THE FEDERAL COURTS LAW REVIEW‡

Volume 14 2021

THE CELL PHONE DONUT HOLE IN THE TRACKING DEVICE STATUTE

*Stephen Wm. Smith**

‡ The *Federal Courts Law Review* is a publication of the Federal Magistrate Judges Association. Editing support is provided by the members of the *Mississippi Law Journal*.
* Retired United States Magistrate Judge, U.S. District Court, Southern District of Texas (2004-18); Non-resident Fellow, Center for Internet and Society, Stanford Law School. Special thanks to SLS student Haley Amster for invaluable research and editorial assistance, and to Susan Freiwald, Al Gidari, James Orenstein, Brian Owsley, Stephanie Pell, Riana Pfefferkorn, Gabriel Fuentes, and David Sanders for helpful comments on earlier drafts.

> Nor is there any such thing as a "canon of donut holes," in which Congress's failure to speak directly to a specific case that falls within a more general statutory rule creates a tacit exception. Instead, when Congress chooses not to include any exceptions to a broad rule, courts apply the broad rule.
>
> —Justice Gorsuch[1]

INTRODUCTION

Legal fictions—that is, propositions known to be false that the law holds to be true—were once a mainstay of English common law, often deployed by judges to blunt the effect of legislative enactments.[2] Though less frequently seen these days in U.S. courts,

---

[1] Bostock v. Clayton Cnty., 140 S. Ct. 1731, 1747 (2020).

[2] *See generally* Eben Moglen, *Legal Fictions and Common Law Legal Theory: Some Historical Reflections*, 10 TEL AVIV U. STUD. L. 33, 40-41 (1990) (discussing the "process

they have not entirely disappeared. A case in point is the recent decision of the First Circuit Court of Appeals in *United States v. Ackies*.[3] Affirming a drug trafficker's conviction based largely on GPS tracking data transmitted by the defendant's cell phones, the court ruled that a cell phone was *not* a tracking device.[4]

We all know that, willingly or not, our smartphones generate a relentless record of our daily movements in minute detail. More than 80% of the U.S. population uses a smartphone with location-based services.[5] In the words of one prominent journalist on the technology beat, "our cell phones are the world's most effective tracking devices, even when they are turned off."[6] The Supreme Court itself has observed that location tracking via cell phone is tantamount to an ankle monitor, the quintessential tracking device.[7] So the proposition that a cell phone cannot be a tracking device surely conflicts with the common understanding of ordinary citizens, tech journalists, and Supreme Court justices.

The *Ackies* opinion created this legal fiction by misconstruing two different statutes. On the one hand, the panel unduly

---

of fictionalization"); L.L. Fuller, *Legal Fictions*, 25 ILL. L. REV. 363, 363 (1930) ("Probably no lawyer would deny that judges and writers on legal topics frequently make statements which they know to be false. These statements are called 'fictions.'").

[3] United States v. Ackies, 918 F.3d 190 (1st Cir. 2019), *cert. denied*, 140 S. Ct. 662 (2019).

[4] *Id.* at 194.

[5] *See* S. O'Dea, *Smartphone Penetration Rate in Selected Countries 2020*, STATISTA (June 24, 2021), https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country/ [https://perma.cc/H4QM-NS82] (stating that as of September 2020, 81.6% of Americans use smartphones); Monica Anderson, *More Americans Using Smartphones for Getting Directions, Streaming TV*, PEW RSCH. CTR. (Jan. 29, 2016), https://www.pewresearch.org/fact-tank/2016/01/29/us-smartphone-use/ [https://perma.cc/L3CX-AV3S] (showing that as of 2015, 90% of smartphone owners use their phones for location-based activities).

[6] JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 141 (2014).

[7] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018). Chief Justice Roberts' ankle monitor analogy is truer than he may have realized. The standard GPS ankle monitor actually *is* a cell phone, transmitting the wearer's geolocation to a monitoring agency's laptop via cell signal. Although typically not used for two-way communication, they can be configured to do so. *See* Debra Cassens Weiss, *GPS Ankle Monitors Can Call and Record People Without Consent; Do They Violate 5th Amendment?*, A.B.A. J. (Apr. 9, 2019, 11:39 AM), https://www.abajournal.com/news/article/electronic-monitoring-devices-can-call-and-record-people-accused-of-crimes-without-their-consent [https://perma.cc/7UTU-NBRS].

constricted the most natural reading of the Tracking Device Statute ("TDS"), holding that it did not apply to this form of location tracking. Along the way, the court (1) disregarded the unambiguous statutory definition of "tracking device"; (2) cherry-picked among alternative meanings of other statutory terms to create "contextual" conflict with the definition, violating the canon of harmonious construction; (3) rewrote the definition to add an unstated limitation; (4) ignored contrary legislative history; and (5) rendered the TDS obsolete by binding its scope to 1980s tracking technology.

On the other hand, the panel unduly expanded the reach of the Stored Communications Act, ("SCA"), by applying it to prospective monitoring of cell phone location. This holding: (1) uncritically extended a record-production regime (the SCA) to real-time surveillance; (2) incorrectly assumed that court-ordered GPS pings are business records of the provider subject to the SCA; (3) misread Advisory Committee Notes on the tracking warrant amendments to Federal Rule of Criminal Procedure 41; and (4) unwittingly expanded the SCA to authorize extra-territorial surveillance, likely in violation of international law.

Unfortunately, the *Ackies* holding on this issue is a matter of first impression at the circuit level, so its influence may not be confined to one circuit. Adding to its significance is the increasing prevalence of cell phone tracking warrants. Though largely ignored in the aftermath of the Supreme Court's landmark Fourth Amendment ruling on cell site location information, real-time tracking of cell phones has likely become the most common form of court-authorized surveillance, surpassing the combined annual volume of wiretap and pen register orders.[8] Left unchallenged, *Ackies* has the potential to cause real mischief by undermining the established regulatory regime for one of law enforcement's most powerful and frequently used surveillance techniques.

This article takes a critical look not only at the justifications offered by the *Ackies* panel in favor of the cell phone tracking donut hole, but also those put forward by lower courts and law enforcement advocates. In order to weigh these arguments properly, it will be necessary to recount the relatively recent history of the precise location information, ("PLI"), warrant, which made

[8] *See infra* Section III.B.

its published opinion debut in 2011. It is a remarkable tale of opportunistic advocacy, involving at least four major reversals of official positions taken by the DOJ and federal prosecutors in other judicial and legislative venues. It is also a cautionary tale of federal courts' failure to adequately probe superficial legal arguments in support of new surveillance technology. The full story has not been previously told, to my knowledge.[9]

Part I will set the stage with a three-part background. Section A is a brief overview of the Electronic Communications Privacy Act of 1986, ("ECPA"), setting the legal contours of electronic surveillance law still in place today. The law has several components, falling into two broad categories: real-time surveillance (wiretaps, pen registers, trap and trace devices, and tracking devices) and retrospective disclosure of stored communications and transactional records. Special emphasis will be given to contrasting the provisions of the Tracking Device Statute (as supplemented by procedural amendments to Federal Rule of Criminal Procedure 41) with those of the Stored Communications Act. Section B will trace the evolution of tracking technology in the caselaw, from the primitive beepers at issue in the Supreme Court decisions in *Knotts*[10] and *Karo*,[11] to the cell phone-based GPS tracker in *Jones*,[12] to cell site simulators,[13] and most recently to computer software remotely installed via so-called NIT warrants.[14] Section C will recount the relatively short legal career of the so-called "precise location information" warrant which *Ackies* approved. As we shall see, this newly-minted warrant made its first official appearance in 2011, when a Maryland magistrate judge wrote a lengthy opinion rejecting the SCA as a legal basis for such warrants.[15]

---

[9] This article is not the first to criticize *Ackies* as wrongly decided, however. *See* Haley Amster, Note, *Rediscovering the Tracking Device Statute*, 24 STAN. TECH. L. REV. 344, 370-72, 382-87 (2021) (explaining how the TDS applies not only to cell phones, but also to wearable health monitors, computers, and other devices in the smart home).

[10] United States v. Knotts, 460 U.S. 276 (1983).

[11] United States v. Karo, 468 U.S. 705 (1984).

[12] United States v. Jones, 565 U.S. 400 (2012).

[13] United States v. Rigmaiden, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012).

[14] *See, e.g.*, *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755-56 (S.D. Tex. 2013).

[15] *In re* Application for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 571-75 (D. Md. 2011).

Part II examines the *Ackies* decision in detail. The first Section considers the court's crabbed interpretation of the TDS to exclude cell phone tracking, beginning with the three rationales explicitly offered by the court: textual context, workability, and Advisory Committee Notes. Also considered are four additional rationales left out of the opinion but sometimes advanced by law enforcement advocates: legislative history, anomalous applications, slippery slopes, and device ownership. None of these rationales are convincing, as I hope to show. The second Section deals with the court's overly expansive reading of the SCA to provide a home for PLI warrants. Two overlooked pitfalls to this holding are examined, rooted in propositions that the DOJ has itself endorsed over the years—GPS ping data are not business records and the SCA does not authorize ongoing surveillance.

Part III explains why *Ackies* matters and outlines the unfortunate possible consequences if followed by other courts. First of all, *Ackies* renders incoherent ECPA's carefully-crafted surveillance schemes; if the SCA authorizes ongoing monitoring of the data it governs (communications, customer records, and location information), then the rest of ECPA's provisions on wiretaps, pen/traps, and tracking devices are redundant, swallowed up by an all-consuming SCA. Of special concern is the prospect of backdoor wiretaps circumventing the special constitutional requirements set out in *Berger v. New York*. A second major difficulty is lack of notice to the target of the surveillance; in some circuits, this could render the surveillance constitutionally invalid. Yet another is the absence of the territorial limits imposed by the TDS on tracking warrants. This territorial concern is exacerbated by the recent CLOUD Act amendments to the SCA, which in theory could allow U.S. law enforcement to track cell phones anywhere in the world, potentially violating international law and destabilizing U.S. relations with other nations. A final troubling concern is the remarkable number of inconsistent legal positions taken by the government in prosecuting this case. Such strategic duplicity is frowned upon by courts, and in the long run, prosecutors may pay a price in diminished credibility in warrant applications.

I conclude with parting thoughts about courts, legislatures, and the abiding gap between law and technology.

I. BACKGROUND

A. ECPA Surveillance: Four Weddings and a Funeral

Often criticized as a fiendishly difficult statute to understand, much less master, the Electronic Communications Privacy Act has a daunting reputation. For present purposes, we may avoid some of the difficulty by focusing upon ECPA's procedural rules regarding electronic surveillance by law enforcement.

ECPA is generally thought of in terms of its three titles: Title I, wiretaps; Title II, stored communications as well as customer and subscriber information; and Title III, pen registers and trap & trace devices.[16] This format offers a limited and somewhat misleading understanding of ECPA's legislative scheme; for one thing, it omits the important Title I provisions concerning mobile tracking devices, a form of electronic surveillance far more common than wiretaps.[17]

A more helpful way of comprehending ECPA might be to focus on the two broad categories of surveillance—prospective monitoring versus retrospective disclosures. This was the perspective of Senator Patrick Leahy, one of the key sponsors behind ECPA in 1986, as he later explained in remarks on the Senate floor:

> ECPA was a careful, bipartisan and long-planned effort to protect electronic communications in two forms—from real-time monitoring or interception as they were being delivered, and from searches when they were stored in record systems. We recognized these as different functions and set rules for each based on the relevant privacy expectations and threats to privacy implicated by the different forms of surveillance.[18]

Viewed through this lens, the structure of ECPA surveillance authority might be pictured as "four weddings and a funeral." Four parts are prospective and forward-looking, like a wedding:

---

[16] *See* 18 U.S.C. §§ 2510-23 (codifying Title I); 18 U.S.C. §§ 2701-13 (codifying Title II); 18 U.S.C. §§ 3121-27 (codifying Title III). *See also Electronic Communications Privacy Act of 1986 (ECPA)*, BUREAU JUST. ASSISTANCE, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 [https://perma.cc/PSG3-5FEF] (last visited Oct. 22, 2021).

[17] *See* 1 JAMES G. CARR ET AL., LAW OF ELECTRONIC SURVEILLANCE § 4:105, Westlaw (database updated Aug. 2021); 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 4.5, Westlaw (database updated Dec. 2020).

[18] 150 CONG. REC. S7,893 (daily ed. July 9, 2004) (statement of Sen. Patrick Leahy).

wiretaps, pen registers, trap and trace devices, and tracking devices. The other part is retrospective and backward-looking, like a funeral: the disclosure of stored communications and transactional records. This four-weddings-and-a-funeral structure gives coherence to ECPA's regulatory scheme, providing carefully drawn boundaries between the various surveillance categories. As we shall see, PLI warrants simply do not fit within any of those categories. Straddling the line between ECPA's retrospective and prospective provisions, a PLI warrant is an entirely novel strain of surveillance authority. It is no less strange, and no more coherent, than a combination wedding/funeral.[19]

Our overview begins with the weddings, then attends to the funeral.

1. Prospective Monitoring: Wiretaps, Pen Registers, Trap & Trace, and Tracking

As enacted in 1986, ECPA covers four surveillance tools—wiretaps, pen registers, trap and trace devices, and tracking devices—in three different regulatory schemes. Title I of ECPA amended the 1968 Wiretap Act by extending its protections to all forms of electronic communication, not just oral and wire (telephone) conversations.[20] Title III (referred to as the Pen/Trap Statute) set out the procedural requirements for court orders authorizing pen registers and trap and trace devices; originally applicable only to telephones,[21] the 2001 Patriot Act expanded the pen/trap definitions to cover email and other forms of internet communication.[22] ECPA provisions on tracking devices, known collectively as the Tracking Device Statute, are easy to overlook,

---

[19] My research has not found an example of a combined wedding/funeral, although condemned Irish patriot Joseph Plunkett came close. His midnight wedding in Kilmainham Gaol took place only hours before his dawn execution for his role in the Easter Rising of 1916. For this story told through song, see *Grace Lyrics by Jim McCann*, BELLS IRISH LYRICS, https://www.bellsirishlyrics.com/grace.html [https://perma.cc/C5C7-H998] (last visited Oct. 22, 2021).

[20] *See* 18 U.S.C. §§ 2510-23.

[21] A pen register is a device that records the numbers dialed for outgoing calls from the target phone. A trap and trace device captures the phone numbers for calls made to the target phone. 18 U.S.C. § 3127.

[22] *Id. See also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, § 216(c), 115 Stat. 272, 290.

occupying a single section of Title 18 of the U.S. Code;[23] the procedural rules for TDS tracking warrants are found in Rule 41 of the Federal Rules of Criminal Procedure.[24]

These ongoing surveillance schemes have many features in common, none of which are found in the SCA.

Law enforcement authorization. Wiretap orders, pen/trap orders, and tracking warrants are directed to law enforcement, authorizing governmental agents to engage in a specified surveillance technique—the interception of communications,[25] the "installation and use of a pen register or trap and trace device,"[26] or the installation and use of a mobile tracking device.[27] Providers may be required to offer necessary technical assistance to the government (see below), but they are not authorized to act without government supervision.

Specified category of data. Each surveillance scheme targets a single type of communication data; there is no overlap.[28] Wiretaps exclusively acquire communications content;[29] pen/traps exclusively gather non-content "dialing, routing, addressing, and signaling" ("DRAS") information;[30] and tracking warrants exclusively collect data "tracking . . . the movement of a person or object."[31] Each scheme likewise specifies a distinct legal threshold:

---

[23] 18 U.S.C. § 3117 (stating, in its entirety, "(a) In general.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction. (b) Definition.—As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.").

[24] *See* FED. R. CRIM. P. 41. *See also* FED. R. CRIM. P. 41 Advisory Committee's Notes to 2006 Amendments.

[25] 18 U.S.C. §§ 2516, 2518.

