Administrative Office of the U.S. Courts' standard form for Tracking Warrants lists another venue basis: "the activity in this district relates to domestic or international terrorism." AO Form 104 (attached at page 15). But courts in the Ninth Circuit have not yet analyzed whether the terrorism-related venue provision—which applies to "a warrant for a person or property"—extends to tracking warrants. *See* Fed. R. Crim. P. 41(b)(3). Rule 41 seems to draw a distinction between tracking warrants and warrants to search or seize people or property. *See, e.g.*, Fed. R. Crim. P. 41(f)(1)–(2) (setting different standards for these two types of warrants). For example, Rule 41 authorizes both federal judges and (sometimes) state judges "to issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1); *see also* Fed. R. Crim. P. 1(c). Yet it authorizes only federal judges "to issue a warrant to install within the district a tracking device." Fed. R. Crim. P. 41(b)(4); *see also* Fed. R. Crim. P. 1(c). The Advisory Committee believed that "only federal judicial officers should be authorized to issue" tracking warrants, because "the authorized tracking may involve more than one district or state." Fed. R. Crim. P. 41(b) advisory committee's notes to 2006 amendments.

judge to whom it must be returned," "specify a reasonable length of time that the device may be used . . . not to exceed 45 days from the date the warrant was issued," and "command the [executing] officer" to: "complete installation . . . within a specified time no longer than 10 days"; install the tracking device "during the daytime," unless the judge finds good cause to authorize nighttime installation; and "return the warrant to the judge designated in the warrant." Fed. R. Crim. P. 41(e)(2)(C).

***Warrant Extensions*:** For "good cause," the court may "grant one or more extensions" of the tracking warrant "for a reasonable period not to exceed 45 days each." Fed. R. Crim. P. 41(e)(2)(C).

***Tracking Outside District*:** Although federal judges may issue warrants to "install" tracking devices only "within the district" in which they sit, Fed. R. Crim. P. 41(b)(4), the court may authorize post-installation "use of the device . . . within the district, outside the district, or both," *id.*; 18 U.S.C. § 3117(a) (same).

***Returning the Warrant*:** "Within 10 days after the use of the tracking device has ended, the officer executing the warrant must return it" to the designated judge, noting "the exact date and time the device was installed and the period during which it was used." Fed. R. Crim. P. 41(f)(2)(A)–(B).

***Service*:** Within that same 10-day period, the officer must also "serve a copy of the warrant on the person who was tracked or whose property was tracked." Fed. R. Crim. P. 41(f)(2)(C).

***Delayed Service*:** "Upon request of the government, the judge may delay notice" to the person tracked or whose property was tracked. Fed. R. Crim. P. 41(f)(2)(C), (f)(3). To do so, the court must: (1) find "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in [18 U.S.C.] section 2705, except if the adverse results consist only of

unduly delaying a trial)," and (2) the warrant must prohibit "the seizure of any tangible property, any wire or electronic communication (as defined in [18 U.S.C.] section 2510)," and—except as authorized by the Stored Communications Act, 18 U.S.C. § 2701, et seq.—"any stored wire or electronic information, except where the court finds reasonable necessity for the seizure[.]"[3] 18 U.S.C. § 3103a(b)(1)–(2); *see* Fed. R. Crim. P. 41(f) advisory committee's notes to 2006 amendments (noting that the delayed-notice provision for tracking warrants "is co-extensive with 18 U.S.C. § 3103a(b)"); *see also id*. advisory committee's notes to 2016 amendments (citing 18 U.S.C. § 3103a in connection with Rule 41(f)(3)'s delayed-notice authority). The initial timeframe of delayed notice must be "a reasonable period not to exceed 30 days after the date of [the warrant's] execution, or on a later date certain if the facts of the case justify a longer period of delay." 18 U.S.C. § 3103a(b)(3).

***Extensions of Delay*:** Delayed service may be extended "for good cause shown, subject to the condition that extensions should only be granted upon an updated showing of the need for further delay." 18 U.S.C. § 3103a(c). Those extensions are presumptively "limited to periods of 90 days or less, unless the facts of the case justify a longer period of delay." *Id*.

[3] For reasons unknown, AO Form 104 for Tracking Warrants (attached at page 15) omits this last required prohibition. Judges who use this form and wish to delay notice will have to add this language to the warrant themselves (or find reasonable necessity for the seizure of stored wire or electronic information).

