Carpe Data:

A Guide for Ninth Circuit Magistrate Judges When Reviewing Government Applications to Obtain Electronic Information

Third Edition

Magistrate Judges Executive Board
United States Courts for the
Ninth Circuit

July 2017

Carpe Data:

A Guide for Ninth Circuit Magistrate Judges When Reviewing Government Applications to Obtain Electronic Information

Third Edition 2017

Magistrate Judges Executive Board
United States Courts for the Ninth Circuit

Table of Contents

A Note of Introduction

The Ninth Circuit Magistrate Judges Executive Board is pleased to present the third edition of *Carpe Data: A Guide for Ninth Circuit Magistrate Judges When Reviewing Government Applications to Obtain Electronic Information.* The first and second editions of the guide, published in July 2015 and July 2016, were well-received by judges throughout the Circuit and have proven especially helpful to newly-appointed magistrate judges grappling with complicated legal issues in the context of woefully outdated statutes.

Practice guides and bench books are usually useful when first written but become obsolete or even misleading as the law changes. To prevent that fate, the Technology Committee presents the third edition of *Carpe Data*, providing updates in the fast-developing areas of law involved in the review of ex parte government applications to obtain electronic information. This edition, for example, addresses the state of the law regarding border searches of computers and smart phones; explores the recent amendments to Rule 41, expanding the jurisdictional reach of search warrants in cases where data is hidden by technological means or involving damage to computers in multiple districts; addresses warrants compelling individuals to unlock smart phones by pressing their finger to the screen; and recent decisions regarding the extraterritoriality of warrants for electronic mail.

I greatly appreciate the efforts of my colleagues on the 2017 MJEB Technology Committee in revising and updating the guide: Mitch Dembin, Chair (S.D. Cal.), Stacie Beckerman (D. Ore.), Laurel Beeler (N.D. Cal.), Stanley Boone (E.D. Cal.), Michelle Burns (D. Ariz.), John Rodgers (E.D. Wa.), Deborah Smith (D. Ak.), Suzanne Segal (C.D. Cal.) and Jennifer Thurston (E.D. Cal.). I am also proud to be part of the group. Credit is also due to Mark Clarke (D. Ore.) and Charles Pyle (D. Ariz.) whose earlier efforts have been updated in this edition. We must acknowledge the invaluable assistance of Assistant Circuit Executive David Madden and the Ninth Circuit Public Information Unit in producing the guide. Finally, we would be remiss in not acknowledging the assistance of the intrepid law clerks and externs who assisted in writing and updating this guide: Jenny Burns, Law Clerk to M.J. Dembin (S.D. Cal.); Andrew Wenker, Extern to M.J. Burns (D. Ariz.); and Lee Baxter and Patrick Stocks, Law Clerks to M.J. Smith (D. Ak.).

James P. Donohue (W.D. Wa.)
Chair
Magistrate Judges Executive Board
Ninth Circuit Court of Appeals

A Word of Advice When Reviewing Government Applications to Obtain Electronic Data and Communications

Magistrate judges handling criminal matters are regularly confronted with varied and sometimes inconsistent applications from federal prosecutors and agents seeking to obtain electronic evidence. During criminal duty, a magistrate judge may see many, if not all, of the following: pen/trap applications, 2703(d) applications (including historical cell site activations), applications to use cell tower simulators, applications for tracking warrants, search warrants for the content of stored electronic communications and search warrants for electronic devices. Keeping apprised of changing technologies and how our rules and laws deal with them can be daunting. If you are lost already, this guide is for you.

With this guide we endeavor to identify the various applications that you may see and the practical and legal issues that attend them. We have tried to be objective and not take a position regarding the issues. There always will be differences of opinions. We hope that this guide will help you identify, navigate and decide the issues that you may confront and perhaps provide some comfort that you are not alone. Preparing this guide has convinced us, however, that we should make a couple of recommendations to you. Here they are:

I. Take Your Time

Criminal duty, for many of us, can be grueling. Between initial appearances and detention hearings, many hours are consumed on the bench. While on the bench, a stack of applications for pen register orders, 2703(d) orders, subpoenas with requests for preclusion of notice ("gag") orders, search warrants for electronic mail directed at service providers, search warrants for computers and other electronic storage devices (such as smart phones and tablets), tracking warrants, and applications for extensions of delay notice pile up. And there are new complaints to be presented and signed and a host of other miscellaneous criminal matters. It is often the path of least resistance, once confirming that the application meets the necessary standard of review, to assume that the boilerplate provisions are consistent with the law and give those only cursory review. The devil is often in the details with these applications, however, often is in the details so we recommend that you confirm that the application or warrant does not overstep reasonableness and is consistent with the law.

II. Request Additional Briefing

There is no shame in requiring the government to provide you with supplemental authority in any area in which you have concern. It has been our collective experience that your discomfort oftentimes is well-founded.

III. Write About It

As you will see, there is a dearth of written opinions in many important areas. We all know that the law develops through written decisions which can be challenged by peers and on appeal. The ex parte nature of these proceedings, however, allow us the luxury of simply denying or granting applications without writing a formal opinion. This can lead to judge shopping within a district and render the issue unresolved for months or years. When you reject an application, consider writing an opinion explaining why. When you do write, think about publishing a redacted version of your order so that you can add to the public record.

IV. Consider Templates

Although it may appear inconsistent with the recommendation to write about these issues, you may want to consider working with your U.S. Attorney's Office to develop templates that meet the concerns of some or all of the members of your bench. Developing templates allows for the focus to be on probable cause and specificity during judicial review rather than on protocols, time limits and the like. If consensus cannot be reached, perhaps magistrate judges on each side of the divide will consider writing opinions when denying an application so that the matter can move forward to the district and appellate courts. If you are interested in examining the templates used by other courts, contact any of us.

Magistrate Judges Executive Board
Mitch Dembin (S.D. Cal.)
Chair, Technology Committee
July 17, 2017

Chapter One

A Starting Point: The Law in this Field

This section contains a very brief description of the type of applications that the government may present to a magistrate judge to obtain electronic information during a criminal investigation. The relevant statutes and standards of review are listed for each type of application. For the most part, the statutes are out of tune with the current state of technology. As the world has shifted from analog to digital, from rotary to mobile, from wired to wireless, government attorneys and agents have been straining to fit new technologies and investigative techniques into a mostly obsolete legal framework. Despite this, it falls to the magistrate judge to grant only applications that conform to the law.

I. Pen Register/Trap and Trace Application: 18 U.S.C. §§ 3121-3127

Standard of Review: The court must grant the application if the prosecutor certifies that the information likely to be obtained is relevant to a criminal investigation.

A pen register is a device that records all numbers dialed from a particular phone—*i.e.*, outgoing telephone calls. § 3127(3). A trap and trace device captures all numbers received by a particular phone—*i.e.*, incoming telephone calls. § 3127(4). The use of a pen register/trap and trace device does not constitute a search under the Fourth Amendment. Nonetheless, by statute, the government must make a minimal showing before it can lawfully use such a device. A prosecutor must certify to the court that the information likely to be obtained is relevant to an ongoing criminal investigation. Once the prosecutor has made that certification, which does not have to be under oath, the court must grant the application.

The USA Patriot Act of 2001 modified the pen register/trap and trace statute to include internet communications. This modification appears to allow the government to obtain such information as the internet address of any computer that accesses an email account (such as Google Gmail) and the address information for all incoming and outgoing emails to and from the target account. 18 U.S.C. § 3127(3) and (4).

A. Cell-Site Simulators as Pen/Trap Devices

The government may request the court to authorize the use of cell site simulators as pen/trap devices to identify the phone number used by a subject of the investigation. Cell site simulators imitate real cell towers and can passively record all numbers dialed or received by phones "registered" to the simulator. The other phones may be unrelated to the investigation. The simulators also can force all cell phones in its coverage area to register with it, thus capturing not only numbers dialed or received by the subject's phone, but also by other phones in the immediate vicinity. Sometimes, use of a simulator may momentarily interrupt legitimate service. By setting up near locations where the suspects are known to gather, a simulator can identify target numbers by process of elimination and then obtain a normal pen/trap order. Simulators, once a suspect's telephone number has been identified, can be used to assist agents in surveillance of the suspect.

What process is required? Title 18 U.S.C. § 3121(a) requires a court order to install or use a pen/trap device. A simulator may fit within the definition of a pen/trap device. *See* 18 U.S.C. § 3127(3) and (4).

The forced registration of nearby cell phones to the cell site simulator (resulting in the collection of information from phones that may be irrelevant to the investigation) has not been addressed in case law. In one case, however, the government obtained a warrant to use a simulator to locate a suspect. *See United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2013). Another court declined to issue a pen/trap order allowing the use of a simulator because the technology was not adequately explained. *See In re Application of United States,* 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012).

B. Subscriber Records Applications: 18 U.S.C. §§ 2701-2712

1. Subscriber Records Excluding Content of Communications

Standard of Review: The court grants the application if the government offers specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing investigation.

Under the 1986 Stored Communications Act (SCA), which is part of the Electronic Communications Privacy Act, the government may obtain, pursuant to a court order, "a record or other information pertaining to the subscriber" of an "electronic communication service or remote computing service." 18 U.S.C. § 2703(c)(1)(B) and § 2703(d). Subscriber records are records which contain

information about a customer but do not include content of communications. Basic subscriber records include a customer's name and address; telephone call records, including the time and duration of calls; length and type of service provided; and method of payment. § 2703(c)(2). Other, non-basic subscriber records include transactional records, such as logs recording account usage, or the email addresses of individuals with whom the customer has corresponded. § 2703(c)(1).

The SCA, § 2703(c), permits the government to obtain basic subscriber records by administrative subpoena or grand jury subpoena, by court order or search warrant. As noted *supra*, when seeking a court order pursuant to §2703(c)(1)(B), the government must "offer specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." § 2703(d).

2. Subscriber Records Including Content of Electronic Communications in Storage over Six Months

The SCA also allows the government to seek the content of electronic communications **in storage for more than six months** by means of a grand jury subpoena or a court order under § 2703(d) supported by specific and articulable facts. Using either form of process for communications requires notice by the government to the subscriber (which may be delayed). The government may also seek an order precluding the provider from notifying its subscriber. 18 U.S.C. § 2705(b).

Most prosecutors, however, opt to obtain the content of stored electronic mail by means of a Rule 41 search warrant, requiring a showing of probable cause. Then notice to the subscriber by the government is not required. § 2703(b)(1)(A). And the government usually seeks a companion order precluding the provider from notifying its subscriber of the warrant. § 2705(b)

C. Search & Seizure Warrants: Rule 41 Fed. R. Crim. P.

Standard of Review: Probable cause.

Whenever the government seeks a search and seizure warrant, including a warrant to search a suspect's home, personal computer, or to collect physical and electronic evidence from third parties, the procedure outlined in Rule 41 of the Federal Rules of Criminal Procedure must be followed. A search and seizure warrant may be issued to obtain evidence of a crime; contraband, fruits of a crime,

or other items illegally possessed; property designed for use, intended for use, or used in committing a crime; or to arrest someone (a fugitive, for instance). Fed. R. Crim. P. 41(c)(1)-(4).

Following amendment in 2016, Rule 41 explicitly permits magistrate judges to issue multidistrict warrants for electronic information in the following circumstances: (1) when the location of the electronic information has been concealed through technological means, or (2) when the warrant is requested in an investigation of a violation of 18 U.S.C. § 1030(a)(5) involving protected computers located in five or more districts. Fed. R. Crim. P. 41(b)(6)(A),(B). These changes are discussed in detail in Chapter Four.

D. Tracking Warrant Applications: 18 U.S.C. § 3117 and Rule 41 Fed. R. Crim. P.

Standard of Review: Probable cause.

Historically, the government had to physically install a tracking device on a suspect's person or personal property to track electronically that person or property. A search warrant has been required to install such a tracking device, even if the installation and tracking all occur in public places, since the Supreme Court's decision in *United States v. Jones*, 132 S. Ct. 945 (2012). In *Jones*, the Court found the physical invasion of the property, in that case magnetically attaching a device to a vehicle, to be a search requiring a warrant based on probable cause. Fed. R. Crim. P. 41(d)(1). Now, however, the government may track a person in real time through their cellular telephone or other mobile device with or without assistance from the service provider.