[26] 18 U.S.C. §§ 3122(a), 3123.

[27] 18 U.S.C. § 3117(a); FED. R. CRIM. P. 41(b)(4), 41(e)(2)(C).

[28] *In re* Application for Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005) ("In other words, do the four broad categories of the ECPA overlap, such that location information obtainable from a [section] 3117 tracking device is simultaneously obtainable under the Wiretap Act, the SCA, or the Pen/Trap Statute? The answer to this question is clearly 'no.'").

[29] *See* 18 U.S.C. § 2516.

[30] 18 U.S.C. § 3121(c).

[31] 18 U.S.C. § 3117(b).

a "super-warrant" for wiretaps,[32] certified relevance for pen/traps,[33] and probable cause for tracking warrants.[34]

Duration and extensions. Each scheme imposes a time limit on the duration of authorized surveillance: thirty days for wiretaps,[35] forty-five days for tracking warrants,[36] and sixty days for pen/traps.[37] Extensions may be granted by the court upon a proper showing.[38]

Sealing. In order to ensure successful monitoring, orders for wiretaps and pen/traps are automatically sealed until further order of the court.[39] While the TDS does not specifically require sealing of tracking warrants, such warrants are routinely sealed like any other electronic surveillance order.[40]

Third party technical assistance. All three surveillance schemes authorize the court to direct third parties to provide facilities and technical assistance necessary to accomplish the surveillance.[41]

It is worth pausing the narrative here to emphasize how much the success of modern law enforcement surveillance depends upon private facilities and technical assistance, especially when that surveillance is linked to ubiquitous communications technology like the telephone.[42] Rather than rely solely upon its own resources and

---

[32] *In re Application*, 396 F. Supp. 2d at 751. These include a finding that alternative investigative techniques "would be futile or dangerous," that the seizure of innocent communications will be minimized, and that particularity requirements relating to targets, facilities, locations, and crimes have been met. CHARLES DOYLE, CONG. RSCH. SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 24-26 (2012).

[33] 18 U.S.C. § 3123(a).

[34] FED. R. CRIM. P. 41(d)(1).

[35] 18 U.S.C. § 2518(5).

[36] FED. R. CRIM. P. 41(e)(2)(C).

[37] 18 U.S.C. § 3123(c)(1).

[38] 18 U.S.C. § 2518(5) (wiretaps); FED. R. CRIM. P. 41(e)(2)(C) (tracking warrants); 18 U.S.C. § 3123(c)(2) (pen/traps).

[39] 18 U.S.C. §§ 2518(8)(b), 3123(d)(1).

[40] *See* Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177, 208-10 (2009).

[41] *See* 18 U.S.C. §§ 2518(4), 3124(a)-(b). *See also* United States v. N.Y. Tel. Co., 434 U.S. 159, 172-78 (1977) (holding that the All Writs Act justified a technical assistance order essential to prevent the nullification of a court surveillance warrant).

[42] Congress recognized the critical role of the telecommunications industry in facilitating law enforcement surveillance in 1994 when it passed the Communications Assistance for Law Enforcement Act ("CALEA"), requiring providers to preserve existing

equipment, law enforcement is able to leverage the advancing technology of an integrated telephone network. This leverage is especially advantageous now that those networks are computerized, with major operations controlled in-house via keystrokes and mouse clicks.[43] Thus, wiretap operations no longer involve physical installation of "[s]mall wires . . . inserted along the ordinary telephone wires" connected to the target phone, as in *Olmstead v. United States.*[44] Pen registers no longer require physical attachment of the device via alligator clips to a telephone line, as in *United States v. New York Telephone Co*.[45] Tracking operations no longer require physical attachment of a beeper to the moving target, as in *United States v. Karo.*[46] All these surveillance operations can now be accomplished digitally, via a provider-managed app with software interface that allows law enforcement officers to monitor the activity remotely from their laptops.[47]

---

wiretap capacities in the face of advancing technology. *See* PATRICIA MOLONEY FIGLIOLA, CONG. RSCH. SERV., RL30677, DIGITAL SURVEILLANCE: THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT 1 (2007).

[43] For an account of this transformation in the phone network, see generally Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz*,* Smith*, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1 (2016).

[44] Olmstead v. United States, 277 U.S. 438, 456-57 (1928). For a description of later pen register operations through law enforcement headquarters, see United States v. Rodriguez, 968 F.2d 130, 135 (2d Cir. 1992).

[45] *N.Y. Tel. Co.*, 434 U.S. at 162-63. *See also* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 982-89 (1996) (discussing the evolution of the pen register from mechanical device to computer system). It is no longer accurate to refer to a wiretap, a pen register, or a trap and trace device as if they were separate tools. In the context of internet communications, for example, a computer program called a "packet sniffer" is used to collect both content and non-content addressing information, depending on the filter setting used. 2 LAFAVE ET AL., *supra* note 17, § 4.7(a).

[46] United States v. Karo, 468 U.S. 705, 707 n.1 (1984). *See generally* Matt Blaze, *How Law Enforcement Tracks Cellular Phones*, EXHAUSTIVE SEARCH (Dec. 13, 2013), https://www.mattblaze.org/blog/celltapping [https://perma.cc/696T-5ZV7]; Freiwald, *supra* note 45.

[47] *See* United States v. Pineda-Moreno*,* 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, C.J., dissenting); *In re* Application for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 531 (D. Md. 2011) (describing Sprint's "Precision Locate Service").

2. Retrospective Disclosure: Stored Communications and Records

As indicated by its descriptive caption in the U.S. Code ("Stored Wire and Electronic Communications and Transactional Records Access"),[48] the SCA is a record-production regime.[49] The Supreme Court describes the SCA's mode of document disclosure as a "subpoena process."[50] According to Justice Alito, an SCA order is "the functional equivalent of a subpoena for documents," because it "merely requir[es] a party to look through its own records and produce specified documents."[51] A subpoena duces tecum imposes no continuing obligation on a party to produce records beyond the return date.[52]

One of the complexities of the SCA is that it is not confined to a single category of data with a single legal threshold. Section 2703(a) regulates disclosure of communication contents less than 180 days in electronic storage; the legal threshold is a warrant "using the procedures described in the Federal Rules of Criminal Procedure."[53] Section 2703(b) governs disclosure of communications held in storage over 180 days; the legal process for such an order may range from a Rule 41 warrant (without notice), or, if notice is given, an administrative subpoena or a section 2703(d) order based

---

[48] Title 18 of the U.S. Code, section 2703, the focus of our interest, is likewise captioned "Required disclosure of customer communications or records." 18 U.S.C. § 2703.

[49] *See* 2 LAFAVE ET AL., *supra* note 17, § 4.8(a) ("[The SCA] regulates acquisition of user account information stored in the ordinary course of business.").

[50] Carpenter v. United States, 138 S. Ct. 2206, 2215 n.2 (2018). The SCA was modelled after another record-production regime, the Right to Financial Privacy Act (RFPA), which governs law enforcement access to bank records. S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. The RFPA similarly does not authorize ongoing prospective access to bank records. *See In re* Order Authorizing Prospective & Continuous Release of Cell Site Location Recs., 31 F. Supp. 3d 889, 895 (S.D. Tex. 2014).

[51] *Carpenter*, 138 S. Ct. at 2247 (Alito, J., dissenting).

[52] *See* CHARLES DOYLE, CONG. RSCH. SERV., RL33321, ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS: A BRIEF LEGAL ANALYSIS 12 (2006) ("[T]he subpoena duces tecum instructs the individual to gather up the items described at his relative convenience and bring them before the tribunal at some designated time in the future."). *See also* FED. R. CIV. P. 45(a)(1)(A)(iii) (requiring subpoenas to command production of designated documents "at a specified time and place").

[53] 18 U.S.C. § 2703(a). Presumably, this circumlocution means (at least) a warrant based on probable cause. According to *Ackies*, it does not encompass all other Rule 41 procedures, such as venue. United States v. Ackies, 918 F.3d 190, 201-02 (1st Cir. 2019).

on "specific and articulable facts."[54] Section 2703(c) regulates disclosure of "a record or other information pertaining to a subscriber or . . . customer . . . (not including the contents of communications)"; this data can be obtained via a Rule 41 probable cause warrant or a section 2703(d) order based on specific and articulable facts.[55] This category includes a subset of basic subscriber information (name, address, call logs, etc.),[56] which are available via administrative subpoena.[57]

What distinguishes an order for disclosure under section 2703 from the three surveillance schemes discussed above is the mode of acquisition, not the type of data acquired. The SCA covers the same types of data—communication content, transactional data, and location data—that are the subject of other ECPA titles, but the text of the SCA has several distinctive features not shared by ECPA's ongoing surveillance schemes:

Orders directed at providers. SCA orders do not "authorize" the government to engage in surveillance of any sort. Rather they compel the provider to "disclose" certain types of data to the government.[58] Like a traditional subpoena, it commands action by the recipient of the order, not by a law enforcement agency.

Preservation orders. The SCA has a unique provision allowing the government to require the provider to "preserve records and other evidence in its possession pending the issuance of a court order or other process" for a period of ninety days.[59] The logical implication of section 2703(f) is that disclosure of records under section 2703 is a one-time event, exactly like a subpoena duces tecum response.[60] If continuous, ongoing disclosures were the norm,

---

[54] 18 U.S.C. § 2703(b), (d). Section 2703(b) has been declared unconstitutional to the extent it permits the government to obtain emails without a warrant. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

[55] 18 U.S.C. § 2703(c)(1). Customer account records may also be obtained with the consent of the subscriber or customer, or by submitting a formal written request as part of a telemarketing fraud investigation. *Id.*

[56] 18 U.S.C. § 2703(c)(2)(A)-(C).

[57] 1 CARR ET AL., *supra* note 17, § 4:101.

[58] *See* 18 U.S.C. § 2703(a)-(d).

[59] 18 U.S.C. § 2703(f).

[60] *See In re* Application for an Order (1) Authorizing the Use of a Pen Reg. & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 314 (E.D.N.Y. 2005).

there would be no need for preservation of records under section 2703(f).

Possession, custody, control. SCA disclosure obligations extend only to records within the provider's "possession, custody, or control."[61] This phrase has long been used as the measure of discovery obligations in civil and criminal procedure.[62] According to the leading treatise on federal practice and procedure, "[a] document or thing is not in the possession, custody, or control of a party if it does not exist. Production cannot be required of a document no longer in existence nor of one yet to be prepared."[63] Federal litigants responding to a subpoena thus have no continuing obligation to disclose future records on an ongoing basis.[64]

To recap, the SCA subpoena process is funereal in nature: disclosure of the specified documents does not continue day after day, week after week, or month after month, but is rather a discrete and terminal event. By contrast, ECPA surveillance schemes resemble a matrimonial commitment: it does not expire the next day, but extends into the future for as long as higher authority allows. Although the metaphor is new, the substance of this distinction has long been understood and accepted by academic commentators.[65] In the words of a leading treatise on criminal

---

[61] 18 U.S.C. § 2713.

[62] *See, e.g.*, FED. R. CIV. P. 34(a)(1) (allowing one party to request another "to produce and permit the requesting party or its representative to inspect, copy, test, or sample [certain] items in the responding party's possession, custody, or control").

[63] 8B CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2210, Westlaw (database updated Apr. 2021).

[64] *See* United States v. Warshak, 631 F.3d 266, 335 (6th Cir. 2010) (Keith, J., concurring) ("The plain language of [section] 2703(f) permits only the preservation of emails in the service provider's possession at the time of the request, not the preservation of future emails."); *In re* Application for an Order Authorizing Disclosure of Location Based Servs., No. H-07-606M, 2007 WL 2086663, at *1 (S.D. Tex. July 6, 2007) ("Nothing in [section] 2703 requires, or authorizes the Government to demand, that a provider *create* records which would not otherwise exist in the ordinary course of business."); *In re* Application, 396 F. Supp. 2d at 313-14 ("[Section] 2703 does not authorize a court to enter a prospective order to turn over data as it is captured [because of the retrospective nature of the statute].") (emphasis omitted).

[65] *See, e.g.*, Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 18 (2004); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1565 (2004). Two widely cited scholars of ECPA co-authored an amicus brief in 2004 making this precise point. *See* Brief for the Center for Democracy and Technology et al. as Amici Curiae Supporting Appellant's Petition for

procedure, "[t]he Wiretap Act regulates prospective continuous surveillance of an account that may result in a particular communication being copied, while the Stored Communications Act regulates a single intrusion to access and copy that communication."[66]

As we shall see, the DOJ itself subscribed to this consensus for many years, until the recent advent of PLI warrants.[67]

B. The Evolution of Tracking Devices in the Caselaw

1. Beepers in *Knotts* and *Karo*

The modern GPS tracking device had not been invented when ECPA was passed in 1986. Then-existing tracking technology, a simple radio transmitter called a transponder, was described in a Senate report:

> These are one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder. Such "homing" devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.[68]

This rudimentary device, known as a "beeper," had been the subject of the first Supreme Court tracking decisions, *United States v. Knotts* and *United States v. Karo*.[69] In both cases, the beeper had been surreptitiously placed in a container of chemicals used by drug traffickers and then monitored over a period of time. The process of

---

Rehearing and Rehearing En Banc, United States v. Councilman, 385 F.3d 793 (1st Cir. 2004) (per curiam) (No. 03-1383), 2004 WL 2058257 ("Congress never intended the Stored Communications Act to govern ongoing surveillance."). The case involved an appeal challenging a district court order that emails in momentary storage could be continually accessed under the SCA as opposed to the Wiretap Act. *See* United States v. Councilman, 418 F.3d 67, 71 (1st Cir. 2005).

[66] 2 LAFAVE ET AL., *supra* note 17, § 4.6(b) n.32.

[67] *See infra* Section II.B.2.

[68] S. REP. NO. 99-541, at 10 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3564.

[69] United States v. Knotts, 460 U.S. 276, 277 (1983) ("A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver."); United States v. Karo, 468 U.S. 705, 707 n.1 (1984) (citing *Knotts*).

monitoring beeper transmissions was fairly primitive.[70] The receiver in the patrol car consisted of a loop antenna and a radio frequency detector. In order to find the direction of the beeper, the loop antenna had to be turned manually to "home" in on the signal source. The distance between receiver and target could only be approximated—the louder the beep, the closer the beeper.[71] Under normal operating conditions, a beeper's signal could be monitored from a distance of two to four miles on an open road and up to 20 miles in the air. In denser cities, the range might drop to a few blocks due to signal interference. Because the beeper system lacked the capacity to ascertain or record the target's actual location, it was more accurately described as a "radio direction finder," indicating the beeper's location *vis-a-vis* the person monitoring the receiver. Due to these limitations, beepers were mainly "used to supplement visual surveillance—a stopgap in case visual contact with the target [was] lost."[72]

Beeper devices were hardly ideal surveillance tools for the police. Four serious shortcomings of beeper-assisted surveillance were highlighted in a 2011 Supreme Court amicus brief by a group of technical experts and the Center for Democracy and Technology (CDT):

- live human observation is necessary to determine the target's actual location;[73]
- the beeper's real-time directional information is ephemeral and cannot be directly presented in court;[74]
- the beeper yields only a crude approximation of distance and direction;[75]

---

[70] *See, e.g.*, William Shaw, *Miniature Tracking Transmitters (Radio Beacon Tails),* L. & ORD., Jan. 1973, at 24, 29; Jerry L. Dowling, *"Bumper Beepers" and the Fourth Amendment*, 13 CRIM. L. BULL. 266, 266-69 (1977).

[71] *See* Shaw, *supra* note 70, at 29.

[72] Dowling, *supra* note 70, at 269. *See also* Shaw, *supra* note 70, at 29-30; Brief of Center for Democracy & Technology et al. as Amici Curiae in Support of Respondent at 16, United States v. Jones, 565 U.S. 400 (2012) (No. 10-1259) [hereinafter CDT Amicus Brief].