UNITED STATES DISTRICT COURT

for the

_____ District of _____

In the Matter of the Tracking of *(Identify the person, property, or object to be tracked)*	)	
	)	Case No.
	)	

TRACKING WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government shows there is reason to believe that the person, property, or object described above has been involved in and likely will continue to be involved in the criminal activity identified in the application, and ❒ is located in this district; ❒ is not now located in this district, but will be at execution; ❒ the activity in this district relates to domestic or international terrorism; ❒ other:

_____.

I find that the affidavit(s), and any recorded testimony, establish probable cause to believe that *(check the appropriate box)* ❒ using the object ❒ installing and using a tracking device to monitor the location of the person, property, or object will satisfy the purpose set out in Fed. R. Crim. P. 41(c) for issuing a warrant.

❒ I find entry into the following vehicle or onto the following private property to be necessary without approval or knowledge of the owner, custodian, or user of the vehicle or property for installing, maintaining, and removing the tracking device:

YOU ARE COMMANDED to execute this warrant and begin use of the object or complete any installation authorized by the warrant by _____ *(no later than 10 days from the date this warrant was issued)* and may continue to use the device until _____ *(no later than 45 days from the date this warrant was issued)*. The tracking may occur within this district or another district. To install, maintain, or remove the device, you may enter *(check boxes as appropriate)*

❒ into the vehicle described above ❒ onto the private property described above

❒ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Within 10 calendar days after the use of the tracking device has ended, the officer executing this warrant must both return it to *(United States Magistrate Judge)* _____ and — unless delayed notice is authorized below — serve a copy of the warrant on the person who, or whose property or object, was tracked.

❒ Pursuant to 18 U.S.C. § 3103a(b)(1), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and this warrant prohibits the seizure of any tangible property or any wire or electronic communications (as defined in 18 U.S.C § 2510). I therefore authorize the officer executing this warrant to delay notice to the person who, or whose property or object, will be tracked *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: _____ _____
Judge's signature

City and state: _____ _____
Printed name and title

Chapter Four
Search and Seizure Warrants
[Fed. R. Crim. P. 41]

***Standard of Review*:** "After receiving an affidavit or other information, a magistrate judge . . . must issue the warrant if there is probable cause to search for and seize a person or property[.]" Fed. R. Crim. P. 41(d)(1).

***Procedural Requirements*:** To issue a search-and-seizure warrant, a magistrate judge must find that: (1) venue is proper for the warrant application and (2) there is probable cause to search for and seize a person or property.

(1) *Venue*: "At the request of a federal law enforcement officer or an attorney for the government," magistrate judges have "authority to issue a warrant to search for and seize a person or property located within the district" in which they sit. Fed. R. Crim. P. 41(b), (b)(1). Based on such a warrant application, magistrate judges may also issue a search-and-seizure warrant for a person or property outside the district under various circumstances: (a) "the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed"; (b) the investigation involves "domestic terrorism or international terrorism"; (c) the target property is located in "a United States territory, possession, or commonwealth" or in premises or residences used or owned by a "United States diplomatic or consular mission in a foreign state"; or (d) the requirements are met for "remote access to search electronic storage media and to seize or copy electronically stored information." Fed. R. Crim. P. 41(b)(2)–(3), (b)(5)–(6).

(2) *Probable Cause*: A search-and-seizure warrant must issue if the warrant application and affidavit establish "probable cause to

search for and seize a person or property" for: (a) "evidence of a crime"; (b) "contraband, fruits of crime, or other items illegally possessed"; (c) "property designed for use, intended for use, or used in committing a crime"; or (d) "a person to be arrested or a person who is unlawfully restrained." *See* Fed. R. Crim. P. 41(c), (d)(1). Probable cause exists when "the totality of the circumstances indicates a fair probability" that such items "will be found in a particular place." *See United States v. Elmore*, 917 F.3d 1068, 1074 (9th Cir. 2019) (cleaned up).

***Search-and-Seizure Warrant's Contents*:** All nontracking warrants must "identify the person or property to be searched, identify any person or property to be seized," "designate the magistrate judge to whom it must be returned," and "command the [executing] officer" to: "execute the warrant within a specified time no longer than 14 days"; "execute the warrant during the daytime" unless the judge finds good cause to authorize nighttime execution; and "return the warrant to the magistrate judge designated in the warrant." Fed. R. Crim. P. 41(e)(2)(A).