Service providers have and maintain records of the cell towers involved in communications to and from a mobile phone. These historical records can assist agents in identifying, with varying degrees of specificity, where a phone was at the time of a particular call. The type of process required to obtain historical cell site activation records from a provider, remains subject to dispute. The Fourth, Fifth, Sixth and Eleventh Circuits have found that because cell-site information voluntarily is provided to a third party, the service provider, it may be disclosed upon a showing of specific and articulable facts in an application under 18 U.S.C. § 2703(d), rather than a search warrant based upon probable cause. Currently, the Ninth Circuit is considering this very question in *United States v. Gilton*, No. 16-10109. This issue is covered more fully in Chapter Three.

E. Use of Court Seal on Warrants.

Title 28 U.S.C. § 1691 provides that "[a]ll writs and process issuing from a court of the United States shall be under the seal of the court and signed by the clerk thereof." The court seal should be placed over the judge's signature on search warrants.

In *United States v. Smith*, 424 F.3d 992, 1008 (9th Cir. 2005), the defendant argued that search and arrest warrants were void because neither warrant contained the seal of the court. The Ninth Circuit rejected this argument, holding that the magistrate judge's failure to use the court seal on the documents amounted only to a "technical violation of 28 U.S.C. § 1691." *Smith*, 424 F.3d at 1008. Because the court concluded there was no deliberate disregard of the rule (the magistrate judge merely forgot) and the defendant was not prejudiced (if the warrants were stamped, the search and seizure would have gone off without issue), it refused to grant the defendant any relief.

F. Incorporating Affidavit of Probable Cause.

In *United States v. Kahre*, 737 F.3d 554, 566 (9th Cir. 2013), the Ninth Circuit held that an affidavit in support of a search warrant may only be incorporated if "(1) the warrant expressly incorporated the affidavit by reference and (2) the affidavit either is attached physically to the warrant or at least accompanies the warrant while agents execute the search." (citation omitted).

Chapter Two

Obtaining Electronic Communications Under the Electronic Communications Privacy Act

I. Introduction

The Electronic Communications Privacy Act (ECPA), also known as the Stored Communications Act (SCA), located at Title 18, United States Code, Section 2701, *et seq*., governs the availability of information about those who subscribe to phone and computer services, including the content of their communications. That the statute is known variously as the ECPA and the SCA may give you some idea of the confusion it has sown.

Back in 2002, the Ninth Circuit decried the difficulties in interpreting this statute, drafted in 1986 (prior to the creation of the World Wide Web) and last amended in 2002, in light of advances in the technology of electronic communications, stating:

> Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results. . . . We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites such as Konop's will remain a confusing and uncertain area of the law.

See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002). Regardless of whether they refer to the statute as the ECPA or SCA, most courts and commentators agree that the statute is woefully out of step with today's technology.

This section of the guide is intended to focus upon issues which arise when the government seeks to obtain the contents of communications and other information from providers, including issues related to court orders for delayed notice and preclusion of notice. Issues related to the court's jurisdiction and extraterritoriality also will be addressed.

II. Types of Information the Government Can Obtain under the ECPA/SCA

A few definitions will assist our discussion.

Electronic Communication Service: "Any service which provides to users . . . the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Electronic communication service providers include land and mobile telephone service providers and Internet service providers such as Google, Yahoo and Microsoft.

Subscriber: An individual or organization that has opened an account with a telephone service provider or Internet service provider. A subscriber is similar to a user, which is defined as "any person or entity who . . . uses an electronic communication service and . . . is duly authorized by the provider" to engage in such use. 18 U.S.C. § 2510(13).

Basic Subscriber Records: Basic subscriber records include a customer's name and address; telephone call records, including the time and duration of calls; length of service including the start date for the account and types of service provided; telephone number or other subscriber number or identity, including temporarily assigned network addresses, and method of payment, including credit card or bank account numbers. 18 U.S.C. § 2703(c)(2). Basic subscriber records include neither the content of communications nor other information about a subscriber such cell site location data or logs of account usage.

Other Subscriber Information: These records include transactional records, such as logs recording account usage and email addresses of individuals with whom the customer has corresponded. They can also include historical cell site data, which may disclose, with varying degrees of accuracy, the physical location of the caller in the past. They do not include the content of communications. 18 U.S.C. § 2703(c)(1).

Content: Any information about the substance, purpose or meaning of a wire, oral or electronic communication. 18 U.S.C. § 2510(8).

Public Service Provider: A person or entity that provides an electronic communication service to the public. *See* 18 U.S.C. § 2702(a).

Private Service Provider: A person or entity that provides an electronic service privately to a limited group, an example would be a large organization that provided Internet access to its networked employees.

III. General Limitations on Government Seizure of Personal Information Pursuant to the ECPA/SCA

As noted above, an "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Consequently, electronic communication

service providers include land and mobile telephone service providers and Internet service providers. The ECPA/SCA differentiates between public and private service providers and between content, subscriber information and other information pertaining to a subscriber.

Public providers of electronic communications services may not disclose the *content* of electronic communications to any person or entity except as authorized by law. *See* 18 U.S.C. § 2702(a)(1) and (2).

Subscriber information and other information pertaining to a subscriber is treated differently from content and from each other. The ECPA/SCA prohibits public providers from disclosing subscriber information of any kind (basic subscriber and other subscriber information) to government entities. *Id.* § 2702(a)(3). It is important to note that the prohibition applies *only* to disclosures to the government.

It is ironic that a statute purporting to protect privacy only applies to the government. The ECPA/SCA expressly authorizes public providers to provide basic subscriber and other subscriber information (excluding content) to "any person other than a governmental entity." *Id.* § 2702(c)(6). There is nothing in the statute that prevents a public provider from providing subscriber information for free or for a fee to marketers and data aggregators all looking to sell you something. Governmental entities may only obtain information from public providers through the mechanisms provided within the ECPA/SCA, or when the subscriber consents, when the provider makes the disclosure to protect the provider's interests, when there is an emergency (but it is the provider, not the government, who must believe that there is an emergency) or when required by 18 U.S.C. § 2258A (pertaining to child molestation and child pornography).

Public providers may disclose contents of communications through the mechanisms provided within the ECPA/SCA or pursuant to the wiretap laws. *See* 18 U.S.C. § 2510, et seq. Public providers also may disclose the contents of communications when sought by the addressee or intended recipient of the communication; there is consent of a party to the communication; there is an emergency (under the same rules as above); anyone authorized to facilitate the communication requests; as necessary to protect the provider; as required by 18 U.S.C. § 2258A; or, when sought by a law enforcement agency, if the contents were

inadvertently obtained by the provider and appear to relate to the commission of a crime. 18 U.S.C. § 2702(b).[1]

IV. Obtaining Basic Subscriber Information

Using a grand jury subpoena, an administrative subpoena authorized by federal or state law, a trial subpoena, a court order pursuant to the ECPA/SCA § 2703(d), or a warrant, a governmental entity may obtain basic subscriber information. This includes a subscriber's name, address, local and long distance telephone connection records or records of session times and durations, length of service and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service. 18 U.S.C. § 2703(c)(2). The governmental entity receiving non-content records or information is not required to notify the subscriber. § 2703(c)(3).

This is relatively non-controversial. Even if the government uses an overbroad subpoena and the provider fully complies, there is no suppression remedy authorized under the statute. The provider is immune from civil suit for compliance with a defective subpoena, order or warrant. *See* § 2703(e). A provider may be sued for other knowing or intentional violations of the statute, such as providing content without process and without a valid exception. § 2707(a). Although the government cannot be sued absent a "willful" violation under § 2712, a complicit government employee may be subject to a mandatory disciplinary investigation. § 2707(d).

It is not uncommon for the government to include in an application for a pen register and trap and trace, a request for basic subscriber information for the target telephone and for subscribers called by or who have called the target telephone. Typically, those applications reference not only to the pen/trap statute, 18 U.S.C. §3122, but also the ECPA/SCA, 18 U.S.C. § 2703(c)(2). Inasmuch as neither requires a showing beyond likely relevance to an ongoing criminal investigation, there

[1] In keeping with the theme of selective privacy, the ECPA/SCA does not prohibit **private providers** from disclosing subscriber information and the contents of its users' communications to anyone. In § 2702, the section dealing with voluntary disclosures of subscriber information and content, Congress carefully prescribed the reach of that section to providers of services to the public. In § 2703, the section dealing with how the government may force disclosure of information from providers, Congress refers to electronic communication service providers generally which, as defined earlier, includes private providers. This means that a private provider can voluntarily disclose anything it wants, including content, to anyone it wants, including the government. If the government wants to compel the information, however, it must use the mechanisms of the statute.

appears nothing inherently wrong with the practice and it provides efficiency for the government. Be wary, however, as sometimes the subscriber information requested in these applications goes beyond the basic subscriber information authorized at § 2703(c)(2); compelled disclosure in this instance may be inconsistent with the law.

V. Obtaining Other Information About a Subscriber

The government can obtain records pertaining to a subscriber, beyond basic subscriber information but short of content, by means of an application based upon specific and articulable facts under § 2703(d). "Other information" about a subscriber can include historical cell site data. § 2703(c)(1). *See Tracking Warrants and Geolocation Data, infra,* Chapter Three. The government is not required to notify the subscriber and may seek an order precluding the provider from notifying its subscriber under § 2705(b) as discussed below. This is one of the typical "(d)" orders that magistrate judges will see. It is mentioned here because under certain circumstances, as discussed below, a § 2703(d) order can be used in some courts to obtain content.

VI. Obtaining Content of Electronic Communications

In § 2703(a), the ECPA/SCA provides that the government may obtain from the service provider the contents of an electronic communication which has been in electronic storage for less than 180 days with a warrant supported by probable cause. No notice to the subscriber by the government is required and the government may preclude the provider from notifying its subscriber of the warrant.

The content of communications which have been in storage more than 180 days can be obtained with a warrant, a court order under § 2703(d) or a subpoena. Use of a (d) order or a subpoena requires prior notice by the government to the subscriber, although notice can be delayed, as described below.

In *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), however, the Court of Appeals for the Sixth Circuit rocked the world of federal prosecutors by finding the ECPA/SCA unconstitutional to the extent that it provided that contents of the communications, regardless of their vintage, could be obtained from the provider upon less than probable cause. As a consequence, most but not all U.S. Attorney's Offices use warrants, rather than subpoenas or orders pursuant to § 2703(d), to obtain contents of communications from service providers. Perhaps due to the decreased use of non-warrant process to obtain content, no other Circuit has ruled upon the issue.

Search warrants directed to service providers usually require the production to the government of the entire contents of a particular email account. The warrant then restricts the government's search of the contents for specific information prescribed in the warrant. Questions have arisen regarding the propriety of seizing the entire account; requiring the provider to do some filtering; requiring the government to use a preapproved search protocol (i.e. identifying in advance specific key words), and requiring sealing, return or destruction of the non-relevant information. The case law in our Circuit derives from considerations of the advisory protocols articulated in *United States v. Comprehensive Drug Testing, Inc. (CDT),* 621 F.3d 1162, 1176 (9th Cir. 2010)(en banc)(per curiam). All but one of our district courts have declined to require the *CDT* guidelines in search warrants for electronic communications to service providers. *See, e.g., United States v. Lustig*, 2014 WL 940502 *14 (S.D. Cal. March 11, 2014). *But see, In the Matter of United States of American's Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius,*770 F. Supp.2d 1138 (W.D. Wash. 2011).

VII. Notice to the Subscriber of Government Action

A. Delayed Notice to the Subscriber by the Government

The ECPA/SCA provides that the government is required to give prior notice to a subscriber when the government is seeking to obtain contents of communications using either a subpoena or a court order pursuant to § 2703(d). No notice by the government to the subscriber is required if a search warrant is obtained for the contents of communications. § 2703(b)(1)(A).

Required notice to the subscriber by the government may be delayed for renewable 90 day periods. If the government is seeking disclosure of contents using a court order under § 2703(d), the court is required to delay notice upon a determination that notification of the existence of the order may endanger the life or physical safety of an individual, may result in flight from prosecution, destruction or tampering with evidence, witness intimidation or otherwise seriously jeopardize an investigation or unduly delay a trial. § 2705(a)(1)(A), (2). If the government is using a subpoena to obtain the contents, notice to the subscriber may be delayed upon the execution of a written certification of a supervisory official that one or more of the adverse results mentioned above may obtain. § 2705(a)(1)(B).