[73] CDT Amicus Brief, *supra* note 72, at 16-17.

[74] *Id.* at 18.

[75] *Id.* at 19.

- beeper surveillance is resource-intensive and becomes impractical over time.[76]

Fortunately for law enforcement, a revolution in location-based technology was imminent, enabling far more efficient means of tracking a suspect.

2. GPS Cell Phone-Based Trackers in *Jones*

Within a few years, the rudimentary beeper was overtaken by two related advances in communications technology—cellular networks and the satellite-based Global Positioning System (GPS). By the 1990s, cell phones began the transition from analog to digital, and cellular networks started to proliferate around the country.[77] Equally significant, in 2000, the highest quality GPS signal was made available for civilian use.[78] In 1997, "the Federal Communications Commission issued final 'Enhanced 911' (E911) rules requiring cellular service providers to upgrade their systems to identify more precisely the longitude and latitude of mobile units making emergency 911 calls."[79] "By the end of 2005, carriers using handset-based location technology [were] required to locate cell phones within 50 meters for 67% of calls."[80]

This regulatory push, combined with emerging market demand for location-based services, led to a new generation of cell phones equipped with special hardware (GPS chips) to receive signals from global positioning satellites. These signals allowed a phone handset to calculate its precise latitude and longitude coordinates, which could then be transmitted back to the phone network (or to a third party such as law enforcement) depending upon the application software running the phone.[81] These GPS

---

[76] *Id.* at 21.

[77] *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Const., C.R., & C.L. of the H. Comm. on the Judiciary*, 111th Cong. 15, 19 (2010) [hereinafter *ECPA Reform Hearing*] (statement of Matt Blaze, Associate Professor, University of Pennsylvania).

[78] *See* CDT Amicus Brief, *supra* note 72, at 8 n.2.

[79] *In re* Application for Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005).

[80] *Id. See also* 47 C.F.R. § 20.18(h) (2005).

[81] *ECPA Reform Hearing*, *supra* note 77, at 21.

location features were integrated with software applications for mapping, street directions, and other location-based services.[82]

Thus was born the GPS tracker. Law enforcement wasted little time in taking advantage.[83] This new generation of tracking devices made its Supreme Court debut in *United States v. Jones*.[84] In September 2005, FBI agents applied for a warrant authorizing the use of a tracking device on the vehicle of a suspected drug trafficker.[85] A warrant was issued, authorizing installation of the device within ten days and its continued use beyond the territorial jurisdiction of the district court.[86] The device was installed on the vehicle in a Maryland public parking lot, and Government agents monitored its movements over the next twenty-eight days. The Court succinctly described how the device operated, "[b]y means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, *and communicated that location by cellular phone to a Government computer*. It relayed more than 2,000 pages of data over the 4-week period."[87]

Read that italicized passage again. The device communicated its tracking data "by cellular phone." Could this mean that a cell phone is an essential component of a GPS tracking device?

---

[82] *Id.*; CDT Amicus Brief, *supra* note 72, at 18.

[83] *See In re Application*, 396 F. Supp. 2d at 754 (quoting another source).

[84] United States v. Jones, 565 U.S. 400, 403 (2012).

[85] *Id.* at 402. The application was based on three separate legal authorities: the All Writs Act (28 U.S.C. § 1651(a)), the Tracking Device Statute (18 U.S.C. § 3117), and Federal Rule of Criminal Procedure 41. Joint Appendix at 21-22, United States v. Jones, 565 U.S. 400 (2012) (No. 10-1259) [hereinafter Jones Joint Appendix]. At the time the application was made, Rule 41 had not yet been amended to expressly cover tracking warrants. *See* FED. R. CRIM. P. 41 Advisory Committee's Notes to 2006 Amendments.

[86] *See* Jones Joint Appendix, *supra* note 85, at 31-34. Justice Scalia's opinion mistakenly asserted that the warrant required installation of the device within the District of Columbia. *Jones*, 565 U.S. at 402-03. But the warrant itself did not impose that restriction. Jones Joint Appendix, *supra* note 85, at 32-33. The defendant's motion to suppress had argued that the out-of-district installation violated 18 U.S.C. section 3117 rather than the express conditions of the warrant. Defendant Jones' Supplemental Omnibus Pre-Trial Motion at 4-5, United States v. Jones, 565 U.S. 400 (2012) (No. 05-CR-386(1)). The government conceded the violation and thus disclaimed any reliance on the warrant to justify the out-of-district monitoring. *Jones*, 565 U.S. at 403 n.1.

[87] *Jones*, 565 U.S. at 403 (emphasis added). At trial, when asked to explain the "nice picture" of the GPS exhibit showing the Jeep's latitude and longitude coordinates on a map, the FBI agent testified, "[t]he tracking device forwards that to the computer *via cell phone* in this case and sends that information there and software puts it in this nice format that we see there." Jones Joint Appendix, *supra* note 85, at 120 (emphasis added).

According to the experts' amicus brief filed by CDT (and co-signed by Roger L. Easton, the father of the GPS),[88] the answer is "yes, absolutely":

> GPS tracking information is generated through the combined operation of four components: a multi-billion dollar system of satellites owned and operated by the U.S. Department of Defense; a small receiver that uses the satellites' transmissions to calculate latitude, longitude and altitude on a precise and continuous basis; *a cell phone that transmits those coordinates to a police computer*; and mapping software that converts those coordinates into human-intelligible information by plotting them on a map and storing them for further analysis and presentation.[89]

The CDT amicus went on to list the significant advantages of the sophisticated GPS tracking system over the primitive beepers used in *Karo* and *Knotts*: GPS tracking (1) is an automated process that renders visual surveillance unnecessary; (2) generates documentary evidence presentable in court; (3) produces precise and detailed tracking data at 10 second intervals for the entire surveillance period; and (4) can be conducted around-the-clock for extensive periods of time, with minimal (if any) human monitoring.[90]

Given its comparative disadvantages, the beeper-style homing device was essentially obsolete by the time *Jones* was decided in 2012, if not before.[91] At trial in 2008, an FBI agent testified that the GPS tracker placed on Jones' vehicle was a "legacy device," that is, an older model designed by the FBI; he agreed that "newer models are much more accurate."[92] During those years, the commercial market for GPS-enabled handsets was seeing explosive growth with an estimated 228 million units sold in 2008-2009 and experts, at

---

[88] CDT Amicus Brief, *supra* note 72, at 2.

[89] *Id.* at 17-18 (emphasis added).

[90] *Id.* at 16-21.

[91] *See id.* at 16-22 (describing the significant advantages of GPS tracking over beeper-assisted surveillance).

[92] Jones Joint Appendix, *supra* note 85, at 86.

the time, predicting sales of more than 770 million units in 2014.[93] That trend has continued unabated in recent years with the advent of the smartphone. In fact, GPS-equipped mobile phone sales have now eclipsed those of dedicated single-use GPS units.[94]

3. Cell Site Simulator in *Rigmaiden*

Not all tracking devices need to be physically attached to the surveillance target. An early example is the cell site simulator, a portable electronic surveillance device that agents can use to identify, locate, and monitor cell phones in a given area. Essentially, the device poses as a cell tower to trick nearby cell phones into transmitting user data, including location information, to the device.[95]

The first reported decision on the use of a cell site simulator as a tracking device is *United States v. Rigmaiden*, a high profile tax fraud case.[96] In July 2008, the FBI obtained a Rule 41 tracking warrant to use and monitor a cell site simulator to locate a digital device used to commit the crime.[97] FBI agents used the simulator in multiple locations, including an apartment complex, to communicate with and track the location of an aircard on Rigmaiden's device.[98] At no point was the FBI's tracking device

---

[93] Brief of Amici Curiae Electronic Privacy Information Center (EPIC) et al. in Support of the Respondent at 13, United States v. Jones, 565 U.S. 400 (2012) (No. 10-1259).

[94] *See* Thomas Alsop, *Navigation Devices & Services - Statistics & Facts*, STATISTA (Nov. 25, 2020), https://www.statista.com/topics/2221/navigation-devices-and-usage/ [https://perma.cc/AV6C-7HEM] ("With the advent of smartphones and wearables, navigational systems and services are now often integrated into one device – eliminating the need for separate navigational devices."). As a result, the global market for singular use portable navigation devices ("PNDs") has shrunk in recent years. The market peaked in 2009 with approximately 40 million in unit shipments. By 2015, however, that number had decreased to around 23 million unit shipments. PNDs are increasingly being replaced by smartphones, which often come with built-in navigation systems or have third-party applications available to purchase. *See* EUR. GLOB. NAVIGATION SATELLITE SYS. AGENCY, GNSS MARKET REPORT: ISSUE 6 38 (2019), https://www.euspa.europa.eu/system/files/reports/market_report_issue_6_v2.pdf [https://perma.cc/U7VF-LS2E].

[95] *See* Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 191-92 (2014).

[96] United States v. Rigmaiden, 844 F. Supp. 2d 982, 987 (D. Ariz. 2012).

[97] Government's Response to Motion for Discovery, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR-08-0814-PHX).

[98] *Rigmaiden*, 844 F. Supp. 2d at 995.

physically installed or attached to Rigmaiden's laptop; the tracking mission was accomplished remotely via cellular signals, including calls made to the aircard using the device. The warrant authorized a monitoring period of thirty days.[99]

To be sure, cell site simulators can be used for purposes other than actively tracking a particular target. The device can be configured as a wiretap to intercept real-time communications, although this is not typically done. Some courts have approved their passive use as pen registers, sweeping up signaling data indiscriminately from all cell phones within range of the device. This use is controversial, however, and in 2015, the DOJ issued policy guidance recommending a probable cause warrant in such situations.[100]

4. Software in NIT Warrant Cases

In 2013, FBI agents in the Southern District of Texas came to me with an application for a novel type of search warrant, targeting a computer used in a bank fraud scheme. The search would be accomplished via a so-called "network investigative technique" ("NIT"), which would remotely and surreptitiously install software on the target device.[101] Once installed, the NIT software would not only search for and extract copious amounts of electronically stored data, but also activate the computer's built-in camera, thereby generating latitude and longitude coordinates over a thirty-day monitoring period.[102] The Government conceded that the location of the target computer was unknown at the time the application was made.[103]

The request was denied on several grounds, including lack of territorial jurisdiction under the tracking warrant provisions of Rule 41. While the proposed NIT probably met the statutory definition of a "tracking device"—by activating the computer's

---

[99] Government's Response to Motion for Discovery, *supra* note 97.

[100] *See Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, DEP'T JUST. (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download [https://perma.cc/543U-9CKE].

[101] *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013).

[102] *Id.*

[103] *Id.* at 756.

camera and monitoring the device's geolocation for a month—the FBI's application violated Rule 41(b)(4)'s requirement that the installation of the tracking device (i.e., the software) must take place within the district. "To the contrary, the software would be installed on a computer whose location could be anywhere on the planet."[104]

Although *In re Warrant to Search a Target Computer at Premises Unknown* was the first reported decision to consider NIT software as a tracking device, it was hardly the last. Less than two years later, the FBI successfully obtained a NIT warrant from a Virginia magistrate judge as part of a massive child pornography investigation known as Operation Playpen.[105] This NIT warrant (the "Playpen Warrant") arguably proved to be more fruitful than any other single warrant in U.S. history. Thousands of computers in more than 120 countries around the world were subjected to search, and hundreds of prosecutions were brought as a result.[106]

The Playpen Operation began with the FBI's seizure of a child pornography website, which it continued to operate on a government-controlled server in the Eastern District of Virginia. The operation of the NIT was described by the Government as follows:

> Under the NIT Warrant, the FBI installed the NIT [malware] on its server in the magistrate judge's district, where it augmented the content of the Playpen website. As users logged into Playpen and downloaded its content, the NIT tracked the movement of that content from the server in the Eastern District of Virginia through the encrypted Tor network finally to the user's computer. At that point, the NIT caused the Playpen user's computer to transmit specified and limited network information back to the government over the open internet, thus enabling the government to track the location where Playpen had been downloaded.[107]

---

[104] *Id.* at 758.

[105] *See* Brief for the United States at 9, United States. v. Eldred, 933 F.3d 110 (2d Cir. 2019) (No. 17-3367-cr).

[106] *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1106 n.156 (2017).

[107] Brief of the United States at 15, United States v. Taylor, 935 F.3d 1279 (11th Cir. 2019) (No. 18-11852), 2018 WL 4933433, at *15.

The NIT warrant was challenged in case after case by defense counsel, who argued that it was not properly authorized under Rule 41.[108] Government prosecutors responded that the NIT warrants were properly issued as tracking device warrants under Rule 41(b)(4). According to the Government, the tracking device definition was broad enough to include the NIT software remotely installed here:

> As applied to older technologies, the rule contemplates that a tracking device may be a mechanical tool used to track the movement of a tangible object—e.g., a transmitter affixed to a container of chloroform placed in a vehicle traveling over public roadways, like the beeper in *United States v. Knotts*, 460 U.S. 276 (1983). As applied to newer technologies, the rule envisions that a tracking device may be an electronic device used to track the movement of information—e.g., computer instructions embedded in digital content traveling on data highways, like the NIT in this case. . . . The NIT is similar to a transmitter affixed to an automobile that is programmed to send location-enabling signals (like GPS coordinates) back to a government-controlled receiver. . . . *Thus, although not a physical beeper affixed to a tangible object, the NIT operated as a digital tracking device of intangible information within the meaning of Rule 41(b)(4).*[109]

In other words, a tracking device need not be a piece of equipment physically attached to the tracking target. As we have seen, this in itself was not a particularly controversial take on the TDS tracking device definition. The Texas NIT warrant case had already accepted the notion in theory, and the Government had conceded the unattached cell site simulator used in *Rigmaiden* was a tracking device.[110]

---

[108] For a discussion of various district court responses to suppression motions in these cases, see Brian L. Owsley, *Network Investigative Source Code and Due Process*, 14 DIGIT. EVIDENCE & ELEC. SIGNATURE L. REV. 39, 40-42 (2017).

[109] Brief for Appellee United States of America at 31-32, United States v. Werdene, 883 F.3d 204 (3d Cir. 2018) (No. 16-3588), 2017 WL 3037622, at *31-32 (emphasis added). This passage appeared nearly verbatim in government appellate briefs in ten different circuits. *See* sources cited *infra* note 312.

[110] *See* United States v. Rigmaiden, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012).

Nevertheless, the Government's theory was vulnerable in two respects. First, unlike the NIT requested in the Texas case, the Playpen NIT software did not track movement at all, as the TDS definition requires. This NIT merely extracted location-identifying data from the user's computer (like an IP address), thus enabling a one-time location fix. The second difficulty was that the NIT malware would be installed on out-of-district devices. Yet, the TDS required installation *within* the district as the precondition for out-of-district monitoring.

In a creative attempt to avoid these objections, the Government devised a so-called "virtual trip" argument.[111] Under this theory, the NIT software was installed on the government Playpen server within the district, where Playpen users would visit online, access the illegal content, and transmit it back to their own computers. At that point, the NIT caused the user's computer to transmit location-identifying information back to the Government over the internet.[112] In other words, instead of tracking the user's computer, the NIT was used "to track the movement of information—the digital child pornography content requested by users who logged into Playpen's website—as it traveled from the server in the Eastern District of Virginia through the encrypted Tor network to its final destination: the users' activating computers, wherever located."[113]

The Government's virtual trip argument met with some success in the lower courts. By the Government's own count, as of October 2018, the argument had been made in approximately 100 cases, and at least nineteen district court decisions had approved the NIT as a tracking device under Rule 41(b)(4).[114]

The appellate courts have been a different story. Eleven courts of appeal have now rejected challenges to the NIT warrant based on the good-faith exception to the exclusionary rule.[115] All but four

---

[111] Government's Opening Brief at 20, United States v. Levin, 874 F.3d 316 (1st Cir. 2017) (No. 16-1567), 2016 WL 6600152, at *20.