***Electronically Stored Information (ESI)*:** A search-and-seizure warrant "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information." Fed. R. Crim. P. 41(e)(2)(B). In such cases, the deadline for "executing the warrant . . . refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." *Id.* Unless the judge specifies otherwise, the warrant presumptively "authorizes a later review of the media or information consistent with the warrant." *Id.*

The upsurge in electronic storage has brought with it unique legal challenges. Six of these are discussed in more detail below: (a) specificity; (b) compelled biometric decryption (such as "thumbpulsion"); (c) the foregone-conclusion exception and compelled decryption; (d) compelled third-party decryption; (e) remote-access warrants; and (f) taint teams/*CDT* protocols.

A. Specificity

All search-and-seizure warrants are subject to a constitutional "specificity" requirement. *United States v. Holcomb,* 132 F.4th 1118, 1127 (9th Cir. 2025). Specificity has two aspects: "breadth and particularity." *Id*. A warrant must be limited in its breadth "by the probable cause on which the warrant is based," while the demand of particularity means that a warrant must "clearly state what is sought." *Id*. "Together, these requirements protect against the principal evil of general warrants," which allowed officials to "search and seize whatever and whomever they pleased while investigating crimes." *Id*. (cleaned up). "[G]iven the vast amount of data" on electronic devices, courts must apply a "heightened specificity requirement" in the "computer context." *Id.* (cleaned up).

In *Holcomb*, for example, the Ninth Circuit invalidated a warrant regarding a computer's hard drive for lack of specificity. The warrant permitted the government to seize information and files "that would show dominion and control for the computer." 132 F.4th at 1128 (cleaned up). That authorization was both overbroad and "insufficiently particular" because it had no "temporal limitation" nor any constraint on the "particular type" of file that could be searched "to determine if it was responsive to the dominion and control provision," leaving the examiner to exercise "his unfettered discretion in determining which files to scroll past and which files to open and examine." *Id*. at 1128–29.

Nonetheless, this is a tightly fact-bound inquiry that defies broad categorical rules. For instance, "warrants describing general categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible." *Id.* at 1130 (cleaned up). Nor must warrants "always contain temporal limitations." *Id.* When faced with a warrant application for digital evidence, judges should carefully review *Holcomb* before concluding the heightened requirement is met.

B. Compelled Biometric Decryption (e.g., "Thumbpulsion")

Today many people unlock their smart phones and other secure digital devices through biometric authentication. That is, instead of a traditional password, they use a biometric marker: a face scan, fingerprint, or the like. As a result, government agents sometimes seek court approval to force suspects to offer their faces or fingerprints to access a seized device. A key question is: Does compelled production of biometric data violate a suspect's Fifth Amendment right against self-incrimination?

In at least one scenario, the Ninth Circuit has permitted forced biometric decryption. It recently held in *United States v. Payne*, 99 F.4th 495 (9th Cir. 2024), that when the police "grabbed Payne's thumb and used it to unlock [his] phone," this "was not a testimonial act and the Fifth Amendment does not apply." *Id.* at 500, 513.

Beyond making suspects give their thumbprints—"thumbpulsion," if you will—are there any Fifth Amendment concerns with court-ordered biometric decryption? The *Payne* court itself cautioned that its "opinion should not be read to extend to *all* instances where a biometric is used to unlock an electronic device." 99 F.4th at 513. And it acknowledged that "Fifth Amendment questions like this one are highly fact dependent . . . ." *Id.*

For the Fifth Amendment privilege to apply, "there must be a 'communication' at issue that is: (1) compelled; (2) incriminating; and (3) testimonial." *Payne*, 99 F.4th at 507 (quoting *Hiibel v. Sixth Jud. Dist. Ct. of Nev.*, 542 U.S. 177, 189 (2004)). "Testimonial communications are those that, 'explicitly or implicitly, relate a factual assertion or disclose information.'" *Id.* at 508 (quoting *Doe v. United States*, 487 U.S. 201, 210 (1988)). The forced thumbprint in *Payne* did not qualify as such a testimonial communication because it "did not intrude on the contents of Payne's mind" and could have been "accomplished even if Payne had been unconscious." *Id.* at 511. By

contrast, the *Payne* court noted, the result might "have been different had Officer Coddington required Payne to independently select the finger that he placed on the phone." *Id.* at 513.