B. Preclusion of Notice to the Subscriber by the Service Provider

Section 2705(b) governs preclusion of notice to the subscriber by the service provider. It provides that a governmental entity seeking information under § 2703

may seek an order commanding the provider not to notify any person of the existence of the subject subpoena, court order or warrant. The preclusion order may remain in effect "for such period as the court deems appropriate...." § 2705(b). When it uses a search warrant, the government is not required to provide notice to a subscriber that the contents of his or her account have been seized. §2703(b)(1)(A). Rule 41(f) only requires that the warrant be served and an inventory and receipt provided to the person from whom the property was taken – the service provider.

Many service providers, however, are contractually obligated or inclined to notify their subscriber about the service of a warrant or other process. The ECPA/SCA, however, provides that in connection with warrants for the content of electronic communications from service providers, the government may obtain, upon a proper showing of the likelihood of adverse consequences, an order precluding the provider from notifying its subscriber of the warrant. 18 U.S.C. § 2705(b).

Most such warrants include a request for the preclusion order. Most such orders provide for preclusion "until further order of the court" which may mean, in reality, never. Some courts are requiring renewable time limits on preclusion, as with warrants requesting delayed notice (tracker warrants, for example). *See Order Denying Motion Pursuant to 18 U.S.C. § 2705(b), In the Matter of the Search Warrant For: [Redacted]@hotmail.com,* 2014 WL 7801298 (N.D. Cal. November 25, 2014) (M.J. Grewal). The court must issue the preclusion order if it determines that there is reason to believe that notice will endanger the life or safety of an individual, flight from prosecution, destruction or tampering with evidence or otherwise seriously jeopardize an investigation or unduly delay trial.

Most recently, Magistrate Judge Frederick F. Mumm of the Central District of California ruled that although § 2705(b) allows for an order precluding a service provider from notifying a subscriber of the existence of a warrant in perpetuity, such orders violate the service provider's First Amendment rights. *In the Matter of the Search Warrant for [redacted].com,* No. 16-2316M (FFM), 2017 WL 1450314 (C.D. Cal. March 31, 2017). Judge Mumm found that the preclusion order is a prior restraint on speech and employing strict scrutiny found that requiring the government to set a time limit, which may be renewed as required, is a less restrictive alternative to the perpetual bar. *Id.* at *9-10.

The Pen/Trap statute, 18 U.S.C. § 3123(d)(2), requires that the provider not disclose the existence of the order to the subscriber or any other person unless and until ordered by the court. No showing of need is required, unlike the ECPA/SCA structure. Many courts now also require that these orders contain renewable time limits regarding non-disclosure.

VIII. Scope of Jurisdiction and Extraterritoriality

To obtain stored communications, the government must obtain a "warrant issued using the procedures described in the Federal Rules of Criminal Procedure...by a court of competent jurisdiction." 18 U.S.C. § 2703(a). The ECPA/SCA defines a federal "court of competent jurisdiction" as a U.S. district or appeals court that has jurisdiction over an offense being investigated, is in the service provider's district, or is acting on a request for foreign assistance under 18 U.S.C. § 3512. *Id.* § 2711(3). What this means is that magistrate judges in any district can issue warrants to service providers located in other districts. The ECPA/SCA is otherwise silent about its territorial reach or the reach of its warrant requirement.[2]

Recently, service providers have challenged whether § 2703(a) reaches content stored outside the United States. The main cases involve the service providers Microsoft and Google. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), *reh'g denied en banc*, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017); *See In re Search Warrant to Google*, No. 2:16-mj-960-JS-1, 2017 WL 471564, at *3 (E.D. Pa. Feb. 3, 2017). They reveal how Microsoft and Google routinely store data outside the United States. Microsoft transfers data associated with a customer's self-reported location to the server associated with that customer's country code and (at the time of the *Microsoft* decision) deleted most data sets in the United States. *Microsoft*, 829 F.3d at 202–03. Google's system automatically moves and stores data — in packets or component parts — in different locations (including different countries) in aid of overall network efficiency. *Google*, 2017 WL 471564, at *3. Both service providers can access the data from the United States, and the government served the warrants in both cases at the providers' U.S. headquarters. *Id.* at *4; *Microsoft*, 829 F.3d at 200. In cases involving Google, only personnel on Google's legal team in the United States are authorized to access and produce the content of communications, even if it is stored outside the United States. *Google*, 2017 WL 471564, at *4.

The Second Circuit is the only circuit court to consider the extraterritorial application of the ECPA/SCA. In *Microsoft*, it held that the ECPA/SCA did not apply outside the United States and Microsoft need not disclose user content stored in

[2] Rule 41(b)'s venue restrictions similarly limit its territorial reach generally to federal districts, sometimes allowing warrants for persons or property only in the issuing court's district and sometimes outside the district (but still in a federal district) in specified contexts. Fed. R. Crim. P. 41(b)(1)–(6). The 2016 amendments to Rule 41 — which allow warrants to issue in one district for searches of computers and media in other districts under certain circumstances — are discussed *infra* in Chapter IV.

Ireland. *Microsoft*, 829 F.3d at 201–02, 216–21. It applied the canon of statutory construction known as the presumption against extraterritoriality and analyzed the statute under the Supreme Court's two-step framework for analyzing whether a statute applies extraterritorially. *Id.* at 209–10; *see RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2100–01 (2016); *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1665–69 (2013); *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255, 261–70 (2010).

At step one, the inquiry is "whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially." *RJR Nabisco*, 136 S. Ct. at 2101. At step two, the court "determine[s] whether the case involves a domestic application of the statute . . . by looking to the statute's 'focus.'" *Id.* "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory." *Id.*

At step one in the *Microsoft* case, the government conceded — and the Second Circuit held — that § 2703 and its warrant provisions do not contemplate or permit extraterritorial application. *Microsoft*, 829 F.3d at 210–16. The Second Circuit thus moved to step two: whether the case involves a domestic application of the statute, which in turn depends on whether the conduct relevant to the ECPA/SCA's focus took place in or outside the United States. *Id.* at 216. It determined that the statute's focus was user privacy, rejected the government's contrary argument that the ECPA/SCA focused on "disclosure of content," and concluded that requiring Microsoft to disclose content stored in Ireland would be an unlawful extraterritorial application of the act. *Id.* at 216–21.

The government sought rehearing *en banc*, which the Second Circuit denied in a four-four decision. *See* 2017 WL 362765 (2d Cir. Jan. 24, 2017). The four dissenters generally concluded that disclosure of information from Microsoft's headquarters in the United States was a domestic application of the ECPA/SCA. *Id.* at *5–18 (four dissenters — Circuit Judges Jacobs, Cabranes, Raggi, and Droney — each wrote a dissent; each dissenter joined the others' dissents). Some of the reasons are as follows. Even if the ECPA/SCA's focus is privacy, the warrant requirement — with its attendant requirement of probable cause — protects privacy. *Id.* at *6 (Jacobs, J., dissenting). Moreover, an ECPA/SCA warrant is not a search warrant in the classic sense: the government does not search a location or seize evidence. Instead, the

conduct relevant to the focus — and what the ECPA/SCA seeks to regulate — is disclosure of the data in the service provider's possession. *Id.* at *10 (Cabranes, J., dissenting). The service provider — Microsoft — could access the information in the United States. "[I]f statutory and constitutional standards are met, it should not matter" where a service provider chooses to store the 1's and 0's. *Id.* at *6–7 (Jacobs, J., dissenting).

After the *Microsoft* denial of *en banc* review, magistrate judges have held that a disclosure by a provider who can access the data from the United States is a permissible domestic application of the ECPA/SCA. *See, e.g.*, *In the Matter of the Search of Content That is Stored at Premises Controlled by Google*, No. 3:16-mc-80263-LB, ECF No. 45 (N.D. Cal. Apr. 19, 2017); *In the Matter of the Search of Premises Located At Yahoo*, No. 6:17-mj-1238, ECF No. 12-1 (M.D. Fla. Apr. 10, 2017); *In re: Information associated with one Yahoo email address that is stored at premises controlled by Yahoo*, No. 2:17-mj-1234-WED, ECF No. 1 at 6–8 (E.D. Wis. Feb. 21, 2017); *In re Search Warrant to Google*, No. 2:16-mj-960-JS-1, 2017 WL 471564, at *9–14 (E.D. Pa. Feb. 3, 2017). In cases involving Google, courts have noted that the warrants are directed to it in the only place — the United States — where it can access and deliver the information that the government seeks. *Google*, 2017 WL 471564 at *4. And unlike *Microsoft*, where storage of information was tethered to a user's reported location, 829 F.3d at 203, there is no storage decision by Google. The process of distributing information is automatic, and in aid of network efficiency. *Google*, 2017 WL 471564 at *3, *12.

The issue is live: Google has objected to the decisions that disclosure is a permissible domestic application of the ECPA/SCA. The legal landscape will be clearer when we next go to press.

Chapter Three

Tracking Warrants and Geolocation Data

I. Introduction

The government often will seek court approval to track a suspect using electronic means. This guide breaks down these tracking applications into two categories: (1) tracking devices that the government has actually installed (*e.g.*, "slap-on" devices), and (2) devices that are carried voluntarily by a person and can be used as tracking devices when the government uses the device's technology to locate its whereabouts (*e.g.*, cell phones). Because there is clear guidance on the first category, this guide addresses that area first before it turns to the more controversial area of cellphone tracking.

II. Tracking Warrants and Rule 41

What is a "tracking device?" Rule 41(a)(2)(E) refers to the Electronic Communications Privacy Act's definition of a tracking device: "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b).

Are there jurisdictional limitations? A magistrate judge only has the authority to issue a warrant to install a device within the district in which the magistrate judge sits. Rule 41(b)(4). Once installed in the district, however, the device may be used to track the movement of the property within and outside the district.

What may be tracked? A tracking warrant may issue for property which is evidence of a crime, contraband, fruits of a crime, items illegally possessed, property designed for the use, intended for use or used in committing a crime, or a person to be arrested or who is unlawfully restrained. Rule 41(c).

Must a tracking device be "installed?" Government agents often want to access the GPS technology contained within a cell phone, a tablet computer or a car equipped with GPS technology to determine the location of the device and/or person under investigation. Rule 41(b)(4) of the Federal Rules of Criminal Procedure authorizes magistrate judges to issue a warrant "to install" within the district a tracking device; the warrant may authorize the use of the device within and outside the district. Rule 41(e)(2)(C)(ii), (iii) provides that the warrant must command the

officer to complete any installation authorized within 10 days and perform any installation authorized during the day. Rule 41(f)(2)(A) commands the officer executing a tracking device warrant to record the exact date and time the device was "installed" and the period during which it was used. Similarly, 18 U.S.C. § 3117(a) provides that if a court is empowered to issue a warrant or other order for the installation of a mobile tracking device it may order the use of the device within the jurisdiction of the court and outside the jurisdiction of the court if the device was installed in the court's jurisdiction. This language suggests that something tangible is "installed" into or onto something else at the request of the government. This begs the question whether ordering a service provider to force a cell phone to report its location to the provider is an "installation."

As mentioned above, a mobile tracking device is defined at 18 U.S.C. § 3117(b) as an electronic or mechanical device which permits the tracking of the movement of a person or object. This raises other questions: Is a cell phone, so long as it is powered on, always a mobile tracking device because it "permits" the tracking of a person or object? Or, does it only become a mobile tracking device when the government seeks to use it as such Read together, do § 3117(a) and (b) apply only to electronic or mechanical devices that the government may "install" or does it apply whenever the government intends to locate someone using that person's own property?

The majority of courts require a tracking warrant when the government seeks to compel a service provider to access the GPS technology in the subject device. The installation question appears to have been bypassed in these cases perhaps because it seems clear that causing the GPS in the phone to activate constitutes a "search" of the phone requiring a warrant based upon probable cause. Whether these warrants are "tracking warrants" that require use of the tracking warrant procedures or standard Rule 41 warrants are issues ripe for decision.

A. Tracking Warrant Procedures:

1) Obtaining a Warrant: Rule 41(d).