[112] *Id.* at 29-31.

[113] *Id.* at 23.

[114] *See* Brief of the United States, *supra* note 107, at 10.

[115] *See* United States v. Taylor, 935 F.3d 1279, 1290 (11th Cir. 2019); United States v. Eldred, 933 F.3d 110, 121 (2d Cir. 2019); United States v. Ganzer, 922 F.3d 579, 581 (5th Cir. 2019); United States v. Moorehead, 912 F.3d 963, 967 (6th Cir. 2019); United States v. McLamb, 880 F.3d 685, 688 (4th Cir. 2018); United States v. Kienast, 907 F.3d

of those circuits declined to consider whether the NIT warrant was validly issued under the rules.[116] The remaining four circuits considered and rejected the government's virtual trip theory, holding that the NIT warrant was not a valid tracking warrant under Rule 41(b)(4); even so, they concluded, suppression was not warranted based on the good faith doctrine.[117]

Significantly, the four appellate courts rejecting the tracking warrant argument did so on the basis of the two vulnerabilities identified above: the NIT's failure to track the *movement* of anything, as opposed to a one-time location fix;[118] and the NIT's installation on target devices located outside the district.[119] None of the Playpen appellate decisions challenged the idea that remotely-installed software could in principle satisfy the TDS definition of a tracking device.[120] To the contrary, that proposition now has

---

522, 527-28 (7th Cir. 2018); United States v. Levin, 874 F.3d 316, 321 (1st Cir. 2017); United States v. Workman, 863 F.3d 1313, 1317-19 (10th Cir. 2017); United States v. Henderson, 906 F.3d 1109, 1119 (9th Cir. 2018); United States v. Werdene, 883 F.3d 204, 207 (3d Cir. 2018); United States v. Horton, 863 F.3d 1041, 1042 (8th Cir. 2017).

[116] The only circuit in which the government did not make the virtual trip argument was the Fifth Circuit, where it relied solely on the good faith exception. Appellee's Brief for the United States of America at 10-24, United States v. Ganzer, 922 F.3d 579 (5th Cir. 2019) (No. 17-51042), 2018 WL 2165527, at *10-24.

[117] *See Taylor*, 935 F.3d at 1286; *Henderson*, 906 F.3d at 1114; *Werdene*, 883 F.3d at 212; *Horton*, 863 F.3d at 1047-48.

[118] *See Taylor*, 935 F.3d at 1286 ("The NIT didn't 'track' anything. Rather, the NIT performed a one-time extraction of information—including a computer's IP address, username, and other identifying material—which it transmitted to the FBI."); *Henderson*, 906 F.3d at 1114; *Werdene*, 883 F.3d at 211; *Horton*, 863 F.3d at 1047-48.

[119] *See Taylor*, 935 F.3d at 1286 n.9 ("By contrast, the NIT software, although deployed and activated from a government computer in the [E.D. Va.], was not 'installed within' that district—it was installed on suspects' computers outside of the district.") (emphasis omitted); *Werdene*, 883 F.3d at 212; *Horton*, 863 F.3d at 1047-48.

[120] A postscript on NIT warrants should be added here. In 2016, the Supreme Court approved a DOJ-sponsored amendment to Rule 41 adding a special venue provision for NIT warrants seeking "to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district." FED. R. CRIM. P. 41(b)(6). As this wording suggests, the new rule does not apply to all NIT warrants, but only those seeking to obtain electronically stored information. NIT software intended for real-time surveillance, such as wiretaps or location tracking, are not affected by the new rule. Thus, the Texas NIT warrant—to the extent it sought location-tracking authority—would not have been covered by the new rule, while the Playpen warrant likely would have been. *See generally* Mark Herlach et al., *Amendment to Criminal Procedure Rule 41 Impacts Data Privacy in U.S. and Abroad*, JD SUPRA (Dec. 7, 2016), https://www.jdsupra.com/legalnews/amendment-to-criminal-procedure-rule-41-10975/.1 [https://perma.cc/6XKS-9VH2] (discussing the DOJ's involvement).

substantial caselaw support, having been tacitly approved by four appellate courts (the Third, Eighth, Ninth, and Eleventh Circuits)[121] and explicitly approved by a dozen district courts in four other circuits.[122]

C. The Brief History of "Precise Location Information" Warrants

PLI warrants are a recent invention. Prior to 2011, there is no reported case of the government seeking a warrant to track a cell phone under SCA section 2703(c)(1)(A). The explanation is fairly simple: until then, the DOJ had taken the position that warrants were unnecessary and that authority for prospective cell phone monitoring could be found in so-called "hybrid" orders, combining the provisions of the Pen/Trap Statute with the "specific and articulable facts" standard of section 2703(d). When that theory met with stiff resistance from magistrate judges, the DOJ was forced to modify its approach.[123]

At first, agents simply asked for a standard Rule 41 warrant, dropping a footnote declaring that the application was not to be construed as an admission that a probable cause warrant was

---

[121] *See* cases cited *supra* note 118.

[122] *See* United States v. Bateman, No. 17-cr-156, 2018 WL 1904674, at *2 (S.D. Ohio Apr. 23, 2018); United States v. Leonard, No. 17-cr-135, 2017 WL 4478330, at *3 (E.D. Va. Oct. 6, 2017); United States v. Caswell, No. 16-cr-134-FtM-29MRM, 2017 WL 3583535, at *1 (M.D. Fla. Aug. 18, 2017); United States v. Hart, No. 16-cr-110-FtM-29CM, 2017 WL 2822747, at *2 (M.D. Fla. June 30, 2017); United States v. Moorehead, 912 F.3d 963 (6th Cir. 2019), *aff'g denial of motion to suppress*, No. 15-CR-10077 (W.D. Tenn. June 6, 2017); United States v. Austin, 230 F. Supp. 3d 828, 833 (M.D. Tenn. 2017); United States v. Jones, 230 F. Supp. 3d 819, 824-25 (S.D. Ohio 2017), *aff'd*, No. 18-3743, 2019 WL 3764628 (6th Cir. June 27, 2019); United States v. Sullivan, 229 F. Supp. 3d 647, 653-56 (N.D. Ohio 2017); United States v. McLamb, 220 F. Supp. 3d 663, 673 (E.D. Va. 2016); United States v. Lough, 221 F. Supp. 3d 770, 770 (N.D. W. Va. 2016); United States v. Kienast, No. 16-CR-103, 2016 WL 6683481, at *4 (E.D. Wis. Nov. 14, 2016); Transcript of the Ruling on Motion to Suppress at 16, United States v. Mascetti, No. 16-CR-308 (M.D.N.C. Oct. 24, 2016); United States v. Smith, No. 15-CR-467, at 14 (S.D. Tex. Sept. 28, 2016); United States v. Eure, No. 16cr43, 2016 WL 4059663, at *8 (E.D. Va. July 28, 2016); United States v. Matish, 193 F. Supp. 3d 585, 612-13 (E.D. Va. 2016); United States v. Darby, 190 F. Supp. 3d 520, 536 (E.D. Va. 2016).

[123] For more background on the hybrid theory, see Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 211-13 (2018).

required.[124] But Rule 41 has additional requirements—such as notice and territorial limits—that the SCA lacks.[125] After a few years, the DOJ hit on a new strategy: pursue a PLI warrant under SCA section 2703(c)(1)(A). This legal theory had the double advantage of satisfying the Fourth Amendment probable cause requirement, while taking advantage of the SCA's lenient notice and territorial requirements. But a PLI warrant has other flaws, as will be seen.

1. 2011 Maryland Case

The first reported opinion to consider this type of SCA warrant was issued by a Maryland magistrate judge in August 2011.[126] In order to locate a fugitive, the Government applied for authorization to prospectively acquire precise location information on the fugitive's phone pursuant to Rule 41 and SCA section 2703(c)(1)(A).[127] Specifically, "[t]he government asked that the Court order the wireless service provider to send a signal to defendant's cell phone ('ping') that would direct the phone to compute its current GPS coordinates and communicate that data back to the provider, which would in turn forward the coordinates immediately to government agents."[128] Those coordinates would be transformed into a visual depiction of the target phone's precise movements by means of the provider's mapping software application.[129]

If this process sounds familiar, it should. It is essentially identical to the GPS tracker system used in *United States v. Jones*, which was pending before the Supreme Court at exactly the same time. There were only two differences: (1) the receiver in *Jones* automatically computed its GPS coordinates every fifteen seconds, while here, the tracking pings were triggered at government-

---

[124] *See, e.g.*, Application for a Tracking Warrant, No. H-09-1013M, at 2 n.1 (S.D. Tex. Dec. 17, 2009).

[125] *See* FED. R. CRIM. P. 41(b), (f).

[126] *In re* Application for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 526 (D. Md. 2011).

[127] *Id.* at 530-31. The application also invoked the authority of the All Writs Act, which was likewise rejected by the judge. *Id.* at 531, 583. That issue is not material for present purposes.

[128] *Id.* at 531.

[129] *Id.* at 535.

specified intervals over a thirty-day period;[130] and (2) the Government used its own device and mapping software in *Jones*, whereas here, the provider's assistance and facilities were co-opted for that purpose.[131] Otherwise, the two tracking systems were functionally indistinguishable.

In a lengthy opinion covering a variety of issues, Judge Gauvey denied the Government's request. On the SCA warrant issue, she elaborated on the nature of the requested GPS data, emphasizing how it differed from ordinary cell site location data generated by the provider in the ordinary course of business[132]:

> At the hearing, the government admitted that the precise location data sought here is neither ancillary information collected by service providers in the course of business nor information that is automatically generated or stored "incidental" to calls. Therefore, the requested information cannot logically be considered "records" and is nothing like the information courts have found to fall under the purview of [section] 2703. . . . Rather than being a "stored record or other information," the precise location information sought falls squarely within the definition of communications from a tracking device . . . . As such, the information is specifically excluded from coverage under the Wiretap Act and ECPA, including [section] 2703.[133]

Judge Gauvey's decision was not appealed by the Government.

2. 2013 New York Case

The Maryland decision remained the only reported precise location warrant case until 2013, when a magistrate judge from the Eastern District of New York issued the first reported decision approving a precise location warrant under the SCA.[134] The *Smartphone* decision disagreed with the Maryland case on a

---

[130] *Id.* at 530-31. In subsequent cases, the pings were generally done at fifteen-minute intervals.

[131] *Id.* at 534-35.

[132] *Id.* at 532-35.

[133] *Id.* at 574.

[134] *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 150 (E.D.N.Y. 2013).

number of issues,[135] but the focus here remains on the tracking device question.

DEA agents in New York applied for a search warrant under SCA section 2703(c)(1)(A), seeking to compel T-Mobile to provide geolocation data for a cell phone used by a physician subject to an arrest warrant for overprescribing controlled substances.[136] The requested warrant would direct T-Mobile to provide "all information, facilities and technical assistance needed" and "to initiate a signal to determine the location of the [subject telephone] . . . at such intervals and times as directed by [the DEA] . . . for a period of 30 days."[137] After granting the warrant, the magistrate judge subsequently wrote an opinion to explain his departure from the Maryland precedent by rejecting the argument adopted by the Maryland district court and many others,[138] that the broad TDS definition of tracking device effectively removed cell phone geolocation data from the reach of SCA section 2703.[139] According to the court, it was a mistake to read TDS section 3117(b) literally because it ignored the "plain meaning" of the term.[140] Citing the 1986 Senate Report glossary describing the beeper devices then in use, the court concluded that "section 3117 incorporated the then-common understanding of tracking device, to wit: a device designed and intended to perform a law enforcement function of tracking an

---

[135] One of the chief differences was a rather narrow legal issue: whether a federal court may issue a search warrant to aid in the apprehension of the subject of an arrest warrant in the absence of a showing of additional criminal activity. *Id.* at 134-37. The other issue was constitutional: whether a cell phone user has a reasonable expectation of privacy in geolocation data. *Id.* at 142-47. In both instances, the Eastern District of New York sided with the government. Five years later, of course, the Supreme Court sided with the defense on the latter issue, holding that cell site location records were protected by the Fourth Amendment. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

[136] Affidavit in Support of Application for a Search Warrant at 1-3, *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129 (E.D.N.Y. 2013) (No. 13-MJ-242). The information to be seized included "all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information," as well as cell tower data. *Id.* at 8.

[137] *Id.* at 4.

[138] *See, e.g.*, *In re* Application for Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 757-61 (S.D. Tex. 2005).

[139] *In re Smartphone*, 977 F. Supp. 2d at 134-37.

[140] *Id.* at 149.

automobile, person or item after being 'placed' by agents."[141] However, the court seemed unaware that "plain meaning" analysis is inappropriate when Congress has enacted its own definition, as it did in section 3117(b).[142]

The court also offered a contextual argument. The reference to the device's "installation" in section 3117(a) "supports the notion that the statute is aimed at devices installed specifically to track someone or something, as opposed to cell phones which, incidental to their intended purpose, can be tracked or traced."[143] But the opinion makes no attempt to square this reading of section 3117(a) with the actual language of the definition, which merely requires that the device "permits" tracking, not that its "intended purpose" must be tracking.[144]

Finally, the court asserted that constructing "tracking device" to encompass a cell phone would lead to "illogical and unworkable" results. It offered three examples of tracking devices under such a construction: "an individual travelling by bicycle, leaving tire tracks in a muddy field; an automobile taillight, which could permit officers to follow a car at night; or the transmitter of a pirate radio station, the signal from which may be located via triangulation."[145] Yet, none of these examples are "particularly troublesome."[146] The bicycle is not a tracking device because it is the object of the search, not a device used to locate that object; nor could tire tracks left in a muddy field be a "mechanical or electrical device." Similarly, the taillight is not a tracking device because it is an integral part of the search target; any tracking of its movement is accomplished through direct visual observation, without the use of a mobile device controlled by law enforcement. As for the pirate radio, a transmitter sending location signals is functionally indistinguishable from the beeper planted in the container in *Karo*

---

[141] *Id.* (quoting S. REP. NO. 99-541, at 10 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3564).

[142] *See* Stenberg v. Carhart, 530 U.S. 914, 942 (2000) ("When a statute includes an explicit definition, we must follow that definition, even if it varies from that term's ordinary meaning.").

[143] *In re Smartphone*, 977 F. Supp. 2d. at 149-50.

[144] *Compare id.* at 149-50, *with* 18 U.S.C. § 3117(b).

[145] *In re Smartphone*, 977 F. Supp. 2d. at 150.

[146] *In re* Order Authorizing Prospective & Continuous Release of Cell Site Location Recs., 31 F. Supp. 3d 889, 898-99 (S.D. Tex. 2014).

and just as easily qualifies as a tracking device when converted to that purpose by law enforcement.[147]

Significantly, the *Smartphone* opinion offered no rationale to support its novel holding that the SCA authorized ongoing surveillance like real-time cell phone tracking.

3. 2015 Mississippi Case

Two years later, the Northern District of Mississippi became the second court to generally approve of PLI warrants in a published opinion.[148] Reversing a magistrate judge's decision, the district judge authorized law enforcement on remand to seek a warrant under SCA section 2703(c)(1)(A) to compel AT&T to provide "prospective cell phone location data" in order to track the location of drug suspects.[149]

In the court's view, the SCA was a "much more flexible and workable statute" than the TDS, "which was designed to deal with physical 'installation' of tracking devices rather than requests for data from third party cell phone providers."[150] Confronted with the observation that an "installation" need not entail physical attachment—e.g., software installation—the court responded with a non sequitur: the tracking device in *Jones* was physically installed on a vehicle.[151] Left unexplained was how this lone example justified ignoring common usage of the term to encompass both physical and remote forms of "installation."[152]

Like the *Smartphone* decision before it, the Mississippi court's opinion did not consider how the requested GPS ping data, generated solely at the behest of law enforcement, could qualify as a genuine business record within the provider's "possession, custody, or control," as the SCA requires.[153] Nor did either case explain how a record-production regime like the SCA could be transformed into a new form of real-time surveillance. Yet, as we

---

[147] *See id.*; Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *8 (N.D. Ill. Mar. 5, 2018) (rejecting *Smartphone*'s analysis).