In fact, the D.C. Circuit recently confronted exactly that scenario and found the distinction dispositive. In *United States v. Brown*, 125 F.4th 1186, 1202 (D.C. Cir. 2025), law enforcement "ordered Schwartz to open the cellphone, and Schwartz complied by placing his thumb on the cellphone." *Id.* at 1202. The *Brown* court ruled that "the compelled opening of the cellphone was testimonial under the Fifth Amendment" and that the resulting evidence must be suppressed. *Id.* at 1201. It reasoned that Schwartz's selection of which finger to use "disclose[d] his knowledge of how the phone could be opened, and specifically his understanding that his thumb would unlock the device, and those disclosures revealed his ownership or control over the phone and the messages it contained." *Id.* at 1203–04.

In ruling on requests to compel biometric decryption, magistrate judges should carefully study the *Payne* court's reasoning and each case's unique factual circumstances.

C. Foregone-Conclusion Exception and Compelled Decryption

The Fifth Amendment right against self-incrimination generally prohibits judges from ordering suspects "to turn over their alphanumeric passcode," as the act of production is testimonial, not merely a physical act. *Payne*, 99 F.4th at 510. That is, it requires "an individual to divulge the contents of his mind." *Id.* But some courts have authorized compelled disclosure of fully "decrypted devices," without first giving the "decryption password" to the government, under the Fifth Amendment's "foregone conclusion" exception. *United States v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018).

Under the "foregone conclusion" doctrine, the compelled production of evidence does not violate the privilege against self-

incrimination when the "existence and location of the papers are a foregone conclusion and the [suspect] adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers." *Fisher v. United States*, 425 U.S. 391, 411 (1976). "For this exception to apply, the government must establish its independent knowledge of three elements" regarding the sought-after information: the evidence's "existence," its "authenticity," and "the defendant's possession or control" of it. *United States v. Oriho*, 969 F.3d 917, 927 (9th Cir. 2020) (cleaned up).

Two circuit cases are instructive in applying this principle. In *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017), a magistrate judge ordered a suspect in a child-pornography case to provide his digital devices to investigators "in a fully unencrypted state." *Id.* at 243. The suspect moved to quash that order, arguing that "his act of decrypting the devices would violate his Fifth Amendment privilege against self-incrimination." *Id.* In denying the motion to quash, the magistrate judge ruled that "any testimonial aspects of that production were a foregone conclusion." *Id.* at 248. Specifically, the court pointed out that the search-warrant affidavit offered detailed factual allegations establishing that the suspect "possessed, accessed, and owned" all the devices in question, and that these devices contained images "that constitute child pornography." *Id.* Among other things, the suspect's sister reported seeing him "unlock his Mac Pro while connected to the hard drives to show her hundreds of pictures and videos of child pornography." *Id.* On appeal, the Third Circuit upheld the "Decryption Order," noting that the "factual findings" underpinning the "application of the foregone conclusion doctrine" were "amply supported by the record." *Id.*

By contrast, in *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335 (11th Cir. 2012), the Eleventh Circuit concluded that the evidence was too weak to support a decryption order in a different child-pornography case. It held that the government

failed to show with "reasonable particularity" that "encrypted files exist on the drives, that [the suspect] has access to those files, or that he is capable of decrypting the files." *Id*. at 1349. In addition, the government failed to establish with "any degree of particularity what, if anything, was hidden behind the encrypted wall." *Id*. On these facts, the court held that "the Government cannot show that the 'foregone conclusion' doctrine applies," so the "Fifth Amendment protects [the suspect's] refusal to decrypt." *Id*.

The Ninth Circuit has acknowledged that courts may have to grapple with the "foregone conclusion doctrine" in the compelled-decryption arena, *see Payne*, 99 F.4th at 513, but it has not yet directly addressed this issue.

D. Compelled Third-Party Decryption

Instead of forcing a suspect to unlock or decrypt a digital device, the government may seek an order under the All Writs Act to compel a third party—usually a service provider or manufacturer—to assist in bypassing the device's security features. The All Writs Act grants federal courts the power to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 26 U.S.C. § 1651(a). In practical terms, the Act "permits the district court, in aid of a valid warrant, to order a third party to provide nonburdensome technical assistance to law enforcement officers." *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979).

The Ninth Circuit has not yet taken up the issue of third-party decryption orders. But in *United States v. Blake*, 868 F.3d 960 (11th Cir. 2017), the Eleventh Circuit held that an "order requiring Apple to assist in bypassing the iPad's security features" did "not exceed the district court's authority" under the All Writs Act. *Id*. at 969, 973. The *Blake* court analyzed the "five requirements that must be met

before a court can compel under the All Writs Act the assistance of a third party in a criminal investigation," namely:

> (1) the order must be necessary or appropriate to effectuate a previously issued order, (2) it must not be covered by another statute, (3) it must not be inconsistent with the intent of Congress, (4) the third party must not be too far removed from the underlying case, and (5) the burden imposed on the third party must not be unreasonable.