Legal Standard: Probable cause. *See United States v. Jones,* 132 S. Ct. 945 (2012). The agent(s) "seeking the warrant must demonstrate to the magistrate their probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense." *Dalia v. United States*, 441 U.S. 238, 255 (1979); *see also United States v. Rigmaiden*, 2013 WL 1932800, *19, No. CR 08–814–PHX–DGC (D. Ariz. May 8, 2013) (applying *Dalia*'s probable cause requirement to tracking warrant).

2) Tracking warrant requirements: Rule 41(e)(2)(C).

A tracking-device warrant must:

- Identify the person or property to be tracked,
- Designate the magistrate judge to whom the warrant must be returned, and
- Specify a reasonable length of time that the device may be used—not to exceed 45 days. The court may, for good cause, however, provide extensions for a reasonable period not to exceed 45 days each.

The warrant must command the executing officer to:

- Complete any installation of the device within a specified time, no longer than 10 days,
- Perform any installation during the daytime (between 6:00 a.m. and 10:00 p.m.), unless the judge for good cause expressly authorizes installation at another time, and
- Return the warrant to the judge designated in the warrant.

3) Executing and Returning the Warrant: Rule 41(f)(2).

- **Time:** The executing officer must note on the warrant the exact date and time the device was installed and the period during which it was used.
- **Return:** The officer executing the warrant must return it to the magistrate judge within 10 days after the use of tracking device has ended.
- **Notifying the person whose property was tracked:** Within 10 days after the use of the tracking devices has ended, the executing officer must serve a copy of the warrant on the person whose property was tracked, unless the court grants the government's request to delay notice.
- **Delayed Notice:** Upon the government's request, the judge may delay notice "if the delay is authorized by statute." Rule 41(f)(3). The court may delay notice if it finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result, as

defined at 18 U.S.C. § 2705(a)(2). 18 U.S.C. § 3103a(b)(1). Under § 3103a, law enforcement authorities must provide delayed notice within a "reasonable period not to exceed 30 days after the date of [the warrant's] execution" or, alternatively, "*on* a later date certain if the facts of the case justify a longer period of delay." 18 U.S.C. § 3103a(b)(3). This initial period can be extended "for good cause" upon "an updated showing of the need for further delay;" such extensions are "limited to periods of 90 days or less, unless the facts of the case justify a longer period of delay." 18 U.S.C. § 3103a(c).

III. GPS Tracking of Vehicle or Container

GPS stands for Global Positioning System, which is a collection of Earth-orbiting satellites. The system works like this: a GPS receiver, which is the actual, electronic tracking device attached or used, locates four or more of these satellites and computes the distance between itself and each satellite by analyzing high-frequency, low-powered radio signals from the GPS satellites. The GPS receiver then uses these combined calculations to determine its own location and can display or report the results. In addition to placing a person or object to which it is attached on a map at any particular location, it can also, in real-time, trace a person's or object's movement.

A. *United States v. Jones*, 132 S. Ct. 945 (2012)—Warrant required for attaching GPS device to vehicle.

In *Jones*, without obtaining a warrant, the government placed a GPS device on the defendant's Jeep and collected data about his movements for a 28-day period. The government later used this tracking data to show that he was distributing large amounts of cocaine. The defendant moved to suppress the GPS evidence as a warrantless search.

The government argued that it did not need to get a warrant under *Katz v. United States*, 389 U.S. 347 (1967) because the defendant had no reasonable expectation of privacy in the location of his car as it drove on public streets. After all, police would not need a warrant to put a 24/7 tail on the defendant's Jeep and record everywhere he went for that four-week period. A GPS did essentially the same thing, the government argued. The Court disagreed, but did not reach the *Katz* argument. Instead, the Court returned to its pre-*Katz* property-rights analysis and held that the government's unwanted physical intrusion onto the defendant's property—when the agents touched the undercarriage of the Jeep to attach the GPS unit—constituted a search within the meaning of the Fourth Amendment because it was a common-law

trespass to the defendant's property. Because the agent did not have a warrant, the evidence was suppressed.[3] *See United States v. Pineda-Moreno*, 688 F.3d 1087, 1090 (9th Cir. 2012) ("*Jones* holds that the government's installation of a Global Positioning System (GPS) tracking device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search' under the Fourth Amendment."); *United States v. Thomas*, 726 F.3d 1086, 1092-93 (9th Cir. 2013) (describing *Jones* as a "watershed" U.S. Supreme Court opinion that "changed the jurisprudential landscape by holding that [the reasonable-expectation-of-privacy test from *Katz v. United States*, 389 U.S. 347 (1967)] was not the exclusive rubric. . . ." for determining whether a search occurred under the Fourth Amendment).

IV. Geolocation Data: Tracking a Person by Phone Using Cell Phone Technologies

Geolocation refers to a variety of technologies law enforcement uses to determine the physical location of a cell phone. When a cell phone is on, it communicates virtually constantly with the cellular network at a level invisible to the user so that if a call is made or received, the network knows where to route the call. These records, however, are not logged or stored by the service provider. The trigger for logging and storing cell tower activations by providers is making or receiving a call. As required under the Communications Assistance of Law Enforcement Act ("CALEA"), 47 U.S.C. §§ 1001, et seq., service providers retain records of the cellular towers activated at the beginning and end of calls made or received. Some maintain records of all towers activated during the progress of a call. Records of cell tower activations, whether obtained historically or in real-time can be used to determine, with varying levels of accuracy, the location of the cell phone at the beginning and end and sometimes during a call. Most cell phones also contain GPS technology, allowing the cell phone to be located by satellite rather precisely provided that the phone is on and regardless of whether calls are made or received.

The state of the law regarding what the government needs to show to collect geolocation data is unsettled. There appears no question that a warrant is required to obtain GPS data from the phone through the service provider. GPS in phones is not always activated. It will activate for an emergency call or if the user otherwise

[3] Notably, the *Jones* Court distinguished two prior tracking cases, *United States v. Knotts*, 460 U.S. 276, 281 (1983) and *United States v. Karo*, 486 U.S. 705 (1984). In those cases the Court held that the government did not conduct a search (and therefore did not need to obtain a warrant) when it placed "beepers" into containers with the then-owner's permission with the understanding that the government could track the object when the containers were transferred to the defendant. Unlike the cases involving third-party permission, the *Jones* Court reasoned the government did not have permission to touch the Jeep to install the device. *Jones*, 132 S. Ct. at 952.

causes the GPS to report its location. For real-time cell site data, which is reported to and logged by the provider whenever a call is made or received, a majority of courts require probable cause to obtain the real-time cell site data. For historical cell site data, most courts do not require a warrant based upon probable cause. Instead, these courts require the lesser showing of "specific and articulable facts showing that there are reasonable grounds to believe" the data is "relevant and material to an ongoing criminal investigation" under 18 U.S.C. § 2703(d). A minority of courts appear to require the lesser showing for both types of data.

A. Methods of Cell Phone Geolocation: (in descending order of accuracy)

GPS Positioning: Determining the location of a cell phone by obtaining the GPS satellite data which a GPS-enabled cell phone transmits. It works best in open areas and less well in urban areas. It can be very accurate regarding ground position but will not disclose vertical height.

WiFi Positioning: Determining the location of an internet-capable cell phone by assessing the signal strengths from the cell phone to nearby wireless internet access points (WiFi routers) of known location. It often is used in dense urban areas that can disrupt GPS satellite signals. It can be accurate to the extent of identifying a specific room or floor within a building.

Triangulation: Determining the location of a cell phone by comparing the relative signal strength it maintains with one or more cell towers. The more towers the cell phone is communicating with, the more accurate the location. Triangulation is the least intrusive method, as it does not require any special technology on the cell phone itself. Accuracy can approach that of GPS, but varies by number of cell towers within range, being most accurate in cities and least accurate in rural areas. Also it is subject to load balancing by the provider so that, due to volume, a given call will not be routed through the nearest cell tower.

Assisted GPS: Modern cell phones often combine these geolocation methods to produce faster, more accurate results. This is often known as assisted GPS, A-GPS, or hybrid positioning system (not to be confused with "hybrid theory," which is a legal argument).

B. Real-Time Cell Site Location Data

1. In the Ninth Circuit

The Ninth Circuit has not yet ruled on whether a warrant based upon probable cause is required to obtain real-time cell site location data. A district court opinion,

however, *United States v. Espudo*, 954 F. Supp. 2d 1029 (S.D. Cal. 2013) is on-point, relatively recently decided, and extensively discusses the relevant issues.

- ***Espudo's* Probable Cause Analysis:** The *Espudo* court determined that a warrant to obtain real-time cell site location data may only be granted if the government makes a showing of probable cause. *Espudo*, 954 F. Supp. 2d at 1043. Because no statute regulates real-time cell site location data, the court found that the terms of Rule 41 govern. *Id.* at 1043.

- ***Espudo's* Stored Communications Act Analysis:** The court found that 18 U.S.C. § 2703(d) did not apply because the SCA regulates access to records and communications in storage. Real-time cell site data is not stored data. *Id.* at 1036-37.

- ***Espudo's* Hybrid Theory Analysis:** This theory argues for statutory authority to obtain real-time cell site location data using a combination of the SCA and the Pen/Trap statute in order to circumvent the requirements of CALEA. *Id.* at 1037. This argument, if accepted, would allow the government to obtain real-time cell site location data on the SCA's lower showing of specific and articulable facts demonstrating relevance and materiality to an ongoing criminal investigation.

The court rejected the hybrid theory for the following reasons:

- A "significant majority" of courts around the country have rejected this theory. *Id.* at 1038.

- There is nothing in the relevant statutory language that would suggest the court may combine SCA with the Pen/Trap statute. *Id.* 1040.

- Such reading together of the SCA and the Pen/Trap statute runs afoul of CALEA. "[W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . call-identifying information shall not include any information that may disclose the physical location of the subscriber...." 47 U.S.C. § 1002(a)(2). "As cell site location data would disclose the physical location of a subscriber, CALEA clearly prohibits the government from obtaining it

solely on the authority of the Pen/Trap statute." *Espudo*, 954 F. Supp. 2d at 1039.

2. Majority Opinion Nationwide

A warrant to obtain real-time cell site location data may only be granted if the government makes a showing of probable cause. *Espudo*, 954 F. Supp. 2d at 1035; *see, e.g., In re App. of U.S. for an Order Authorizing Disclosure of Location Information*, 849 F. Supp. 2d 526, 539–42 (D. Md. 2011) ("Thus . . . the Fourth Amendment requires that the government must show probable cause prior to accessing such [location] data."); *United States v. Powell*, 943 F.Supp.2d 759, 768-771 (E.D. Mi. 2013) (a specific showing of probable cause must be made - that is, the user and use of phone must be in connection with illegal activity in area where suspected activity takes place); *In re App. of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 2006 WL 2871743 at *5, No. 06-MISC-004 (E.D. Wis. Oct. 6, 2006) ("I find that cell site information should be obtained under Fed. R. Crim. P. 41 and § 3117(b), or § 2518, rather than the Pen/Trap statute coupled with the SCA."); *In re App. of the U.S. for an Order Authorizing the Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone*, 2006 WL 6217584 at *3, Misc. No. 06–0186, 187, 188 (D.D.C. Aug. 25, 2006) ("the Court agrees with what is thus far the majority view that prospective cell site geolocation information is available upon a traditional probable cause showing under Rule 41"); *United States v. Myles*, 2016 WL 1695076 at *6, No. 5:15-CR-172-F-2 (E.D.N.C. April 26. 2016) (recognizing that majority of federal courts have held that there is a reasonable expectation of privacy in real-time cell phone location data – also good faith exception to exclusionary rule applicable to violations);

3. Minority Opinion Nationwide

A minority of federal courts allow the government to obtain real-time cell site information on a showing that is less than probable cause. *See, e.g., In re App. of U.S. for an Order for Prospective Cell Site Location Info.*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (concluding that the Pen/Trap statute and SCA may be read together to permit the disclosure of prospective cell site information on a showing lower than probable cause); *In re App. of U.S. for an Order*, 411 F. Supp. 2d 678, 682 (W.D. La. 2006) (request for prospective cell site information granted upon showing of "specific and articulable facts demonstrating reasonable grounds to believe that the information sought . . . is relevant and material to an ongoing criminal investigation"); *United States v. Booker*, 2013 WL 2903562 (N.D. Ga. 2013) (recognizing that there are "still several court opinions that have expressly approved of the practice" of obtaining

prospective cell site information under the SCA and Pen Register Statute); *In re App. of the U.S. for an Order for Disclosure of Telecomm. Records*, 405 F. Supp. 2d 435, 448 (S.D.N.Y. 2005) ("Section 2703 [of the SCA] is an appropriate mechanism to 'combine' with the Pen Register Statute").