[148] *In re* Application for an Order for Authorization to Obtain Location Data Concerning an AT&T Cellular Tel., 102 F. Supp. 3d 884, 896 (N.D. Miss. 2015).

[149] *Id.* at 885, 893, 896.

[150] *Id.* at 892.

[151] *Id.* at 886.

[152] *See infra* Section II.A.1.

[153] 18 U.S.C. § 2713.

shall see, both decisions were cited uncritically by the *Ackies* opinion.

II. THE *ACKIES* DECISION

Carey Ackies was convicted of drug trafficking, in part, based on evidence derived from two PLI warrants issued by a magistrate judge sitting in Maine.[154] The warrants authorized DEA agents to acquire "specific latitude and longitude or other precise location information" for the target phones by "directing AT&T, the service provider for [the target phone], to initiate a signal to determine the location of [the target phone] at such times and intervals as directed by law enforcement for a period of 30 days."[155] Because the target phones were already in New York, the venue limitation of the TDS would have precluded out-of-state monitoring. Instead, the Government invoked the authority of a different law, the Stored Communications Act, which has a much broader jurisdictional reach than the TDS.[156]

On appeal, Ackies challenged the PLI warrants on jurisdictional grounds, claiming that the out-of-state monitoring violated the venue provisions of the TDS and Rule 41(b)(4).[157] The Government responded (1) that the TDS did not apply to cell phones and (2) that the warrants were properly issued under the authority of the SCA.[158] The First Circuit Court of Appeals agreed with the Government on both counts. Rejecting the defendant's argument that a cell phone was a "tracking device" within the TDS definition, the court wrote:

---

[154] United States v. Ackies, 918 F.3d 190, 194 (1st Cir. 2019).

[155] United States v. Ackies, No. 16-cr-20, 2017 WL 3184178, at *2 (D. Me. July 26, 2017). The district court elsewhere defined the term "PLI" as "shorthand for any cell phone location information, including GPS or latitude-longitude data and less precise cell-site location information." *Id.* at *8 n.24.

[156] *Id.* at *2. *See* 18 U.S.C. § 2703(c)(1)(A).

[157] *Ackies*, 918 F.3d at 197-98.

[158] *Id.* at 201.

> Section 3117(a) refers to the "installation of a mobile tracking device." By their plain meanings, "installation" and "device" refer to the physical placement of some hardware or equipment (such as the GPS device installed on a car mentioned in Carpenter). . . . A reading of [section] 3117(b) which includes cell phones as "tracking device[s]" ignores the relevant textual context . . . . Further, as the district court correctly stated, use of [section] 3117 does not work when considering cell phone location data, because "it could be exceedingly difficult in situations involving PLI to determine where 'installation' is to occur," and the government "may be seeking data concerning a cell phone whose present location is unknown."[159]

Finally, the court relied upon the 2006 Advisory Committee Notes to Rule 41 referring to the magistrate judge's authority to permit "installation," "maintenance," and "removal" of the device; according to the court, these words operate to exclude a cell phone as a tracking device under section 3117.[160]

The court further held that the warrants were properly issued under section 2703 of the SCA. Because the District of Maine had jurisdiction over the drug trafficking offenses being investigated, the magistrate judge there was a "court of competent jurisdiction" empowered to issue orders under the SCA.[161] As to whether the substance of the PLI warrant was authorized by the SCA, the court disposed of the issue in a single sentence: "The government requested precise location information from the 'provider of electronic communication service' and this precise location information 'pertain[ed] to a subscriber to or customer of such service.'"[162] At this point, the court proceeded to address other issues not pertinent here, such as whether the geographic limitations in Rule 41(b) apply to warrants under the SCA (no), and

---

[159] *Id.* at 199 (alteration in original) (citation omitted) (citing *In re* Application for an Order for Authorization to Obtain Location Data Concerning an AT&T Cellular Tel., 102 F. Supp. 3d 884, 892 (N.D. Miss. 2015); *Ackies*, 2017 WL 3184178, at *11). *Carpenter* did not involve a GPS tracker installed on a car; that case was *United States v. Jones*. United States v. Jones, 565 U.S. 400, 403 (2012).

[160] *Ackies*, 918 F.3d at 199-200.

[161] *Id.* at 200.

[162] *Id.* (alteration in original) (quoting 18 U.S.C. § 2703(c)(1)).

if so, whether the *Leon* good faith exception to the exclusionary rule would apply (yes).[163]

In the next several Sections, we examine the arguments advanced by the court in support of its interpretations of the TDS and the SCA. We also consider other arguments sometimes offered by law enforcement proponents, but not explicitly relied upon by the First Circuit.

A. TDS Holding: Unpersuasive Rationales

Considered in isolation, the unqualified language of the tracking device definition ("an electronic or mechanical device which permits the tracking of the movement of a person or object") is not limited to a particular technology or mode of installation.[164] In order to escape the literal meaning of section 3117(b), the court resorted to other interpretive techniques.

1. Physical Placement

The court began with an argument from textual context, relying on two words in the venue provision of section 3117(a): "installation" and "device." According to the court, these words necessarily imply "physical placement of some hardware or equipment," and so, this "plain meaning" supplies sufficient context to alter the unqualified statutory definition next door in section 3117(b).[165]

However, standard dictionaries do not support the court's crabbed reading of those terms.[166] According to Webster's Third New International Dictionary, published the same year ECPA was enacted, a primary meaning of the root word "install" is "to set up for use or service."[167] Other dictionaries before and since have consistently adopted the same broad reading of the term, one that

---

[163] *Id.* at 201-03.

[164] 18 U.S.C. § 3117(b).

[165] *Ackies*, 918 F.3d at 199.

[166] The court cited no dictionary to justify its unorthodox reading of "installation." Instead, the court cited the New York and Mississippi lower court decisions, which likewise offered no dictionary authority for their holdings. *Id. See also supra* Sections I.C.2-3.

[167] WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1171 (Philip Babcock Gove ed., 1986).

includes but, unlike the interpretation in *Ackies*, is not limited to the physical placement of hardware.[168] This "set up for use" definition obviously includes the installation of computer software, which typically requires no physical placement or attachment at all.[169] Thus, the true plain meaning of "installation" easily covers the computerized process by which the phone company remotely activates a cell phone's GPS functionality.[170]

In a footnote, the court's opinion attempts to rebut the software counterexample, contending that software is not a "device" because that word necessarily refers to a "piece of equipment" like hardware.[171] Once again the court's interpretation is arbitrarily narrow; standard dictionaries do not confine "device" to tangible items.[172] Even the Supreme Court has described software as a

---

[168] *See Install*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/install [https://perma.cc/MM4M-4YCL] (Oct. 22, 2021) ("to set up for use or service"); *Install*, VOCABULARY.COM, https://www.vocabulary.com/dictionary/install [https://perma.cc/25TS-KS73] (last visited Oct. 24, 2021) ("set up for use"). *See also Install*, DICTIONARY.COM, https://dictionary.com/browse/install [https://perma.cc/LJY3-UXHL] (last visited Oct. 24, 2021) ("to place in position or connect for service or use"); *Install*, WIKTIONARY, https://en.wiktionary.org/wiki/install [https://perma.cc/J3GD-DB9N] (Oct. 22, 2021, 11:40 AM) ("[t]o connect, set up or prepare something for use"); THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 908 (Am. Heritage Inc. ed., 5th ed. 2011) ("[t]o connect or set in position and prepare for use"); RANDOM HOUSE WEBSTER'S UNABRIDGED DICTIONARY 987 (2d ed. 2001) ("to place in position or connect for service or use"); *Install*, BLACK'S LAW DICTIONARY (rev. 4th ed. 1968) ("[t]o set up or fix in position for use or service").

[169] This usage is now so common that some dictionaries use it in example sentences. *See Install*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/install [https://perma.cc/MM4M-4YCL] (Oct. 22, 2021) ("The software *installs* automatically."); *Install*, VOCABULARY.COM, https://www.vocabulary.com/dictionary/install [https://perma.cc/25TS-KS73] (last visited Oct. 24, 2021) ("You can *install* new software on your computer . . . .").

[170] Although ECPA was passed at an early stage of the digital revolution, the installation of computer software was already a familiar usage in court opinions. *See, e.g.*, Loews Corp. v. Sperry Corp., 449 N.Y.S.2d 715, 716 (N.Y. App. Div. 1982).

[171] *Ackies*, 918 F.3d at 199 n.5.

[172] *See, e.g.*, *Device*, MERRIAM-WEBSTER, www.merriam-webster.com/dictionary/device [https://perma.cc/RL7D-FBLZ] (Oct. 17, 2021) ("something devised or contrived: such as [a] plan, procedure, [or] technique"); *Devices*, VOCABULARY.COM, www.vocabulary.com/dictionary/devices [https://perma.cc/J8DG-8S7H] (last visited Oct. 24, 2021) ("Devices are objects or systems that have a specific purpose or intention, like electronic . . . devices like cell phones.") (emphasis omitted); *Device*, BLACK'S LAW DICTIONARY (rev. 4th ed. 1968) ("[a]n invention or contrivance; any result of design; . . . a plan or project"). Even the dictionary cited by the court gives a broader general definition of the term: "something that is formed or formulated by

"device."[173] Electronic devices such as computers consist of both hardware and software. Complete installation of any digital device—such as a GPS tracker—requires setting up *both* the physical hardware *and* the intangible software necessary for the device to function.

The court's contextual argument, based on its idiosyncratic reading of section 3117(a), is simply unpersuasive. Moreover, had the *Ackies* court slightly expanded its field-of-vision to the rest of ECPA, it would have seen the term "installation" frequently used to refer to remote activation of surveillance software. The Pen/Trap Statute, in Title III of ECPA, contains more than two dozen references to the words "install" or "installation."[174] As previously shown in Section I.A.1, pen registers and trap and trace devices are remotely activated in much the same way as GPS cell phone pings.[175] Gone are the days when "pen registers involved physically tapping into the target's phone wires and installing a device that detected rotary dialed digit pulses on the line."[176] And yet, the Pen/Trap Statute still applies the same "installation" terminology to the modern software incarnation of that device.[177] When two parts of the same statute employ similar terminology, it is reasonable to conclude that Congress intended the terminology to bear a consistent meaning.[178] Statutory context thus confirms, rather than undermines, the plain text of section 3117(b)'s tracking device definition.

Besides failing on its own terms, the court's contextual argument flouts traditional tenets of statutory interpretation. The

---

design." WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 618 (Philip Babcock Gove ed., 1993).

[173] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 940 (2005) (referring to "the device, the software in this case").

[174] *See* 18 U.S.C. §§ 3121-25.

[175] *See supra* Section I.A.1. Professor Matt Blaze has described this computerized process as a "'lawful access' interface that can be configured [by the telephone company] to electronically deliver call information about targeted subscribers to law enforcement agencies in real time." Blaze, *supra* note 46.

[176] Blaze, *supra* note 46.

[177] The original definition of pen register referred to "the telephone line to which such device is attached." *In re* Application for an Order Authorizing the Use of a Cellular Tel. Digit. Analyzer, 885 F. Supp. 197, 199-200 (C.D. Cal. 1995) (emphasis omitted). That phrase was deleted by the 2001 PATRIOT Act amendments. *See* 18 U.S.C. § 3127(3).

[178] Tanzin v. Tanvir, 141 S. Ct. 486, 490-91 (2020).

court here assigns unusually restrictive meanings to certain statutory terms, inexplicably ruling out standard usages consistent with the statutory definition. In so doing, the court has generated an avoidable clash between sections 3117(a) and 3117(b). It is as if a stalled vehicle blocked one freeway lane, while traffic flows freely in all the other lanes. Rather than steer around the obstruction, the *Ackies* panel heads straight for the pile-up.

But judges are not demolition derby drivers. A cardinal rule of statutory construction is to interpret one section of a statute in harmony with all the others, wherever possible.[179] "A court must therefore interpret the statute 'as a symmetrical and coherent regulatory scheme,' and 'fit, if possible, all parts into an harmonious whole.'"[180] By shunning the common usages of section 3117(a) terms that are perfectly compatible with section 3117(b), the *Ackies* opinion violated this rule of harmonious construction.

Other canons of interpretation were likewise disregarded. "[W]hen the statute's language is plain, the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms."[181] A corollary of this plain meaning rule applies to statutory definitions: "[w]hen a statute includes an explicit definition, we must follow that definition, even if it varies from that term's ordinary meaning."[182] Just as nothing in the TDS requires physical installation of a tracking device, nothing in the seventeen words of section 3117(b) rules out remote installation. Under the technology-neutral definition of tracking device enacted by Congress, the mode of installation is simply not relevant. In other words, if it walks like a duck and quacks like a duck, the coloration of its feathers does not

---

[179] *See* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 180-82 (2012).

[180] FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000) (citation omitted) (first quoting Gustafson v. Alloyd Co., 513 U.S. 561, 569 (1995); and then quoting FTC v. Mandel Brothers, Inc., 359 U.S. 385, 389 (1959)).

[181] United States v. Ackies, 918 F.3d 190, 201 (1st Cir. 2019) (quoting Lamie v. U.S. Tr., 540 U.S. 526, 534 (2004)). *See also* United States v. Wilson, 503 U.S 329, 334 (1992); Armstrong Paint & Varnish Works v. Nu-Enamel Corp., 305 U.S. 315, 333 (1938) ("[T]o construe statutes so as to avoid results glaringly absurd, has long been a judicial function.").

[182] Stenberg v. Carhart, 530 U.S. 914, 942 (2000). *See also* Borden v. United States, 141 S. Ct. 1817, 1829 (2021) ("A court does not get to delete inconvenient language and insert convenient language to yield the court's preferred meaning.").

matter; it is still a duck. As Monty Python would say, "[t]he plumage don't enter into it."[183]

A final point before moving on. While the government successfully persuaded the trial and appellate courts in *Ackies*' case that the TDS must be limited to "the physical installation" of a piece of equipment,[184] federal prosecutors were simultaneously rowing the opposite direction in ten different federal appellate courts and dozens of district courts around the country.[185] Part III will address this and other reversals of position by the government.[186]

2. Workability

The *Ackies* panel also endorsed a rationale the lower court had found persuasive: the "use of [section] 3117 does not work when considering cell phone location data," for essentially two reasons.[187] First, it could become "exceedingly difficult" to determine where the "installation" takes place. Is it the district from which the instructions are sent to the phone, causing its movements to be reported to FBI laptops? Or is it the district where the target phone is located when it receives those instructions? The other concern is that law enforcement may not even know where the phone is located, making it difficult to satisfy the venue requirement.[188]

Workability is a problematic argument to make in statutory interpretation, especially as applied to unambiguous statutory definitions. Just as there is no "donut hole" canon of construction, neither is there a "workability" canon. As the Supreme Court has long made plain, pleas of administrative inconvenience never "justify departing from the statute's clear text."[189] Of course, if the literal terms of a statute are impossible to satisfy, a court may

---

[183] LUKE DEMPSEY, MONTY PYTHON'S FLYING CIRCUS: COMPLETED AND ANNOTATED 150 (2012).

[184] Government's Consolidated Response to Defendant's Motions to Suppress at 12, United States v. Ackies, No. 16-cr-20, 2017 WL 3184178 (D. Me. July 26, 2017), 2017 WL 10155132.

[185] *See supra* note 109 and accompanying text.

[186] *See infra* Section III.D.

[187] United States v. Ackies, 918 F.3d 190, 199 (1st Cir. 2019).