868 F.3d at 970–71 (citing *United States v. New York Tel. Co.*, 434 U.S. 159, 172–78 (1977)).

It's unclear whether the Ninth Circuit will follow the Eleventh Circuit's lead on compelled third-party decryption. Even if it does, the analysis of an All Writs Act order under *Blake* and *New York Telephone* is a fact-bound inquiry. For any given case, factual nuances or new statutory investigative tools could change the court's analysis and lead to a different result.

E. Remote-Access Warrants

***Pre-2016 History of Remote Access*:** It is useful to understand how Rule 41's remote-access provisions came about. Before the 2016 amendments to the Federal Rules, there was a wealth of cases about a remote-access (or hacking) program called the "Network Investigative Technique ('NIT'), which allowed the FBI to circumvent the anonymizing features of the dark web and collect computer-related identifying information, including internet protocol ('IP') addresses." *United States v. Eldred*, 933 F.3d 110, 111 (2d Cir. 2019). NIT worked like malware that downloaded from a law-enforcement-seized website—typically a site hosting child pornography—onto a user's computer and surreptitiously "transmit[ted] identifying information back to the government server." *See id.* at 113. But courts struggled to figure out which district, if any, had jurisdiction to issue such warrants since the location of those users' computers was unknown at the time the court

authorized the use of the hacking software. *See, e.g.*, *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (noting that the "search of the Target Computer" "takes place, not in the airy nothing of cyberspace," but in some physical location that remains unspecified, which "means that the Government's application cannot satisfy the territorial limits of Rule 41(b)(1)").

***Current Practice for Remote Access*:** In 2016, Congress solved this conundrum by amending Rule 41 with specific rules for remote-access warrants. If the other, non-venue requirements for a warrant are satisfied, a magistrate judge may "issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside" the judge's district under either of two circumstances. Fed. R. Crim. P. 41(b)(6). First, a remote-access warrant is proper if "the district where the media or information is located has been concealed through technological means." Fed. R. Crim. P. 41(b)(6)(A). Alternatively, such a warrant may issue in an investigation regarding damage or access to protected computers, in violation of 18 U.S.C. § 1030(a)(5), when "the media are protected computers that have been damaged without authorization and are located in five or more districts." Fed. R. Crim. P. 41(b)(6)(B).

Rule 41's remote-access provisions do not address "constitutional questions, such as the specificity of description that the Fourth Amendment may require in a warrant for remotely searching electronic storage media or seizing or copying electronically stored information." Fed. R. Crim. P. 41(b)(6) advisory committee's notes to 2016 amendments. The Advisory Committee intended to leave the application of "constitutional standards to ongoing case law development." *Id*. Unfortunately, contemporary guidance on the remote-access particularity requirement remains sparse.

F. Taint Teams/*CDT* Protocols

Because data seizures often require sifting through a massive amount of information—only some of which will be authorized for seizure—the Ninth Circuit briefly mandated that a "warrant application" for electronic data "should normally include . . . a protocol for preventing agents involved in the investigation from examining" the initial electronic data seized. *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1000 (9th Cir. 2009), *opinion revised and superseded*, 621 F.3d 1162 (9th Cir. 2010). One such *CDT* protocol included "segregation" of the responsive information by a taint team—"specially trained computer personnel who are not involved in the investigation" and who "will not communicate any information they learn during the segregation process" to the investigators. *Id.* Similarly, when "the privacy interests of numerous other parties who are not under suspicion of criminal wrongdoing are implicated by the search," the "presumpt[ive]" protocol involved "segregation of the data" by "an independent third party selected by the court." *Id.*

That mandate was lifted on reconsideration and instead found its way, along with other suggestions, into a concurring opinion as "guidance" for magistrate judges. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179–80 (9th Cir. 2010) (Kozinski, C.J., concurring). The Ninth Circuit has since made clear that the "absence" of those "precautionary search protocols" is not "fatal" to many warrants. *United States v. Schesso*, 730 F.3d 1040, 1043 (9th Cir. 2013). Instead, the trial court must carefully weigh whether there are substantial risks of "an over-seizure of data that could expose information about other individuals not implicated in any criminal activity" or "expose sensitive information about [the warrant's target] other than his possession" of computer contraband. *Id.* at 1049. To date, the Ninth Circuit has not invalidated a search warrant for failing to include the *CDT* protocols or guidance.