C. Historical Cell Site Data Applications

So far, the Courts of Appeals have uniformly held that the government may obtain historical cell-site location data of a cellphone under the SCA's "specific and articulable facts" standard. *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013); *United States v. Davis*, 785 F.3d 498, 513 (11th Cir. 2015) (*en banc*). Both the Fifth and Eleventh Circuits reasoned that prior U.S. Supreme Court's decisions—*United States v. Miller*, 425 U.S. 436 (1976) (holding that bank customer has no reasonable expectation of privacy in bank records subpoenaed by the government) and *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that a customer has no reasonable expectation of privacy in business records compiled by the telephone company)—were controlling. Under this line of Supreme Court authority, the Fifth and Eleventh Circuits ruled that a cellphone user cannot harbor a reasonable expectation of privacy in information he voluntarily transmits to a service provider and the service provider memorializes as business records. *In re U.S. for Historical Cell Site Data*, 724 F.3d at 612; *Davis*, 785 F.3d at 507-509, 511-13. The Fifth Circuit has also held that suppression of evidence is not a remedy for violations of the SCA. *See, United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014). The Fourth and Sixth Circuit are also in accord: *United Sates v. Graham*, 846 F.Supp.2d 384, 389 (4th Cir. May 31, 2016) (*en banc*) (On rehearing *en banc*, the Fourth Circuit vacated the panel opinion, and, siding with the "majority of courts," found that defendants did not have expectation of privacy in historical CSLI); *United States v. Carpenter*, 819 F.3d 880, 884 (6th Cir. 2016) (rejecting argument that the government's collection of business records containing CSLI constituted a search under the Fourth Amendment).

The Ninth Circuit heard argument on the issue in *United States v. Gilton,* No. 16-10109, on March 17, 2017. In the underlying case, the district judge found that a warrant based upon probable cause is required to obtain historical cell site data but refused to suppress the evidence based upon good faith. *See United States v. Williams,* No. 13-cr-0764-WHO, 2016 WL 492934 (N.D. Cal. 2/9/2016). Only the Northern District of California, so far, has taken this position. *See United States v. Cooper*, 2015 WL 881578 at **6-8, No. 13-cr-00693–SI–1 (N.D. Cal. March 2, 2015); *In re: Application for Telephone Information Needed for a Criminal Investigation*, 119

F. Supp. 3d 1011, 1025 (N.D. Cal. 2015); *United States v. Alvarez,* 2016 WL 3163005 at *3, No. 14-cr-00120-EMC (N.D. Cal. June 3, 2016).

Six states have legislated privacy protections for historical cell site location information. "Colorado, Maine, Minnesota, Montana, Tennessee, and Utah have passed statutes expressly requiring law enforcement to apply for a search warrant to obtain this data." *In re Application for Telephone Information Needed for a Criminal Investigation*, 119 F.Supp.3d 1011, 1026-27 (N.D.Ca. 2015) ("Passive generation of CSLI by user does not amount to voluntary conveyance under the third party doctrine.).

Chapter Four

Search Warrants for Computers and Mobile Devices

I. 2016 Amendments to Rule 41

On April 28, 2016, the Supreme Court transmitted proposed changes to Rule 41 to Congress, pursuant to the Rules Enabling Act.[4] Because Congress failed to act upon the proposed changes, the changes became effective on December 1, 2016. Although amendments are often used merely to clean up technical issues, the 2016 amendments formally added Rule 41(b)(6), authorizing magistrate judges to issue remote access digital warrants, commonly known as Network Investigatory Techniques ("NIT") Warrants.

Rule 41(b)(6) provides:

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> > (A) the district where the media or information is located has been concealed through technological means; or
> >
> > (B) in an investigation of a violation of 18 U.S.C.§1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Thus, Rule 41(b)(6) now allows a magistrate judge in one district to issue warrants to search computers in other districts, under certain circumstances. Rule 41(b)(6) specifically permits these extraterritorial searches if the magistrate judge is located in a district where activities related to the crime have occurred and the district where the "media or information is located has been concealed through technological means." Rule 41(b)(6)(A). The magistrate judge may also issue these warrants when the investigation relates to allegations that someone has knowingly caused malware to be distributed over the Internet for the purpose of intentionally causing damage to a protected computer. Rule 41(b)(6)(B).

[4] 28 U.S.C. §§ 2071-77.

These amendments are not without controversy. The new rule does not require the traditional showing of "particularity" when describing the thing or place to be searched because, indeed, the government cannot do so. This failure risks improper invasions of privacy because the rule does not build in specific oversight by the court of which computer will be searched, or where the specific computer is located. Likewise, the real-time nature of the searches seems to lack safeguards, such as those required by similar searches under Title III wiretaps, which require a showing that other investigatory efforts have been exhausted before resort to the remote access search.

The Rule 41 amendments also raise concerns that they allow for the possibility of forum shopping. Under the new Rule, law enforcement agents may be able to seek the warrant in the most amenable district. Finally, as is always the case, the warrant will be issued ex parte with information being provided only by the government. This is troubling based upon the unique privacy risks at issue and is further complicated by the highly technical issues that may be challenging for some judges to understand.

A. Emerging Issue: NIT Warrants

At the current time, NIT warrants appear to be used by the government most frequently in cases involving (1) locating the source of computer malware, (2) child pornography cases where distribution is accomplished using the The Onion Router ("Tor") Network,[5] and (3) personal threats routed through anonymizing routers, thereby hindering the government's ability to pinpoint the location of the target.

NIT warrants are executed by the government delivering malware to the target computer, and become effective when the user accepts the malware. One way of accomplishing this is to send an email to the suspect account, with a link and a description to lure the suspect into downloading it, by clicking on the link. This is often referred to as "phishing" and is generally targeted to specific individuals.[6] Another way to accomplish this is to attract Tor users to a "watering hole":

---

[5] The Tor network provides anonymity to individuals sending messages by hiding and replacing typical IP addresses with a Tor-based address which consists of a series of alphanumeric characters followed by ".onion". The transmission on the Tor network provides an encryption actuated by sending it through a series of Tor routers (or nodes) each of which changes the IP address of the sender. The Tor network also provides anonymity to individuals who run websites or forums on it. Websites may be set up on the Tor network as "hidden services" that may only be accessed through the Tor network. A hidden service functions much like a regular website except that its IP address is hidden. Thus there is no way to look up the IP address of the computer hosting a hidden service. *U.S. v. Johnson,* No. 15-00340-01-CR-W-GAF, 2016 WL 6136586, at *1 n.2 (W.D. Mo. Oct. 20, 2016).

[6] Mayer, Jonathan, "Constitutional Malware" (Nov. 14, 2016) at 13, Available at SSRN:https://ssrn.com/abstract+2633247 (hereinafter "Mayer").

> 'Dark web' communities . . . facilitate illicit activity and are only accessible to Tor users .... Once the government has identified the hidden service operator and seized the infrastructure, it continues the service's operation – but with the addition of malware. When criminals interact with the website under certain triggering conditions – by visiting or logging in ..., for example the malware is delivered. Thus, unlike a phishing attack, this type of 'watering hole' attack is *not* targeted at specific individuals. Rather, it is targeted at *any* individuals who engage in *specific behavior*.

Mayer at 13-14.[7] Once the malware is activated, it retrieves the information it was designed to obtain and transmits it back to law enforcement.

In 2013, Magistrate Judge Stephen Wm. Smith, from the Southern District of Texas, was confronted with a request from the government to authorize a government hack into a computer suspected of being used to violate the bank fraud, identity theft, and computer security statutes. The government identified an email account, but otherwise did not know the computer being used or the location of the computer. The software that the government sought to install on the computer by means of the user opening the email was designed to extract certain ESI and to generate user photographs and location information over a 30-day period.

Judge Smith rejected the warrant request in *In re Warrant to Search a Target Computer,* 958 F.Supp.2d 753 (S.D. Tex. 2013). He concluded that the warrant request violated the venue limitations in Rule 41(b) and the "particularity requirements" of the Fourth Amendment. As to the particularity requirement, the government assumed that only the person who opened up and accessed the suspected email account would receive the government malware. Judge Smith opined that this was not necessarily the case in the age of spoofing, which could route the government's search through one or more "innocent" computers on its way to the target computer. In addition, if the computer was located in a public library, for example, or if the email was accessed by multiple people, the impact of the government's surveillance would not be limited to the defendants committing the crimes at issue.

[7] The watering hole strategy can impact large numbers of computers. In *U.S. v. Michaud,* No. 3:15-cf-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016), the court noted that the FBI "may have anticipated tens of thousands of potential suspects" in a child pornography investigation using the watering hole strategy.

1. Pre-Amendment Venue Concerns

Judge Smith's reasoning on venue was followed, in large part, by most courts considering NIT warrants prior to the 2016 Rule 41 amendments.[8] In 2015, the FBI tracked down and took over a website for child pornography, accessible only through the Tor network. Rather than immediately shutting it down, the agents ran the site for a two-week period to identify and ultimately prosecute users of the website. The site was operated from a facility in the Eastern District of Virginia ("Operation Playpen"), and the FBI sought and obtained a NIT warrant from a magistrate judge in the Eastern District of Virginia. The NIT warrant authorized the transmission of a computer code to those who accessed the website in question. The computer code then generated a communication from those users' computers to the government-operated server in the Eastern District of Virginia, containing various identifying information, including the users' IP addresses. *See U.S. v. Levin,* 186 F. Supp. 3d 26 (D. Mass. 2016).

As noted above, prior to the 2016 amendments, most courts considering the limitation restrictions in Rule 41(b) concluded that this would exceed the authority granted in Rule 41(b). Indeed, after reviewing the existing limitations on the "Authority to Issue a Warrant" provisions of the then-existing Rule 41, the *Levin* court concluded "[t]oday, . . . no magistrate judge has the authority to issue this [Operation Playpen] NIT warrant." *Id.* at 37.[9]

If a NIT warrant is issued, but the warrant failed to comply with the geographical limitations of pre-amendment Rule 41, courts were faced with three alternatives: (1) holding that the NIT warrant issued by a magistrate judge violated Rule 41(b), but nonetheless concluding that suppression was not warranted; (2) determining the NIT warrant did not violate Rule 41(b), analogizing it to a tracking warrant, but also concluding that suppression was unwarranted; and (3) concluding that the NIT warrant violated Rule 41(b), holding that the warrant was void *ab*

---

[8] *But see U.S. v. Jean,* 207 F. Supp. 3d 920 (W.D. Ark. 2016); *U.S. v. Johnson,* No. 15-00340-01-CR-W-GAF, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016) (analogizing the NIT warrant to a "tracking device" authorized by Rule 41 (b)(4)). In addition, three cases from the Eastern District of Virginia have upheld the validity of a magistrate judge-issued NIT warrant, but those violated none of the territorial limitations set out in Rule 41(b) because the warrants at issue were authorized by a magistrate judge in the Eastern District of Virginia. *See, e.g.*, *U.S. v. Eure*, No. 2:16cr43, 2016 WL 4059663 (E.D. Va. July 28, 2016); *U.S. v. Matish*, 193 F. Supp. 3d 585 (E.D. Va. 2016); and *U.S. v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. 2016).

[9] The Court specifically held that while magistrate judges lacked the authority to issue a watering hole NIT warrant, district judges would not be so limited. *Id.* at 43. Note, as well, that this conclusion would not preclude a magistrate judge from issuing a NIT warrant for activities occurring in the district in which the magistrate judge sits. *See, e.g., U.S. v. Darby,* 190 F. Supp. 3d 520, 536 (E.D. Va. 2016).

initio, and ordering suppression as a remedy.[10] *See U.S. v. Austin,* No. 3:16-cr-00068, 2017 WL 496374 (M.D. Tenn. Feb. 2, 2017) for case summaries.