[188] *Id.* (citing United States v. Ackies, No. 16-cr-20, 2017 WL 3184178, at *11 (D. Me. July 26, 2017)).

[189] Niz-Chavez v. Garland, 141 S. Ct. 1474, 1485 (2021) (quoting Pereira v. Sessions, 138 S. Ct. 2105, 2118 (2018)).

justifiably craft an interpretation which avoids that absurdity. But neither of the workability issues cited in *Ackies* rises to that level.

By the time *Ackies* was decided, two Courts of Appeals had already shown the place-of-installation issue to be quite workable indeed. The Eighth Circuit was the first to do so in *United States v. Horton*, one of many Playpen appeals arising out of the NIT warrant issued by a Virginia magistrate judge:

> The government argues that the defendants made a "virtual" trip to the Eastern District of Virginia to access child pornography and that investigators "installed" the NIT within that district. Although plausible, *this argument is belied by how the NIT actually worked: it was installed on the defendants' computers in their homes in Iowa.*[190]

The Third Circuit reached the same result in another Playpen case, *United States v. Werdene*.[191] Considering the same government argument that installation of the NIT had occurred in Virginia, the court was dismissive:

> It is difficult to imagine a scenario where the NIT was "installed" on Werdene's computer—which was physically located in Pennsylvania—in EDVA. The Eighth Circuit, which is the only other Court of Appeals to address the Government's Rule 41(b)(4) argument . . . , rejected it on this basis . . . .[192]

Shortly after *Ackies* was decided, the Eleventh Circuit in *United States v. Taylor*[193] became the third appellate court to confront the issue. Like its predecessors, the Eleventh Circuit agreed that, "the NIT software, although *deployed and activated* from a government computer in the Eastern District of Virginia,

---

[190] United States v. Horton, 863 F.3d 1041, 1047-48 (8th Cir. 2017) (emphasis added). The Eighth Circuit also agreed with the lower court's reasoning that the NIT did not meet the definition of a tracking device because "it did not 'track' the 'movement' of anything." United States v. Croghan, 209 F. Supp. 3d 1080, 1088 (S.D. Iowa 2016).

[191] United States v. Werdene, 883 F.3d 204 (3d Cir. 2018).

[192] *Id.* at 212. The court also found it dispositive "that the NIT did not track *movement*" because it merely searched for and transmitted the IP address and other identifying information, and thus, it did not satisfy the tracking device definition. *Id.*

[193] United States v. Taylor, 935 F.3d 1279 (11th Cir. 2019).

was not '*installed* within' that district—it was installed on suspects' computers outside of the district."[194]

Given the unanimity and dispatch with which these three circuit courts disposed of the district-of-installation issue, the *Ackies* panel's worry about workability seems overblown. The solution is common sense: installation of a digital tracking device occurs wherever the device is located when set-up is complete—that is, when both the hardware and software are in place and ready for use. In *Ackies*, the installation took place in New York, where the cell phone was located when AT&T personnel made the necessary keystrokes to set up its tracking function for law enforcement.

The second proffered "workability" argument is just as feeble: sometimes, the location of the target cell phone is unknown, so the venue restriction may become difficult to satisfy. To the extent this is a real problem (my personal experience in granting dozens of cell phone tracking warrants suggests not), the ready response is that Rule 41 has several other territorial restrictions that might prove equally troublesome. The general rule is that a court may authorize searches and seizures that take place within its district; out-of-district searches are the exception to the rule.

Congress and the Supreme Court have approved territorial exceptions in the past, following the statutory rule-making process. In fact, one of the stated purposes behind the 2006 tracking warrant amendments was to "avoid[] the necessity of obtaining multiple warrants if the property or person later crosses district or state lines."[195] In other words, Rule 41(b)(4) was itself created to resolve a perceived workability problem for law enforcement seeking tracking warrants. Another exception occurred in 2016 when Rule 41(b) was amended to specify the appropriate venue for NIT warrants authorizing remote access searches for electronically stored information. The rule was amended upon the specific request of the Department of Justice, citing a recent ruling by "one magistrate judge . . . that an application for a warrant for a remote search did not satisfy the territorial jurisdiction requirements of

---

[194] *Id.* at 1286 n.9. As in *Horton* and *Werdene*, the court also based its ruling on the alternative ground that the NIT "didn't 'track' anything. Rather, the NIT performed a one-time extraction of information—including a computer's IP address, username, and other identifying material—which it transmitted to the FBI." *Id.* at 1286.

[195] FED. R. CRIM. P. 41 Advisory Committee's Notes to 2006 Amendments.

Rule 41."[196] In direct response to the DOJ's workability concerns, Rule 41(b)(6) was added as another exception to the in-district search rule.[197]

As these examples demonstrate, workability exceptions to the usual territorial limits on search and seizure are policy questions for rule-makers and legislators, not an excuse for courts to rewrite unambiguous definitions in the United States Code. In the blunt words of the Supreme Court, "no amount of policy-talk can overcome a plain statutory command."[198]

3. Advisory Committee Notes

The final justification offered by the *Ackies* court was a bit unusual. As we have seen, Rule 41 was amended in 2006 to include procedures for tracking warrants. Rather than examine congressional intent by looking to the 1986 legislative history of section 3117, the court turned to the deliberations of the 2006 Advisory Committee on the Criminal Rules, as reflected in its notes to the Rule 41 tracking warrant amendments. The two key provisions of Rule 41's treatment of tracking devices—the definition and the venue provision—were carried over from the TDS. Rule 41 expressly provides that it "does not modify any statute regulating search or seizure," and the Advisory Committee Notes disclaim any intention "to expand or contract the definition of what might constitute a tracking device."[199] So, the preliminary question arises—how could Advisory Committee Notes pertaining to a 2006 rule amendment shed any light on the congressional intent behind a statute passed in 1986?[200]

---

[196] Letter from Mythili Raman, Acting Assistant Att'y Gen., U.S. Dep't of Just., to the Hon. Reena Raggi, Chair, Advisory Comm. on the Crim. Rules 2 (Sept. 18, 2013), https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf [https://perma.cc/D2PR-9GV4].

[197] See *supra* Section I.B.4 for more discussion of the case providing the impetus for this rule change. *See also In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 761 (S.D. Tex. 2013) (suggesting that "there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology").

[198] Niz-Chavez v. Garland, 141 S. Ct. 1474, 1486 (2021).

[199] FED. R. CRIM. P. 41(a)(1); FED. R. CRIM. P. 41 Advisory Committee's Notes to 2006 Amendments.

[200] The panel opinion attempts to finesse the issue by citing a Supreme Court decision interpreting a different procedural rule in a different statutory context. United States v.

Be that as it may, the court cites two portions of the Advisory Committee Notes in support of its holding. The first cited passage states that a "magistrate judge's authority under [the tracking device warrant] rule includes the authority to permit . . . installation of the tracking device, and maintenance and removal of the device."[201] Stressing the underlined words, the court argued that "[t]here is no 'maintenance' or 'removal' of a 'device' when gathering precise location information from a cell phone."[202] But this argument just assumes the conclusion. If software can be a "device," as the Supreme Court said in *Grokster* and the DOJ persistently argued in the *Playpen* cases,[203] then tracking software is subject to "maintenance" and "removal" just like any other computer program on a digital device.

The second cited reference to the Advisory Committee Notes reflects some confusion on the part of the court. Supposedly, this note reflects the committee's understanding that the SCA authorizes a form of "continuous monitoring" that is separate and distinct from tracking devices. Here is the relevant passage from the opinion:

> In addition, the 2006 Advisory Committee Notes differentiate [section] 3117 from the SCA, stating that the "[u]se of a tracking device is to be distinguished from other continuous monitoring or observations that are governed by statutory provisions or caselaw. See Title III, Omnibus Crime Control and Safe Streets Act of 1968, as amended by *Title I* of the 1986 Electronic Communications Privacy Act [ECPA]." Id. The SCA is part of the ECPA.[204]

The court's opinion misreads the quoted portion of the note. True, the SCA is "part of the ECPA"—but it is not part of ECPA's

---

Vonn, 535 U.S. 55, 64 n.6 (2002) ("In the absence of a clear legislative mandate, the Advisory Committee Notes provide a reliable source of insight into the meaning of a rule, especially when, as here, the rule was enacted precisely as the Advisory Committee proposed."). But the "legislative mandate" at issue in *Vonn* was the Congressional adoption of a rule drafted by the Committee itself. Here, by contrast, the legislative mandate was a decades-old statute which the Committee had no role in drafting.

[201] United States v. Ackies, 918 F.3d 190, 200 (1st Cir. 2019) (alterations in original) (quoting FED. R. CRIM. P. 41 Advisory Committee's Notes to 2006 Amendments).

[202] *Id.*

[203] *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 940 (2005).

[204] *Ackies*, 918 F.3d at 200 (emphasis added).

Title I, which contains the amendments to the Wiretap Act covering electronic communications. SCA is in Title II of ECPA, codified in a different chapter of the U.S. Code, and is not mentioned anywhere in the Advisory Committee Notes.[205]

Correctly understood, this note actually undermines the court's argument. The note lists several types of "continuous monitoring or observations that are governed by statutory provisions or caselaw," such as tracking devices, wiretaps, video cameras, and television surveillance. Absent from the list is any mention of continuous monitoring under the SCA. This omission is not hard to explain—SCA precise location warrants had yet to be invented.[206]

This concludes the discussion of the three lines of argument deployed by the court in support of the legal fiction that cell phones are not tracking devices. For the sake of completeness, the article will next consider four other arguments sometimes advanced by law enforcement advocates in lower courts and elsewhere, but not relied upon by the *Ackies* panel.

4. Legislative History

Although the First Circuit does not mention it, some lower courts have been persuaded that ECPA's legislative history supports the proposition that the tracking device definition applies only to homing devices, like the beepers used in *Knotts* and *Karo*.[207] The source of this argument is a misreading of a Senate Report's glossary of technology,[208] in particular a passage describing a type of electronic tracking device known as a "transponder." The Senate Report accurately describes the operation of such one-way radio "homing" devices, the predominant tracking technology of the time. But nothing in the glossary purports to be a substitute for the broad

---

[205] *See* 18 U.S.C. §§ 2701-13. The wiretap provisions are codified at 18 U.S.C. §§ 2510-23.

[206] *See supra* Section I.C.

[207] *See, e.g.*, *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 149 (E.D.N.Y. 2013).

[208] *See* S. REP. NO. 99-541, at 8-11 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3562-65. The glossary describes various technologies referred to in the Senate Report, such as electronic mail, computer-to-computer communications, electronic bulletin boards, microwave, cellular telephones, cordless telephones, and electronic pagers. Most of these terms are not later defined in the statute as enacted.

definition of "tracking device" which Congress ultimately enacted. As Judge Richard Posner wrote in a related context concerning the same Senate Report, its description of certain technology was "illustrative rather than definitional."[209] The same is true of the beeper described in the report.

Legislative history has legitimate uses in statutory construction, but only when the language is ambiguous. As the Supreme Court recently reaffirmed in *Bostock*, "legislative history can never defeat unambiguous statutory text."[210] Nor is a statute rendered ambiguous simply because it is broadly written and applies to situations not contemplated by the drafters: "'the fact that [a statute] has been applied in situations not expressly anticipated by Congress' does not demonstrate ambiguity; instead, it simply 'demonstrates [the] breadth' of a legislative command."[211]

Assuming for the sake of argument that ambiguity could be found in section 3117(b), legislative history confirms that Congress intended to encompass tracking by cell phone. In October 1985, as ECPA was being drafted, the congressional Office of Technology Assessment issued a long-awaited report assessing the impact of emerging electronic surveillance technology upon civil liberties.[212] In a chapter devoted to "Telephone Surveillance," the OTA Report listed three separate issues that needed to be addressed in designing policy for cellular and cordless phones. One of those issues "relates to the tracking potential of cellular phones." As the Report explained:

---

[209] United States v. Ramirez, 112 F.3d 849, 852 (7th Cir. 1997).

[210] Bostock v. Clayton Cnty., 140 S. Ct. 1731, 1750 (2020).

[211] *Id.* at 1749 (alterations in original) (quoting Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479, 499 (1985)).

[212] *See* U.S. CONG. OFF. OF TECH. ASSESSMENT, OTA-CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985). The OTA Report was very influential in shaping the legislation finally enacted as ECPA. United States v. Councilman, 418 F.3d 67, 77 (1st Cir. 2005) (en banc) (stating that Congress responded to concerns raised in the OTA Report). *See also* S. REP. NO. 99-541, at 4 (citing the OTA Report as a significant event in ECPA's legislative history).

> By monitoring the switching of cellular phone calls from one frequency to another, the cellular carrier can determine the location of individuals placing and receiving calls. Moreover, some companies record this information in a computer for billing purposes. At this time, precise locations cannot be determined because the cell sizes are large, but as cellular phones become more popular, cell sizes will be reduced allowing more precise tracking.[213]

The OTA Report went on to recommend that "[t]he issue of tracking individuals by monitoring cellular phone calls could be dealt with by requiring investigative authorities to get a court order . . . ."[214] The Report did not specify a particular legal threshold for such an order, but suggested a higher level of protection for real-time tracking: "The nature of the information will vary depending on whether it is real-time information, in which case the present location of both parties is also divulged, or historical information. The former would appear to warrant more protection as it is more specific."[215]

This section of the Report closed by emphasizing the increasing significance of real-time monitoring of phone transactions in criminal investigations. While historical phone records were used primarily in the initial phase of the investigation to determine whether criminal activities were occurring, "[r]eal-time information on phone transactions is also valuable in determining the location of parties, and is, therefore, valuable at any stage of an investigation. There are no traditional techniques for obtaining this information."[216]

Other parts of ECPA's legislative history also discuss cell phone tracking. A prominent telecom executive raised the subject in written testimony at a House committee hearing on the bill. He warned that "the definition of the term 'tracking device' in the current bill is broad enough that it could be read as including

---

[213] U.S. CONG. OFF. OF TECH. ASSESSMENT, *supra* note 212, at 39. Note the prescience of the Report in predicting more precise tracking as cell phone popularity (hence cell tower density) increases. *See ECPA Reform Hearing*, *supra* note 77, at 29-30 (statement of Matt Blaze).

[214] U.S. CONG. OFF. OF TECH. ASSESSMENT, *supra* note 212, at 39.

[215] *Id.* at 41.

[216] *Id.* at 42.

paging or cellular equipment."[217] The same witness made the same point in testimony before a Senate committee: "Telocator suggests clarification of the definition of 'tracking devices' and/or the installation provision so as not to impede the installation or use of paging and cellular telephone equipment."[218] Despite these calls for clarification, the broad definition stayed in the final version of the legislation.

Congress was acutely aware that it was legislating in a time of rapid and accelerating evolution in communication technology.[219] Given that mindset, it is no accident that Congress would define "tracking device" in broad, technology-neutral terms. Binding the new law to existing technology would have defeated the purpose. The prescience of the 1986 Congress was confirmed in 2006 when the tracking warrant provisions were added to Rule 41. The rule-makers had no need to alter the tracking device definition of section 3117(b)—its technology-neutral language just as easily accommodated 21st century GPS trackers as it had 20th-century beepers.

5. Anomalous Applications

Some courts have argued that a literal reading of section 3117(b) might lead to anomalous results that Congress could not have intended. As we have seen, the *Smartphone* court cited some

---

[217] *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Cts., C.L., & the Admin. of Just. of the H. Comm. on the Judiciary*, 99th Cong. 99 (1985-1986) [hereinafter *ECPA House Hearings*] (statement of John Stanton, Chairman, Telocator Network of America).