In his early opinion, Judge Smith noted that "there may well be a good reason to update the territorial limits of [Rule 41] in light of advancing computer search technology." *In re Warrant to Search a Target Computer,* 958 F. Supp. 2d at 761. This opinion was cited as one of the reasons to adopt the new Rule 41(b)(6).[11]

The Rule 41 venue amendments now permit magistrate judges to issue extra-district warrants,[12] as long as the issuing district is one in which "activities related to a crime may have occurred," *and* the actual district where the media is located has been "concealed through technological means." Presumably this would include any communications using the Tor network.

2. Fourth Amendment Concerns

Regardless of venue concerns, the Fourth Amendment is implicated by any request for a NIT warrant. The drafters of the Rule specifically noted the existence of unresolved Fourth Amendment concerns:

> The amendment does 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, leaving the application of this and other constitutional standards to ongoing case law development.

2016 Amendment Committee notes.

As in most Fourth Amendment cases, three issues predominate: (1) probable cause; (2) particularity; and (3) overbreadth. However, it is important to note that some courts have suggested in dicta that perhaps a NIT warrant to locate IP addresses might not even be necessary. In *U.S. v. Acevedo-Lemus*, No. SACR 15-

---

[10] Of particular interest, perhaps, is *U.S. v. Krueger,* 809 F.3d 1109 (10th Cir. 2016), in which the Tenth Circuit upheld a district court suppression order when a District of Kansas magistrate judge issued a search warrant for a search that took place in Oklahoma. In a concurring opinion, then Judge, now Justice, Gorsuch opined that a magistrate judge issued warrant in excess of limitations of the Federal Magistrates Act, 28 U.S.C. § 636, was like "no warrant at all." *Id.* at 1126. He further noted that district judges would not be so constrained, as the Federal Magistrates Act was not applicable to district judges. Because 28 U.S.C.§ 636(a)(1) authorizes magistrate judges to issue warrants within their districts authorized by the Rules, presumably this would incorporate the new Rule 41(b)(6). However, in a cryptic footnote, Judge Gorsuch reserved this specific issue for another day. *Id.* at 1119, n.2.

[11] See Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure, Congressional Research Service Report, Sept. 8, 2016 (hereinafter "CRS Report").

[12] But see discussion regarding U.S. v. Krueger, supra fn. 7.

00137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016), the court held that the defendant did not have an expectation that his IP address would remain private because he routinely disclosed it to his ISP provider, as well as to websites that he visited on the open Internet, including the Tor network. *See also U.S. v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016); *U.S. v. Matish*, 193 F. Supp. 3d 585 (E.D. Va. 2016).

Other courts have held that the focus on whether an IP address is protectable ignores what is happening in the execution of a NIT warrant. The NIT warrant sends malware to the target computer and obtains information from that computer, which then transmits it to the government. In *U.S. v. Darby,* 190 F. Supp.3d 520 (E.D. Va. 2016), the court rejected the argument that a warrant was not required because the defendant had no reasonable expectation of privacy in his IP address as too superficial an inquiry:

> The government does not address whether Defendant had a reasonable expectation of privacy in the other information gathered by the NIT, such as the type of operating system on Defendant's computer and his computer's Host name. But this piecemeal analysis of what this NIT was authorized to extract from Defendant's computer misses the mark. The NIT surreptitiously placed code on Defendant's personal computer that then extracted from the computer certain information. … In placing the code on Defendant's computer, the NIT gave the government access to the complete contents of Defendant's computer. The relevant inquiry is whether Defendant has a reasonable expectation of privacy in the contents of his personal computer, which was located in his home.

Id. at 528-29. Citing *Riley v. California,* 134 S. Ct. 2473 (2014), the court concluded that "if an individual has a reasonable expectation of privacy in the contents of his or her personal computer, as he or she does, and the deployment of the NIT invades that privacy, then the NIT is a search." *Id.* at 530. *See also U.S. v. Croghan,* No. 1:15-cr-48, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016).

a. Particularity and Overbreadth

The Fourth Amendment provides that no warrant shall issue unless it "*particularly describe[s]the place to be searched, and the persons or things to be*

seized." As noted in a recent Congressional Research Service report[13], there are several different iterations of the argument that NIT warrants fail the particularity requirement. First, if the government seeks to attach malware to every computer visiting a site (often a child pornography site on the Tor Network), a message is sent to governmental authorities with the actual IP address of the computer visiting the site (*i.e.,* a "watering hole" attack). CRS Report at 7. This will, according to critics, result in the government searching computers of people whom the government cannot identify, or describe, and as to whom it lacks probable cause.

A variation of the "watering hole" attack targets a specific email account, which could result in the email being forwarded to another person who, upon opening it, would find his or her computer being searched with no probable cause. This is a variation of the scenario described by Judge Smith in *In re Warrant to Search a Target Computer, supra. See* CRS Report at 7.

In the context of a botnet attack (the subject of the authorization in Rule 41(b)(6)(B)), critics have argued that this would also violate the particularity requirement as probable cause is supposed to require the establishment of probable cause as to each person or place to be searched. The scenario involved in a botnet attack often involves searching multiple computers with one warrant which would most likely have no particular information describing each computer to be searched or demonstration of probable cause as to each computer. CRS Report at 8.

Most challenges to particularity and overbreadth concerns have been rejected in the cases of watering hole NIT warrants that seek to identify IP addresses of users who have accessed the services on an offending website. Generally, these NIT warrants seek only IP addresses and other computer configuration information about computers accessing the prohibited sites. *See, e.g., Henderson, supra; Darby, supra; and Michaud, supra.*

However, in *In re Warrant to Search a Target Computer,* 958 F.Supp.2d 753 (S.D. Tex. 2013), the warrant that Judge Smith was asked to authorize permitted the government to remotely install software that would transmit more extensive data to the FBI, including all IP addresses used, Internet activity, user names and passwords, user profiles, browsing activity, email content, photographs, and chat messaging logs and documents. It also asked for prospective data over a 30-day monitoring period by activating a built-in camera, location coordinates for the computer's locations and accounting entries. Moreover, because the "lure" might also

[13] Richard M. Thompson, II, Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure, Congressional Research Serv. (Sept. 8, 2016) ("CRS Report").

be forwarded to other computers and due to the risk of spoofing causing computers other than the target computer to become infected with the government malware, Judge Smith held that the request failed the Fourth Amendment's particularity requirement. Generally, the more information sought by the remote access, the more rigorous the particularity requirement should be.

b. Probable Cause

Probable cause challenges have primarily arisen from concerns utilizing the watering hole and botnet attack warrants that sweep a large number of computers within its reach. Courts in cases challenging child pornography obtained from websites on the Tor network have generally rejected the challenges to probable cause. This is because the website involved in the cases hosted child pornography, and access to it required registering with the website. *See, e.g., U.S. v. Henderson,* No. 15-CF-00565-WHO-1, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *U.S. v. Darby,* 190 F. Supp.3d 520 (E.D. Va. 2016); *U.S. v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). Child pornography cases are somewhat simple in this regard, because possession and viewing creates criminal liability. But, what about websites where the possession of materials hosted and viewing is not always illegal? This was one of the concerns raised by opponents of the amendment, who argued that the dragnet approach of a NIT warrant could improperly impact researchers and journalists.[14]

3. Practical Considerations When Considering a Remote Access Warrant[15]

a. Is the NIT warrant necessary? Because of some of the difficulties and unknown consequences that can flow from the execution of a NIT warrant, is this the only or the best means to achieve the law enforcement objective?

b. What technical means were used to conceal the location of the targeted media or data? Before you can authorize the use of a NIT warrant that may locate a target outside your jurisdiction, a showing must be made that the actual location is concealed through "technological means."

---

[14] *See* CRS Report at 7.

[15] These practical considerations are largely taken from Judge Smith's 2016 presentation entitled "Remote Access Electronic Searches Under Rule 41(b)(6): A NIT-Picker's Guide," at the FJC's Workshop for Magistrate Judges, and from conversations with Judge Jonathan Feldman, a U.S. Magistrate Judge sitting in the Western District of New York.

c. **How does the NIT software work?** The government agents should be able to explain how the government malware will be triggered, and what information will be sent back to the government data collection site. Will the data collected be limited, for example, only to IP address site information? Why should collection of data other than simply the IP address be authorized by a NIT? How long will the "lure" be effective? Once activated, how long will it continue to collect data? What is the means to take down the data collection?

d. **What are the risks that the NIT software installation will damage the infected target computer or other computers that unwittingly become target computers?**

e. **How likely is the NIT software to target only those computers involved in a crime?**

f. **How long will it take to execute the search?**

g. **When and how will the NIT software be removed?**

h. **Does the application seek continuous monitoring over a period of time?**

i. **If this is an anticipatory warrant, is there probable cause to believe the triggering condition will target only computers involved in a crime?**

j. **What steps are being taken to minimize over-collection?**

k. **What is the effective date of the execution of the warrant?** A warrant generally has to be executed within 14 days. Does the running of this time operate from the signing of the warrant, or from the time the "lure" is taken by the target computer?

l. **Does activation of the lure on multiple occasions constitute multiple searches on the same warrant?**

m. **How does the government intend to comply with the warrant notice requirements? Who will receive notice?**

n. **Has main Department of Justice approved or been consulted about the warrant application?** The CCIPS provisions contain a set of protocols recommending that these powerful investigative tools be used sparingly, only in the most serious cases, and even then with careful safeguards.

o. **What steps can be taken to ensure that the search resulting from the warrant is limited to U.S. territory?** The authors of the rule make it clear that it was not intended to authorize extra-territorial searches, which could violate international law.

When struggling with some of these concepts, magistrate judges should expect to receive an explanation of the workings of the NIT warrant and the possible impacts on computers other than the target computer. In addition, one helpful suggestion is to direct the government to file a "log" of contacts, dating each contact, and filing an updated status log under seal with the magistrate judge who authorized the warrant. This log should then be turned over to the defense when discovery materials are due.

B. Emerging Issue: The Border Search Exception and Mobile Devices

In the era of the Travel Ban(s), issues relating to searches of mobile devices at the border are emerging.

Two cases define current Ninth Circuit law on border searches of digital devices. First, in *United States v. Arnold*, the Ninth Circuit held that reasonable suspicion is not needed to search "a laptop or other personal electronic storage devices at the border." *U.S. v. Arnold*, 533 F.3d 1003, 1008 (9th Cir. 2008). Five years later, the Ninth Circuit provided two standards for border searches of digital devices: (1) manual or routine searches of digital devices do not require any suspicion at all; and (2) forensic or non-routine searches of digital devices require "reasonable suspicion." *See U.S. v. Cotterman*, 709 F.3d 952, 967-68 (9th Cir. 2013) (*en banc*). *Cotterman* also explained that there is no extended border search where the mobile device was seized and never cleared to pass through the border because the individual never regained an expectation of privacy in the device. *See id.* at 961-62. Thus, no warrant is required so long as the device has not been returned to the individual, even if the device is moved to a location away from the border and the search is not conducted promptly. *U.S. v. Kolsuz*, 185 F. Supp. 3d 843, 851-52 (E.D. Va. 2016) (quoting *U.S. v. Stewart*, 729 F.3d 517, 526 (6th Cir. 2013); *see also id.* at 852 n.11 (finding that *Cotterman* concluded that a search of a laptop seized at the border and examined 170 miles away in a specialized lab was a border search

because the laptop was not cleared to pass through the border and that *U.S. v. Feiten*, No. 15-20631, 2016 WL 894452, at *2 (E.D. Mich. Mar. 9, 2016), held that an off-site, month-long forensic search of a laptop was a border search).