[218] *Electronic Communication Privacy: Hearing on S. 1667 Before the Subcomm. on Pats., Copyrights & Trademarks of the S. Comm. on the Judiciary*, 99th Cong. 118-19 (1985) [hereinafter *ECPA Senate Hearing*] (statement of John Stanton, Chairman, Telocator Network of America). The definition was subsequently modified in a later version of the legislation, but not in the direction Mr. Stanton was pushing. Instead, the original definition was shortened by eliminating a qualifying clause at the end ("in circumstances in which there exists a reasonable expectation of privacy with respect to such tracking"). In effect, this modification made the definition even broader than it had been when Mr. Stanton testified. *Compare* H.R. 3378, 99th Cong. § 201(a) (1985), *with* H.R. 4952, 99th Cong. § 108(a) (1986) (enacted).

[219] *See* S. REP. NO. 99-541, at 5 (1986) ("Most importantly, the law must advance with the technology to ensure the continued vitality of the fourth amendment."), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

supposedly illogical results flowing from a broad reading of section 3117(b), which on closer inspection are not at all problematic.[220]

Another asserted anomaly often cited by the government is a credit card transaction, which could yield evidence of the card user's location at the time of purchase.[221] Once again, the ready response here is that the TDS applies to devices that track "movement," not just a one-time location snapshot. Learning a credit card user's location at the point of sale is far different from continuously monitoring a cell phone user's movement at fifteen-minute intervals over a thirty-day period. Section 3117(b) plainly applies to the latter, and, just as plainly, not to the former.

Three circuit courts of appeals have now rejected the proposition that a one-time extraction of location data satisfies the criteria for a tracking device under the TDS. Responding to the government's assertion that the NIT warrant in the *Playpen* investigation was authorized under Rule 41(a)(4) as a tracking warrant, the Third Circuit wrote in *United States v. Werdene*:

> [T]he NIT was designed to *search*—not *track*—the user's computer for the IP address and other identifying information, and to transmit that data back to a government-controlled server. . . . This fact—that the NIT did not track *movement*—is dispositive, because Rule 41(b)(4) is "based on the understanding that the device will assist officers *only* in tracking the movements of a person or object." Fed. R. Crim. P. 41 Advisory Committee's Notes (2006) (emphasis added) . . . .[222]

The Ninth Circuit followed the Third Circuit's lead later that year in *United States v. Henderson*, by holding that "[t]he NIT instructions did not actually 'track the movement of a person or property,' as required by the tracking-device provision."[223] The following year, the Eleventh Circuit joined the chorus in *United States v. Taylor*:

---

[220] *See supra* Section I.C.2. *See also* Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *8 (N.D. Ill. Mar. 5, 2018) (explaining why the *Smartphone* examples are "unpersuasive").

[221] *See In re* Application for Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 755-56 (S.D. Tex. 2005).

[222] United States v. Werdene, 883 F.3d 204, 211-12 (3d Cir. 2018).

[223] United States v. Henderson, 906 F.3d 1109, 1114 (9th Cir. 2018).

> The NIT didn't "track" anything. Rather, the NIT performed a one-time extraction of information—including a computer's IP address, username, and other identifying material—which it transmitted to the FBI. . . . But that the FBI eventually used the NIT-transmitted information to discover additional facts that, in turn, enabled it to then determine a Playpen user's *location* in no way transformed the initial information transmittal into "tracking." Indeed, if the term "tracking device" included every gadget capable of acquiring and transmitting information that could somehow, in some way, aid in identifying a person's *location*, the term would be unimaginably broad, including any phone or camera capable of sending a photo, as images of buildings, street signs, or other landmarks can surely be used to identify a *location*.[224]

As these decisions show, courts have had no problem drawing the fundamental distinction between surveillance techniques merely identifying location and those monitoring movement over time; only the latter are true tracking devices. Properly understood, the tracking device definition is neither impractical nor overbroad.

6. Slippery Slopes

An argument raised by the government in some early cases was that, if cell phone tracking were covered by the TDS, then it "would eviscerate privacy protection under the Wiretap Act and the SCA for most communications now deemed electronic communications."[225] This unfortunate consequence was said to follow logically from ECPA's definition of "electronic communication," which specifically excludes "any communication from a tracking device."[226]

This argument rests on a fallacy: if a cell phone can potentially be used as a tracking device, then it necessarily becomes a tracking device at all times and for all purposes. Such reasoning ignores the multi-functional nature of the modern cell phone emphasized by the Supreme Court in *Riley*: "The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that

---

[224] United States v. Taylor, 935 F.3d 1279, 1286 (11th Cir. 2019) (emphasis added).

[225] *In re Application*, 396 F. Supp. 2d at 756.

[226] 18 U.S.C. § 2510(12)(C).

also happen to have the capacity to be used as telephones. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[227] This wondrous device can be configured to deliver a wide variety of information, covering a wide spectrum on the privacy-intrusion scale. Understandably then, the legal threshold for acquiring the various data will likewise vary under ECPA, notwithstanding that the same device delivers them all.[228]

Viewed in this light, the obvious purpose of the tracking communication exclusion in section 2510(12)(E) is to maintain the coherence of ECPA's organizational structure. Tracking information is placed in a category all its own, separate and apart from wire, oral, or electronic communications. Section 2510(12)(E) should thus be understood to refer only to tracking-related communications, that is, any communication from a device *when in tracking mode*. This interpretation, faithful to the overall textual context of ECPA, avoids tumbling down the slippery slope posited by the government. As one district judge has written, it would be "nonsensical to say that a device capable of tracking an individual is not a tracking device simply because it performs other functions."[229]

A slightly different version of the slippery slope argument was advanced in a recent decision from a Utah district court, *In re Search of a Cellular Telephone*.[230] After citing ECPA's tracking communication exclusion, the court pointed to ECPA's definition of "electronic communication service" ("ECS"), which reads, "any service which provides to users thereof the ability to send or receive wire or electronic communications."[231] The court then reasoned as follows, "[t]hus, if a cellular telephone qualifies as a tracking device under 18 U.S.C. [section] 3117, then the Stored Communications Act excludes cellular telephone communications and companies from coverage. However, Congress definitely wrote the Stored

---

[227] Riley v. California, 573 U.S. 373, 393 (2014).

[228] *See* 2 LAFAVE ET AL., *supra* note 17, § 4.7(a) (stating that the applicable legal standard depends "on the information collected, not the nature of the device itself").

[229] Vasil v. Kiip, Inc., No. 16-CV-09937, 2018 WL 1156328, at *8 (N.D. Ill. Mar. 5, 2018).

[230] *In re* Search of a Cellular Tel., 430 F. Supp. 3d 1264 (D. Utah 2019).

[231] 18 U.S.C. § 2510(15).

Communications Act to apply to cellular telephone companies."[232] This particular slippery slope is built on a non sequitur—if a company provides electronic communication services, then it cannot also provide tracking services. But why not? Nothing in the statute suggests these services are mutually exclusive, such that a company must fall into one bucket or the other. The ECS definition thus adds nothing to the original version of the slippery slope argument.

It should be acknowledged that the literal text of section 2510(12)(C) is ambiguous and that the interpretation advanced here is not the only possible one. However, it is the only legally permissible one under the canon of harmonious construction.[233] Moreover, the government's position—that a cell phone can never be a tracking device, even when used for tracking purposes—slides down a slippery slope of its own. By that logic, the GPS tracker in *Jones*, transmitting its geolocation data via cell phone,[234] was not a tracking device either. This would have come as a surprise not only to the Supreme Court (which called it a tracking device in its opinion), but also to the Solicitor General (who called it a tracking device in his brief) and to the FBI (which called it a tracking device in its tracking warrant application).[235] If the modern GPS tracker—commonly regarded as the quintessential tracking device—falls outside the TDS definition, then the TDS tracking warrant scheme effectively becomes obsolete, useable only for rudimentary single-function devices like beepers.

In short, the government's argument avoids one slippery slope only to careen down another into statutory incoherence. Both slopes can be avoided only by giving section 2510(12)(C) the sensibly limited interpretation proposed here—the exclusion applies to tracking-related communications from a tracking device *qua* tracking device, but not to communications related to other device functions.

---

[232] *In re Search*, 430 F. Supp. 3d at 1271.

[233] *See* FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000) (first quoting Gustafson v. Alloyd Co., 513 U.S. 561, 569 (1995); and then quoting FTC v. Mandel Brothers, Inc., 359 U.S. 385, 389 (1959)).

[234] United States v. Jones, 565 U.S. 400, 403 (2012).

[235] *Id.*; Brief for the United States at 3, United States v. Jones, 565 U.S. 400 (2012) (No. 10-1259), 2011 WL 3561881, at *3; Jones Joint Appendix, *supra* note 85, at 21-26.

7. Device Ownership

Implicit in some government arguments for the cell phone donut hole is the notion that the TDS applies only to tracking devices owned or controlled by the government. This argument was advanced by a prominent private attorney and former prosecutor at a 2010 congressional hearing on ECPA reform.[236] While agreeing that the SCA did not provide law enforcement with the authority to access real-time location data, the witness opined that the TDS cannot apply to a consumer's own electronic devices because "there is simply no text or legislative history to support that conclusion."[237]

But, as previously discussed, the legislative history actually does support that conclusion. The 1985 OTA Report specifically flagged as a civil liberties issue the technique of "tracking individuals by monitoring cellular phone calls" and recommended legislation requiring "a court order before getting such records from the cellular company."[238] A prominent telecom executive also testified before House and Senate committees that the TDS tracking device definition would reach consumer devices like pagers and cell phones.[239]

As for the statutory text, the TDS makes no distinction between government-owned and consumer-owned tracking devices. Nor is such a distinction called for as a matter of policy. Chief Justice Roberts explained in *Carpenter* that an individual has a reasonable expectation of privacy in her cell phone location records regardless of "[w]hether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier."[240] The government routinely leverages carrier technology to wiretap conversations over consumer-owned devices; in fact, the DOJ in 1994 pushed hard for the Communications Assistance for Law Enforcement Act ("CALEA") to ensure that law enforcement's wiretapping capabilities would not be eroded by the

---

[236] *ECPA Reform Hearing*, *supra* note 77, at 68-75 (statement of Marc J. Zwillinger, Partner, Zwillinger Genetski LLP).

[237] *Id.* at 74.

[238] U.S. CONG. OFF. OF TECH. ASSESSMENT, *supra* note 212, at 39.

[239] *ECPA House Hearings*, *supra* note 217, at 99 (statement of John Stanton); *ECPA Senate Hearing*, *supra* note 218, at 118-19 (statement of John Stanton).

[240] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

advances in consumer cell phone technology.[241] Likewise, modern pen registers are not government-owned devices; rather, they are computerized processes on facilities owned by private carriers.[242] Neither the Wiretap Act nor the Pen/Trap Statute confine their scope to government-owned surveillance equipment.[243]

Like wiretap and pen/trap orders, tracking warrants issued under Rule 41 are often accompanied by third-party technical assistance orders.[244] The Supreme Court has held that district courts have authority to compel third parties to provide facilities and equipment when necessary to execute Rule 41 surveillance orders.[245] The Administrative Office of the United States Courts has even adopted an official form—entitled "Order Requiring Assistance in Executing a Tracking Warrant"—which directs a third party recipient to assist by "providing facilities and installing, operating, and monitoring any tracking devices."[246] No similar official form has been approved for PLI warrants.

B. SCA Holding: Overlooked Pitfalls

As previously shown, the First Circuit misconstrued the Tracking Device Statute by giving it an unduly cramped reading, devising an unwritten cell phone exception to section 3117(b)'s tech-neutral definition of "tracking device." We now turn to the other

---

[241] *See In re* Application for Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 762 (S.D. Tex. 2005).

[242] Blaze, *supra* note 46. *Cf.* 18 U.S.C. § 3123(a)(3)(A) (imposing additional record-keeping requirements when a law enforcement agency uses its own pen/trap device).

[243] 18 U.S.C. §§ 2518(4), 3124.

[244] *See, e.g.*, Order Requiring Assistance in Executing a Tracking Warrant, *In re* Tracking of a Cellular Tel., No. H-16-528M (S.D. Tex. Apr. 8, 2016); Order Requiring Assistance in Executing a Tracking Warrant, *In re* Tracking of a Mobile Tel., No. H-09-1013M (S.D. Tex. Dec. 17, 2009).

[245] *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 175 n.23 (1977) (stating that the All Writs Act justified a technical assistance order to the phone company because it was essential "to prevent nullification of the court's warrant and the frustration of the Government's right under the warrant to conduct a pen register surveillance.").

[246] *Order Requiring Assistance in Executing a Tracking Warrant (Under Seal)*, U.S. CTS., https://www.uscourts.gov/sites/default/files/ao103.pdf [https://perma.cc/6Z64-3D7U] (last visited Oct. 29, 2021). Such forms are approved by the Judicial Conference of the United States in its supervisory capacity over the Administrative Office. *See Governance & the Judicial Conference*, U.S. CTS., https://www.uscourts.gov/about-federal-courts/governance-judicial-conference [https://perma.cc/QUB6-XQ4L] (last visited Oct. 29, 2021).

statutory misinterpretation by the *Ackies* court, this time in the opposite direction—an unduly *expansive* reading of the Stored Communications Act to authorize real-time cell phone tracking. There are two fundamental difficulties with this holding,[247] neither of which is addressed (or even mentioned) in the court's opinion.

1. Non-Business Records

Under SCA section 2713, a provider may be obligated to provide information "within [its] possession, custody, or control."[248] Government-compelled GPS ping data flunks this test. Nothing in SCA section 2703 authorizes the government to compel a provider to create "records which would not otherwise exist in the ordinary course of business."[249]

As noted by the first magistrate judge to consider (and reject) a PLI warrant back in 2011,[250] GPS ping data is fundamentally different from ordinary cell site location information because it is not a business record of the provider. This was not a controversial position at the time; it was even shared by the DOJ. Here is an Associate Deputy Attorney General explaining the distinction between CSLI and GPS pings to the Senate Judiciary Committee in a 2011 hearing:

---

[247] Other textual arguments could be advanced against the holding that SCA section 2703(c) authorized this particular warrant. First of all, Ackies was neither a customer nor subscriber of AT&T, as section 2703(c) requires—he was merely a *user* of the target phones. *Cf. In re* Application for an Order Authorizing the Installation & Use of a Pen Reg. with Caller Identification Device & Cell Site Location Auth. on a Certain Cellular Tel., 415 F. Supp. 2d 663, 666 (S.D. W.Va. 2006) (distinguishing between the "user" and the "subscriber" of a cell phone); 2 LAFAVE ET AL., *supra* note 17, § 4.8(c) (stating that records "that do not belong to customers and subscribers are not regulated by the SCA"). Second, the GPS ping data was itself the *contents* of the communication to law enforcement, as opposed to ancillary metadata of a call made by Ackies; thus, it is subject to the "contents of communications" exclusion of SCA section 2703(c). However, the thrust of both arguments may be avoided simply by asserting that the PLI warrant was authorized under a different section of the SCA, such as section 2703(a). By contrast, the two arguments advanced in the text negate SCA coverage entirely.

[248] 18 U.S.C. § 2713.

[249] *In re* Application for an Order Authorizing Disclosure of Location Based Servs., No. H-07-606M, 2007 WL 2086663, at *1 (S.D. Tex. July 6, 2007). *See also* United States v. Warshak, 631 F.3d 266, 335 n.2 (6th Cir. 2010) (Keith, J., concurring) (quoting the magistrate judge's order with approval).

[250] *In re* Application for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 526 (D. Md. 2011).