District courts in the Ninth Circuit have noted that the Supreme Court's decision in *Riley v. California*, 134 S. Ct. 2473 (2014), which held that police must get a warrant before searching a cell phone seized incident to an arrest, is not irreconcilable with the Ninth Circuit's decision in *Cotterman*. *U.S. v. Caballero*, 178 F. Supp. 3d 1008, 1018-19 (S.D. Cal. 2016); *U.S. v. Ramos*, 190 F. Supp. 3d 992, 1001-03 (S.D. Cal. 2016); *U.S. v. Mendez*, No. CR-16-00181-001-TUC-JGZ (JR), 2017 WL 928460, *2 (D. Az. Mar. 9, 2017). As such, some district courts have concluded that the border search is an exception to *Riley's* warrant requirement. *Caballero*, 178 F. Supp. 3d at 1019; *Ramos*, F. Supp. 3d at 1003; *U.S. v. Mendez*, No. CR-16-00181-001-TUC-JGZ(JR), 2017 WL 928460, at *3 (D. Az. Mar. 9, 2017). District courts outside of the Ninth Circuit have also held that a warrant is not required to search a cell phone after a person has been arrested at the border. *U.S. v. Molina-Isidoro*, No. EP-16-CR-1402-PRM, 2016 WL 8138926, *6 (W.D. Tex. Oct. 7, 2016); *U.S. v. Kolsuz*, 185 F. Supp. 3d 843, 858 (E.D. Va. 2016). The Ninth Circuit has explained that "*Riley* did not address border searches, and expressly acknowledged that 'even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone.'" *U.S. v. Gonzalez*, 658 Fed. App'x 867, 870 (9th Cir. 2016). In *Gonzalez*, the Court found the government relied on the "well-established border search exception to the warrant requirement" in searching the defendant's cell phone without a warrant. *Id.*

In sum, despite *Riley v. California*, no warrant is required to search a mobile device at the border and no suspicion whatsoever is required to conduct a manual search of a mobile device at the border. However, reasonable suspicion must exist to conduct a *forensic* search of a mobile device at the border.

Chapter Five

Compelled Decryption and "Thumbpulsion"

I. Compelled Decryption

A. The All Writs Act

Under the All Writs Act, the court has the authority to order third parties to assist in law enforcement activities when "necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. 1651(a). Appropriate circumstances are those in which the third party is in a position to frustrate the implementation of the order of the court or the administration of justice. *U.S. v. New York Telephone*, 434 U.S. 159, (1977). When deciding whether to exercise this discretion the court should consider: 1) the closeness of the relationship between the or entity to whom the proposed writ is directed and the matter over which the court has jurisdiction; 2) the reasonableness of the burden to be imposed on the writ's subject; and 3) the necessity of the requested writ to aid the court's jurisdiction. *Id*. at 174-178.

In two recent cases courts have come to differing decisions related to whether the All Writs Act can be used to order Apple, Inc., to assist the government to bypass the security of certain iPhones. In the Eastern District of New York, Magistrate Judge James Orenstein determined the court lacked the authority to order Apple's assistance. *See In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2016 WL 783565, at *5, 15–MC–1902 (JO) (E.D.N.Y. Feb. 29, 2016),

Judge Orenstein ruled that requiring Apple's assistance was not "agreeable to the usages and principles of law." Relying upon the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. §§ 1001-1010, Judge Orenstein held that CALEA, at least arguably, exempted companies like Apple from providing the type of assistance sought. CALEA prohibits law enforcement from requiring companies from decrypting any communication encrypted by a customer "unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." *Id.* § 1002(b)(3). CALEA also exempts "information providers" and other businesses, such as those that facilitate the transfer of communications for private networks, from having to assist law enforcement. *Id.* § 1002(c). Judge Orenstein said, "The absence from that comprehensive scheme of any requirement that Apple provide the assistance sought here implies a legislative decision to prohibit the imposition of such a duty. [Footnote omitted]. Thus, even

under the government's reading of the AWA, I would conclude that while the matter is a close call, the Application seeks an order that is not "'agreeable to the usages and principles of law.'" *In re Apple, Inc.*, at *12.

In this Circuit, Magistrate Judge Sheri Pym of the Central District of California, came to a different conclusion although without the benefit of full briefing. Relying only upon the government's *ex parte* application, Judge Pym ordered Apple to assist the FBI in unlocking an iPhone used by one of the suspected gunmen in the San Bernardino mass shootings. Judge Pym found the All Writs Act permitted the Court to order Apple's assistance and ordered Apple to provide technical assistance that would accomplish three tasks: "(1) it will bypass or disable the auto-erase function whether or not it has been enabled; (2) it will enable the FBI to submit passcodes to the [iPhone] for testing electronically via the physical device port, Bluetooth, Wi-Fi, or other protocol available . . . ; and (3) it will ensure that when the FBI submits passcodes to the [iPhone], software running on the device will not purposefully introduce any additional delay between passcode attempts beyond what is incurred by Apple hardware." *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus*, No. ED-15-451 (C.D. Ca. Feb. 16, 2016). The application was withdrawn by the government after full briefing but before a hearing.

In March 2017, the Third Circuit found that an All Writs Act order issued by a magistrate judge requiring the subject of a search warrant to produce his iPhone, his Mac Pro computer and two external hard drives in a fully decrypted state was a necessary and appropriate means of effectuating the original search warrant. *United States v. Apple Macpro Computer,* 851 F. 3d 238, 246 (3d Cir. 2017).

Procedurally, the case was complicated in that the appeal was from an order holding the subject in civil contempt and the subject may not have fully preserved his rights. *Id.* at 245-247. Nonetheless, the court of appeals considered and rejected the subject's assertion of his Fifth Amendment right against compelled self-incrimination. The court of appeals relied upon the "foregone conclusion" rule enumerated in *Fisher v. United States,* 425 U.S. 391, 411 (1976), to find that the testimonial aspects of the production – the existence, custody and authenticity of the evidence – were a "foregone conclusion" in the circumstances of this case. *Apple Macpro,* 851 F. 3d at 247-248. The Magistrate Judge, in issuing the decryption order, found that the government had custody of the devices; that the subject owned the devices prior to the seizure; and, that there were images of child pornography on the devices. *Id.* at 248. The court of appeals agreed that any testimonial component of

the production of decrypted devices added little or nothing to the information already in the possession of the government. *Id.*

In that regard, the court of appeals distinguished the Eleventh Circuit's contrary view in *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011,* 670 F.3d 1335 (11th Cir. 2012), finding that the testimonial aspects of production of decrypted devices survived where the government could not demonstrate that files existed on the drives and that the subject could access them.

B. Thumbprint Compulsion ("Thumbpulsion")

What is "thumbpulsion"? When the government requests, as part of a search warrant application, authorization for agents to compel a "thumbprint" from a suspect to unlock a cell phone. This issue has been addressed in several cases and law review articles.

The issue raises potential Fifth Amendment concerns by arguably compelling a criminal defendant to reveal incriminating information about himself. It is well established that any admission of incriminating information must be made without compulsion or inducement of any sort. *Haynes v. State of Washington*, 373 U.S. 503, 513-14 (1983); *see also United States v. Coutchavlis*, 260 F.3d 1149, 1158 (9th Cir. 2001). The cases and articles below examine the application of this doctrine to the issue of "thumbpulsion."

1. Cases

In one of the earlier decisions considering this issue, *Commonwealth v. Baust*, 89 Va. Cir. 267 (Va. Cir. Ct. 2014), the Virginia Court of Appeals found that requiring a target to press his thumbprint to a cell phone failed to implicate Fifth Amendment concerns. The court held that, "the thumbprint, like a key . . . does not require the witness to divulge anything through his mental processes." As such, no Fifth Amendment concerns arose.

In *State v. Diamond*, 890 N.W.2d 143 (Minn. Ct. App. 2017), the Minnesota Court of Appeals similarly held that an order compelling the defendant to provide his fingerprint to unlock his cell phone did not violate the Fifth Amendment. By ordering the defendant to provide a fingerprint, law enforcement did not require the defendant to "reveal his knowledge or speak his guilt." *Id.* at 150. A fingerprint compulsion order is distinguishable from ordering a suspect to decrypt a hard drive or produce a combination because it does not involve a level of knowledge or mental capacity. Thus, it is not considered testimonial.

In contrast, *In Re Application for a Search Warrant*, No. 17M081, 2017 WL 758218 (N.D. Ill. Feb. 16, 2017), the district court reached the opposite conclusion, finding a Fifth Amendment violation. After an exhaustive discussion of the application law, that court held: "By using a finger to unlock a phone's contents, a suspect is *producing* the contents on the phone. With a touch of a finger, a suspect is testifying that he or she has accessed the phone before… and that he or she currently has some level of control or relatively significant connection to the phone and its contents." Thus, the court denied the request for a fingerprint.

2. Commentary

Two law review articles also have analyzed this topic. In the first article, the author argues that fingerprint or other biometric compulsion ought to receive the same protection afforded by the Fifth Amendment to traditional testimonial evidence. If passwords of letters and numbers are entitled to constitutional protection, then its modern technological counterpart should be treated similarly. *See* Kara Goldman, *Biometric Passwords and The Privilege Against Self-Incrimination*, 33 Cardozo Arts & Ent. L.J. 211.

The article notes that the courts have not traditionally offered constitutional protection to the production of a fingerprint because it was used to identify individuals who were already suspected of violating the law, to tie the suspect to evidence used in a crime such as a gun or knife. The current purpose of obtaining a fingerprint has expanded this use two important ways: (1) the use of a fingerprint can be used as a direct link to communicative, as well as potentially incriminating, information, and (2) the fingerprint itself serves as a replacement for the traditional numerical or alphabetic password, which has received some Fifth Amendment protection from courts.

A second law review article argues that the standards under which law enforcement officials can obtain a fingerprint should be different depending on the context in which the fingerprint is being used. This article was critical of the *Baust* decision in particular, contending that the court overlooked the true purpose of the fingerprint compulsion, i.e., the revelation of incriminating evidence:

> "The Virginia court [*Baust*] correctly applied the case law from *Hubbell* and *Fisher* but applied it blindly. Instead of looking to the purpose of the fingerprint (a type of password), it simply looked at the physical act it was requiring the defendant to do. The court analogized compelling the defendant's fingerprint (to unlock his phone) to compelling a defendant to provide a writing exemplar or blood sample but rejected the comparison between a fingerprint

> and a password. The difference, the court found, was the lack of communication required--a defendant need not "communicate 'knowledge'" when using his fingerprint to unlock his phone. Not only did the court ignore the similar purpose of the fingerprint and the password, but it also rejected the motion to compel the password, while granting the motion to compel the fingerprint."

Matthew J. Weber, *Warning-Weak Password: The Courts' Indecipherable Approach to Encryption and the Fifth Amendment*, U. Ill. J.L. Tech. & Pol'y, Fall 2016, at 455, 471–72.

3. Conclusion

While the courts appear prepared to conclude that compelling a fingerprint does not implicate Fifth Amendment concerns, the law review articles are critical of these opinions for taking a superficial view of the consequences of these orders.

No consensus has yet emerged, but magistrate judges confronting this type of warrant have taken pains to ensure that there is probable cause that the device contains evidence and that the person being subjected to "thumbpulsion" is the owner or user of the device.

About The Authors

The Honorable Mitchell D. Dembin is a United States Magistrate Judge for the Southern District of California and serves as Chair of the Technology Subcommittee of the Magistrate Judges Executive Board. Prior to his appointment to the bench in 2011, he was an Assistant U.S. Attorney in San Diego and served as the Cybercrime Coordinator. Before that, he was the Chief Security Advisor for Microsoft Corporation, assisting Microsoft's business customers in creating and implementing strategic security plans. Prior to joining Microsoft, Judge Dembin was the president of EvidentData, Inc., a firm specializing in computer forensics, digital evidence and computer security. Judge Dembin served four different terms as an AUSA over 20 years in San Diego and in Boston, including six years as a supervisor. Judge Dembin's career started at the Securities and Exchange Commission in Washington, D.C. Judge Dembin is an accomplished musician and released his first CD of original music, entitled "Fat Man on Thin Ice," in 2013.

The Honorable Stacie F. Beckerman is a United States magistrate judge for the District of Oregon. She was appointed to the bench in 2015 after serving as the assistant U.S. attorney for the District of Oregon, prosecuting violent, white collar and environmental crimes. She has also served as an assistant attorney general in the Appellate Division of the Oregon Department of Justice, and as an adjunct professor at Lewis and Clark Law School. Prior to government service, Judge Beckerman was a litigator for many years at Skadden, Arps, Slate, Meagher & Flom LLP, where her practice focused on securities class actions, shareholder derivative actions, insurance defense and pro bono civil rights cases. She received her J.D. from Harvard Law School, graduating *cum laude* in 1998, and her undergraduate degree from the University of Iowa, graduating with highest distinction in 1995. Judge Beckerman currently serves on the Ninth Circuit Magistrate Judges Executive Board and the Ninth Circuit Pro Se Committee. She is the coordinator of her court's pro bono panel, participates as a Court Assisted Pretrial Supervision judge, and chairs a group of federal criminal practice stakeholders. Judge Beckerman serves on the board of Oregon Women Judges, the

local chapter of Oregon Women Lawyers, and the U.S. District Court of Oregon Historical Society.

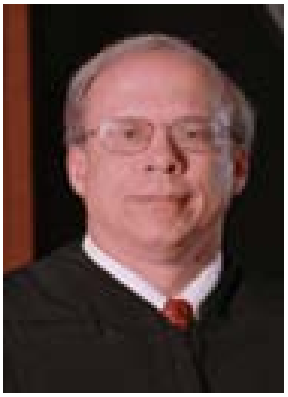
The Honorable Laurel Beeler is a United States magistrate judge for the Northern District of California. She was appointed to the federal bench in 2010 and has presided over and settled hundreds of cases in many practice areas. Judge Beeler was previously an assistant U.S. attorney in the Northern District, serving as deputy chief of the Criminal Division and as the professional responsibility officer. She is one of four national judicial liaisons to the Joint Electronic Technology Working Group formed by U.S. Department of Justice and the Office of Defender Services. She chairs the Northern District's Criminal Practice Committee and implemented the court's reentry and diversion courts. She previously served on the Ninth Circuit Jury Trial Improvement Committee. Judge Beeler received her J.D. from the University of Washington School of Law, where she was Order of the Coif and an articles editor on the Washington Law Review, and her A.B. with honors from Bowdoin College. She served as a law clerk to Judge Cecil F. Poole of the U.S. Court of Appeals for the Ninth Circuit. She also worked at the court as a staff attorney, serving as chief of the Civil Appeals Division. Judge Beeler teaches civil trial practice at University of California, Berkeley, School of Law and taught Criminal Procedure at U.C. Hastings College of the Law.

The Honorable Stanley A. Boone is currently a U.S. Magistrate Judge for the Eastern District of California, Fresno Division, appointed to the bench on December 31, 2012. Previously, he worked in the U.S. Attorney's Office, as White Collar Crime Chief and as an Assistant United States Attorney in the criminal section since 1996, prosecuting a wide variety of white collar crime and terrorism cases. During this time, Judge Boone held positions as misdemeanor unit supervisor, Elections Officer, Bankruptcy Fraud Coordinator and International Coordinator. From 2009 to 2010, Judge Boone was White Collar Crime Coordinator for the Executive Office for United States Attorneys, United States Department of Justice, in Washington, D.C. From 1989 to 1995, Judge Boone worked for the Office of United States Trustees as a paralegal specialist and student certified attorney. He was law clerk to the Honorable Peter A. Nowinski, United States Magistrate Judge in Sacramento, California. He is an adjunct professor at

San Joaquin College of Law in Fresno. Judge Boone received his J.D. from the McGeorge School of Law, University of the Pacific, and his B.A. from the University of California, Berkeley. He was elected Class Clown of his high school graduating class.

The Honorable Michelle H. Burns is currently a U.S. Magistrate Judge for the District of Arizona, Phoenix Division, appointed to the bench on March. 1, 2007. Previously, she worked in the U.S. Attorneys Office, white collar/public corruption crime unit, and before that spent 11 years in private practice as a partner with Carpenter and Hamilton, PA. She started out her legal career as a county public defender. She spent 22 years as a trial attorney, in both city, county and federal courts. She has been a member of the Horace Rumpole Inn of Court, the Arizona Judicial Performance Review Committee, the Board of Directors of the Federal Bar Association, the Ninth Circuit's Wellness Committee, the Arizona State-Federal Judicial Council, the AO National Steering Group on Pro Se Staffing Formula Review, and has served as a lawyer delegate to the Ninth Circuit. Judge Burns received her J.D. from the University of Toledo, and her B.A. from the University of Michigan. She currently serves as a member of the Ninth Circuit's Magistrate Judges Executive Board.

The Honorable Mark Clarke is a United States Magistrate Judge for the District of Oregon, appointed in 2007. He is a native Oregonian, graduating from the University of Oregon School of Law. He was a trial attorney specializing in liability and commercial litigation in Portland and Medford before being appointed to the bench in southern Oregon. As an attorney, he participated in many state bar committees, CLE programs and authored CLE publications. He is the past President of the Oregon Association of Defense Counsel and the Southern Oregon Federal Bar Association. Judge Clarke is the current President of the Southern Oregon American Inn of Court chapter. He served as a member of the Ninth Circuit's Magistrate Judges Executive Board from 2013-2016.

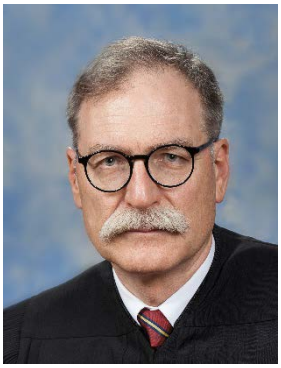


The Honorable James P. Donohue was appointed United States Magistrate Judge for the Western District of Washington on February 8, 2005. In March 2015, he was appointed Chief Magistrate Judge for the District. Prior to his appointment to the bench, Judge Donohue was a shareholder in the Seattle office of Heller Ehrman White & McAuliffe, LLP where his practice was focused on commercial and intellectual property litigation. He served as chair of the Intellectual Property Section of the Washington State Bar Association. He is the author of Chapter 9, Personal Jurisdiction, in Thomson/West's treatise INTERNET LAW AND PRACTICE. Judge Donohue also served as the Articles editor for the Federal Courts Law Review. Judge Donohue received his A.B. from the University of Illinois in 1973, and his J.D. from the University of California, Los Angeles, in 1976, where he was a member of the UCLA Law Review. After his graduation, he served as a VISTA volunteer before going into private practice. Since coming to the bench, Judge Donohue has worked on local rules for patent litigation in the Western District of Washington. He also served on the Ninth Circuit Pro Se Committee, a committee he chaired from 2009-13, and has served on the Ninth Circuit Magistrate Judge Education Committee. Judge Donohue was elected to serve on the Board of Directors of the Federal Magistrate Judges Association, representing the Ninth Circuit. He was one of the founding members and first president of the Seattle Intellectual Property Inns of Court. Judge Donohue also serves on the Board of Directors of Special Olympics of Washington.

The Honorable Charles R. Pyle is a United States Magistrate Judge in the District of Arizona, Tucson Division, and served as the Chair of the Ninth Circuit Pro Se Litigation Committee. In that capacity, he was co-chair of the ground-breaking Ninth Circuit Pro Se Conference in November, 2015, which focused on prisoner rights and conditions, bringing together all stakeholders to discuss the issues. Before his appointment to the bench in 2001, Judge Pyle supervised the Tucson Office of the Liability Management Section of the Arizona Attorney General's Office. In that role, he frequently wrote and lectured on the use of Alternative Dispute Resolution, particularly mediation, to resolve civil disputes. Prior to that, he was with the Civil Division of the Pima County Attorney's Office, working extensively with the Pima County Health Department in their response to the AIDS crisis. Early in his career, for ten years, Judge Pyle was a staff attorney with the Southern Arizona Legal Aid, specializing in consumer law and

indigent health care. He graduated from Stanford University and the University of Arizona College of Law. He was a member of the Ninth Circuit's Magistrate Judges Executive Board from 2012-2015.

The Honorable Suzanne H. Segal was appointed as a Magistrate Judge for the Central District of California in 2002. She served as Chief Magistrate Judge from 2012-2016, providing leadership to 25 Magistrate Judges. Before her appointment to the bench, Judge Segal served as the Chief of Civil Appeals for the Los Angeles U.S. Attorney's Office, supervising all matters before the Ninth Circuit Court of Appeals involving the Civil Division. She was an Assistant U.S. Attorney for 12 years prior to her appointment as Chief of Civil Appeals. Judge Segal began her career as an associate at Dewey, Ballantine in Los Angeles. Judge Segal currently serves as Chair of the Federal Courts Committee of the California Commission on Access to Justice. She is also on the Board of Directors for the Federal Bar Association of Los Angeles and is a member of the Judicial Advisory Council for the Association of Business Trial Lawyers. She represents the Central District on the Ninth Circuit's Magistrate Judges Executive Board. Judge Segal graduated cum laude from Claremont McKenna College and from Cornell Law School. She maintains her chambers in Los Angeles.



The Honorable John T. Rodgers was appointed as a magistrate judge for the U.S. Court for the Eastern District of Washington on September 1, 2013. Prior to coming onto the bench, Judge Rodgers was Director of the Spokane County Public Defenders Office. He practiced as a criminal defense attorney in state and federal courts in Washington State from 1978 to 2003. Judge Rodgers received his B.A. in English Literature and B.A. in business administration from the University of Washington in 1975, and his J.D. from Gonzaga University School of Law in 1978. He maintains chambers in Spokane.

The Honorable Deborah M. Smith is the United States Chief Magistrate Judge for the District of Alaska and serves as Chair of the Ninth Circuit's Magistrate Judges Executive Board. Prior to her appointment to the bench in 2007, Judge Smith served as Acting U.S. Attorney and First Assistant U.S. Attorney for the District of Alaska. As U.S. Attorney, she served as the federal co-chair of the Alaska Rural Justice Law Enforcement Commission in 2006. After graduating from Northeastern Law School, she began her career as the staff attorney for the Alaska Court of Appeals. She then worked with the Alaska Public Defender Agency. She later served as a federal litigator and supervisor in various positions within the U.S. Department of Justice: as the New England Bank Fraud Task Force Director in Boston, Massachusetts; as Deputy Chief of the Environmental Crimes Section and as Senior Litigation Counsel in the Fraud Section in Washington, D.C. She co-authored *The Federal Grand Jury Practice Manual* (U.S. Department of Justice, 1993, rev. 2000). Prior to law school, Judge Smith was the education editor of the Fort Lauderdale News and Sun Sentinel in Florida.

The Honorable Jennifer L. Thurston is a United States Magistrate Judge for the Eastern District of California, appointed in 2009. She has presided over numerous bench trials and jury trials. She has extensive experience with discovery matters and case-dispositive and non-dispositive law and motion practice. She has conducted hundreds of settlement conferences, successfully settling cases involving complicated and highly technical issues. Before appointment, Judge Thurston was an active litigator and handled a variety of cases including civil rights matters, personal injury claims, wrongful death actions, premises liability claims, elections law challenges, subrogation actions and employment disputes. She became a Certified Appellate Specialist in 2005 and, before her appointment, had handled more than 100 appeals and writs. In addition to her role as the ADR Judge for the Fresno Division of her District, she is a member of the District's Technology User Group Committee, the Ninth Circuit Conference's Magistrate Judge Education Committee and the Technology Subcommittee of the 9th Circuit Magistrate Judge Executive Board. Judge Thurston also is a member of the editorial board for the Federal Magistrate Judge Association newsletter committee.

Table of Cases

Table of Statutes

STATUTES – ENACTMENTS BY NAME

STATUTES – U.S. CODE

2703(c)(2)	3, 7, 9, 10
2703(c)(3)	9
2703(d)	ii, 2 thru 4, 9 thru 11, 21, 22
2703(e)	9
2705(a)(1)(A)	11
2705(a)(1)(B)	11
2705(a)(2)	19
2705(b)	3, 10 thru 12
2707(a)	9
2707(d)	9
2711(3)	13
2712	9
3103a	19
3103a(b)(1)	19
3103a(b)(3)	19
3103a(c)	19
3117	4
3117(a)	17
3117(b)	16, 17, 23
3121-3127	1
3121(a)	2
3122	9

3123(d)(2)	12
3127(3)	1, 2
3127(4)	1, 2
3512	13

Title 28, Sections

636	30
1651(a)	37
1691	5
2071-77	26

Title 47, Sections

1001	20, 26, 37
1002(a)(2)	22
1002(b)(3)	37
1002(c)	37
1001-1010	37

Federal Rules of Criminal Procedure

Office of the Circuit Executive
Elizabeth A. Smith, Circuit Executive
P.O. Box 193939, San Francisco, CA 94119-3939
Ph: (415) 355-8900, Fax: (415) 355-8901
http://www.ca9.uscourts.gov