> It should be noted that cell-site information is distinct from GPS coordinates generated by phones as part of a carrier's Enhanced 911 Phase II capabilities. *Such data is much more precise, although wireless carriers generally do not keep it in the ordinary course of business*. When the government seeks to compel the provider to disclose this sort of GPS data prospectively, it relies on a warrant. When prosecutors seek to obtain prospective E-911 Phase II geolocation data (such as that derived from GPS or multilateration) from a wireless carrier, the Criminal Division of the Justice Department recommends the use of a warrant based on probable cause. *Some courts, however, have conflated cell site location information with more precise GPS (or similar) location information.*[251]

To be clear, the Justice Department's position was not simply that an SCA section 2703(d) order was inappropriate to compel GPS ping data, while a probable cause warrant under SCA section 2703 would do the trick. It was that the SCA did not cover GPS ping data in the first place because it was not a "record or other information" within the meaning of SCA section 2703. Any doubt on that score is eliminated by the FBI's own Domestic Investigation and Operations Guide, which instructed its agents as follows:

---

[251] *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 42 (2011) (statement of James A. Baker, Associate Deputy Att'y Gen., U.S. Department of Justice) (emphasis added). *See also id.* at 28 ("[T]he Department recommends that prosecutors obtain a warrant based on probable cause before requiring providers to disclose ongoing precise location data generated using GPS technology embedded in a particular cell phone.").

> In the ordinary course of providing service to the customer, the provider does not typically use this GPS location data. Accordingly, the data may not constitute a "record or other information" in the provider's custody within the meaning of 18 U.S.C. [sections] 2702 and 2703. Consequently, a FRCP Rule 41 search warrant should be obtained to compel the disclosure of such provider-assisted geo-location data.[252]

Even so, the Associate Deputy Attorney General was quite right to note that some courts ignore the critical distinction between CSLI and GPS ping data. *Ackies* is one such case. Another was the Fifth Circuit case of *United States v. Wallace*, decided the previous year.[253] Fortunately, in *Wallace*, the mistake was recognized and corrected—but not before the court was forced to withdraw not one, but two published opinions.

Like Ackies, William Wallace had been convicted of drug trafficking based partly on real-time GPS geolocation data obtained via two "Ping Orders." In its initial opinion issued May 22, 2017,[254] the Fifth Circuit concluded that the GPS ping data was acquired by AT&T in the ordinary course of business, and therefore, it was no different than the historical CSLI the court had previously held unprotected by the Fourth Amendment.[255] In response to Wallace's rehearing motion, the government not only conceded the panel's error, but (even more remarkably) *apologized* for its role in creating the confusion:

---

[252] FED. BUREAU OF INVESTIGATION, U.S. DEP'T OF JUST., DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE § 18.6.8.4.2.5.3 (2011), https://theintercept.com/document/2017/01/31/domestic-investigations-and-operations-guide/#page-366 [https://perma.cc/MS4L-WAWW].

[253] United States v. Wallace, 885 F.3d 806 (5th Cir. 2018).

[254] United States v. Wallace, 857 F.3d 685 (5th Cir. 2017), *withdrawn*, 866 F.3d 605 (5th Cir. 2017).

[255] *Id.* at 690-91. That case, *In re* Application for Hist. Cell Site Data, 724 F.3d 600 (5th Cir. 2013), was one of five circuit court decisions overruled by *Carpenter* in June 2018. (Full disclosure: I authored the district court decision that the Fifth Circuit had reversed in Historical Cell Site. I also authored two other cell site decisions that were purportedly reversed by the initial *Wallace* opinion. All three of those decisions remain good law post-*Carpenter*.)

> [T]he state obtained a court order that required AT&T to collect E911 [GPS] location information for Wallace's phone. E911 location information is different from cell-site data, in part because *cellular-service providers typically do not collect and maintain E911 location information in the ordinary course of business. To the extent that our brief did not adequately draw this distinction, we apologize*.[256]

The Fifth Circuit soon thereafter withdrew its initial opinion, issuing another on August 3, 2017. The revised opinion deleted the problematic Fourth Amendment ruling, while still affirming the conviction on good faith grounds.[257] A third opinion was issued in 2018 to further clarify its ruling.

The two-month interval between the first and second *Wallace* opinions proved fateful for Mr. Ackies. During that time, the Maine district court rejected Ackies' challenge to the GPS pings, expressly relying upon the initial *Wallace* opinion to hold that GPS geolocation monitoring was a business record obtainable via SCA section 2703.[258] While the First Circuit did not cite *Wallace* in its own opinion, the court ignored the critical difference between CSLI and GPS geolocation data, exactly as the Fifth Circuit had mistakenly done.

In sum, the GPS ping data transmitted by Ackies' phone was in no sense a business record within the possession, custody, or control of the provider. Absent the court orders compelling the provider to assist in its creation, it would not exist at all because it serves no business purpose, only a law enforcement purpose. The SCA simply does not reach so far.

---

[256] Response to Petition for Rehearing En Banc at 2, United States v. Wallace, 885 F.3d 315 (5th Cir. 2018) (per curiam) (No. 16-40701) (emphasis added).

[257] United States v. Wallace, 866 F.3d 605, 609 (5th Cir. 2017). The initial *Wallace* opinion, reported in the advance sheets at 857 F.3d 685, was withheld from the bound volume after it was superseded by a second opinion on August 3, 2017. *See id.* at 605. The second opinion was itself later withdrawn and superseded by a third opinion on March 20, 2018. *See Wallace*, 885 F.3d at 806. The petition for rehearing en banc was denied by an 8-7 vote with Judges Dennis and Graves joining in a dissenting opinion. *See* United States v. Wallace, 885 F.3d 315, 315 (5th Cir. 2018) (per curiam).

[258] United States v. Ackies, No. 16-cr-20, 2017 WL 3184178, at *10 (D. Me. July 26, 2017).

2. Ongoing Surveillance

For the first quarter-century of its existence, the SCA was understood to set the rules for one-time disclosure of provider-held information. As a leading treatise on criminal procedure has explained, it is the mode of data acquisition that distinguishes the SCA from surveillance statutes like the Wiretap Act.[259] Courts and commentators have long concurred that the SCA does not authorize ongoing surveillance.[260]

For many years, this view was also shared by the Department of Justice. For example, FBI Director Louis Freeh testified before Congress in 1994 regarding proposed legislation (CALEA) to maintain wiretap and pen/trap surveillance capabilities in the face of technological advances in telecommunications. FBI Director Louis Freeh stressed that the proposed real-time surveillance legislation had nothing to do with telecommunications "transactional" information, which he emphasized "is *exclusively* dealt with in Chapter 121 of Title 18 of the United States Code ('stored wire and electronic communications and transactional records access')."[261]

This continued to be the considered view of the Department of Justice after the passage of the 2001 PATRIOT Act. Here is a passage from a 2009 DOJ brief to the Third Circuit in the first appellate case to consider whether the Fourth Amendment protects historical CSLI:

---

[259] 2 LAFAVE ET AL., *supra* note 17, § 4.6(b) n.27.

[260] *See* sources cited *supra* note 65.

[261] *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearing Before the Subcomm. on Tech. & the L. of the S. Comm. on the Judiciary and the Subcomm. on Civ. & Const. Rts. of the H. Comm. on the Judiciary*, 103d Cong. 32 (1994) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (emphasis added). For more background on this hearing, see *In re* Application for Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 762-64 (S.D. Tex. 2005).

> In crafting the federal statutes regulating governmental access to telecommunications records, Congress has unambiguously distinguished between historical (stored) and future records. Most prominently, Chapter 121 of Title 18 (the Stored Communications Act, [sections] 2701 *et seq.*) stands in contrast to the Wiretap Act (Chapter 119) and the pen register statute (Chapter 206), both of which exclusively regulate prospective, ongoing surveillance (of content and non-content, respectively). Thus, the mechanism for obtaining historical telephone calling records – a subpoena, as provided for at [section] 2703(c)(2)(C) – differs from the authority under the pen/trap statute for monitoring the telephone numbers of future calls to or from a target telephone.[262]

In a similar vein, the 2009 DOJ search and seizure manual instructed agents as follows: "[Section] 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the [Wiretap Act and the Pen/Trap statute]."[263]

The DOJ's understanding that the SCA did not authorize real-time surveillance is further confirmed by its initial approach to prospective cell phone tracking—the so-called "hybrid theory," which first surfaced in 2005. The government refused to accept that the Tracking Device Statute applied (for reasons we consider elsewhere), but also realized that, given its retrospective orientation, the SCA did not provide stand-alone authority to monitor cell phone location in real-time.[264] The DOJ attempted to

---

[262] Brief for the United States at 16, *In re* Application for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Recs. to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 3866618.

[263] *See* United States v. Warshak, 631 F.3d 266, 335 (6th Cir. 2010) (Keith, J., concurring) (alterations in original) (quoting OFF. OF LEGAL EDUC., U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 140 (2009)).

[264] As the leading judicial proponent of the hybrid theory wrote in 2005:

> The principal reason why [section 2703] does not serve easily as a fully independent source of authority for providing such data is a structural one: the statute does not contain certain procedural features, such as a time limitation, that Congress has typically included in statutes that permit the gathering of ongoing information.

avoid this conundrum by inventing the so-called "hybrid" order, which combined the record disclosure provisions of SCA section 2703(d) with the prospective monitoring features of the Pen Register Statute. For now, it is unnecessary to rehearse all of the detailed steps in the government's complicated argument.[265] The hybrid theory has been rejected by a majority of lower courts,[266] and the government never sought to test the theory in any reported appellate case.[267]

Ackies silently walks away from this long-standing consensus with no apparent recognition that it ever existed. What is the affirmative case in favor of extending the SCA to real-time surveillance? The court never says. Like the two district court opinions on which it relies, the *Ackies* court never identifies any flaws in the consensus view of the SCA. Its sole focus is why the TDS does *not* cover the continuous monitoring of cell phones, not why the SCA *does*.

The next section outlines some possibly pernicious consequences if *Ackies*' holdings are followed by courts outside the First Circuit.

III. WHY IT MATTERS

A. Surveillance Backdoors

By failing to observe the four-weddings-and-a-funeral dichotomy upon which ECPA was built, *Ackies* fundamentally alters the existing legal architecture of electronic surveillance law. Large swaths of ECPA become redundant if the SCA's "subpoena process"[268] is deemed to cover live surveillance. The result would be a statute rendered largely incoherent and (in at least one instance) unconstitutional.

In re Application for an Order for Disclosure of Telecomms. Recs. and Authorizing the Use of a Pen Reg. & Trap & Trace, 405 F. Supp. 2d 435, 447-48 (S.D.N.Y. 2005).

[265] *See In re* Application for an Order Authorizing (1) Installation and Use of a Pen Reg. & Trap & Trace Device or Process, (2) Access to Customer Recs., and (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 829-35 (S.D. Tex. 2006).

[266] *See* RICHARD M. THOMPSON, CONG. RSCH. SERV., R42109, GOVERNMENTAL TRACKING OF CELL PHONES AND VEHICLES: THE CONFLUENCE OF PRIVACY, TECHNOLOGY, AND LAW 12-13 (2011).

[267] *See generally* Freiwald & Smith, *supra* note 123, at 211-13.

[268] Carpenter v. United States, 138 S. Ct. 2206, 2215 n.2 (2018).

As shown in Part I, what distinguishes the SCA from the rest of ECPA is not subject matter, but mode of acquisition. Erase that dividing line, as *Ackies* has done, and the SCA overlaps the Wiretap Act, the Pen/Trap Statute, and the Tracking Device Statute. Law enforcement can then use an SCA order as an alternative route to acquire the same data covered by those three statutes (communications content, non-content, and location data) on the same continuous basis. The SCA would thereby become a sort of surveillance "wild card"; or, to borrow the words of one government official in a slightly different context, it is a game of "dealer's choice and the government is the dealer."[269]

For law enforcement, the game of choice will almost always be the SCA. Its provisions would allow one-stop shopping for both retrospective and prospective communications and customer records. If the provider's "disclosure" obligation under section 2703 is stretched to include real-time monitoring, then it will become easier to get a backdoor wiretap under section 2703(a) than to comply with the Wiretap Act; easier to get a backdoor tracking warrant under section 2703(c)(1) than to comply with the Tracking Device Statute; and easier to get a backdoor pen register under section 2703(c)(2) than to comply with the Pen/Trap Statute. It is difficult to believe Congress had such slippery redundancy in mind when it enacted ECPA.

Maintaining the distinction between record-disclosure and ongoing surveillance is necessary to ensure not only the coherence of ECPA's regulatory regime, but also its constitutionality.[270] Of the three surveillance backdoors listed above, backdoor wiretapping under section 2703(a) poses the most serious threat to the Fourth Amendment. Here is the problem.

---

[269] Albert Gidari, *US and UK CLOUD Act Wiretapping in Third Countries: It Is a Real Problem*, CTR. FOR INTERNET & SOC'Y (Oct. 24, 2019, 10:17 AM) http://cyberlaw.stanford.edu/blog/2019/10/us-and-uk-cloud-act-wiretapping-third-countries-it-is-a-real-problem [https://perma.cc/3CNH-3DQR] (recounting a conversation with government officials on the issue of where an interception occurs under the Wiretap Act).

[270] SCA section 2703(b) has already been found unconstitutional to the extent it permits the government to obtain emails via administrative subpoena or section 2703(d) order. *See* 18 U.S.C. § 2703(b), (d); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

Section 2703(a) allows the government to "require the disclosure . . . of the contents of a wire or electronic communication, that is in electronic storage . . . for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure."[271] There is no minimum storage duration requirement; ECPA's definition of the term includes "any temporary, intermediate storage . . . incidental to the electronic transmission."[272] So, if disclosure equals continuous monitoring under 2703(a), then the government can effectively procure a wiretap using only a Rule 41 probable cause warrant. This would of course violate the Fourth Amendment under *Berger*, where the Supreme Court imposed stringent additional requirements for surveillance techniques like eavesdropping and wiretapping, which involve a continuous "series of intrusions," unlike an ordinary search or seizure.[273] As Sixth Circuit Judge Keith recognized in *Warshak*, construing the SCA to permit prospective monitoring of emails would amount to "back-door wiretapping," a practice both impermissible under the Fourth Amendment and contrary to the purpose of the statute as a whole.[274]

Logically speaking, there is very little daylight between the *Ackies*-approved GPS ping orders under 2703(c) and a backdoor wiretap under 2703(a). The key step is ongoing monitoring—once that camel's nose is under the 2703 disclosure tent, the game is up. *Ackies* itself foreshadows this result, often referring to SCA section 2703(a) in the course of its opinion.[275]

---

[271] 18 U.S.C. § 2703(a).

[272] 18 U.S.C. § 2510(17)(A).

[273] Berger v. New York, 388 U.S. 41, 59 (1967).

[274] *Warshak*, 631 F.3d at 335 (Keith, J., concurring). Magistrate Judge James Orenstein was the first to make this point in an early cell site decision. *See In re* Application for an Order (1) Authorizing the Use of a Pen Reg. & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 313-14 (E.D.N.Y. 2005).

[275] At one point, the opinion mistakenly asserted that the PLI warrants in question were issued under *both* sections 2703(a) *and* 2703(c)(1)(A). *See* United States v. Ackies, 918 F.3d 190, 198 (2019). A few pages earlier, the opinion had correctly noted that the warrants were obtained under "[section] 2703(c)(1)(A) and Rule 41." *Id.* at 195-96. The district court record confirms that the warrant application did not invoke section 2703(a). *See* United States v. Ackies, No. 16-cr-20, 2017 WL 3184178, at *2 (D. Me. July 26, 2017).

It may be argued that the exclusivity provisions of the Wiretap Act would forestall such a result.[276] However, the line between a communication "intercept" and a communication in "electronic storage" is fuzzy.[277] In early CSLI cases, the government argued that electronic data instantaneously becomes a "record" as soon as it is retrievable from the provider's network, a matter of seconds or nanoseconds.[278] It would be a trivial matter to construct a system in which communication contents are digitally stored for a few seconds before their transmittal to law enforcement.[279] Such a continuous series of intrusions would arguably not constitute an "intercept" under the Wiretap Act, but would likely violate the additional constitutional protections imposed by *Berger*.

Has SCA section 2703(a) been used for backdoor wiretapping in the manner described here? No such cases have been reported to date. But that is no reassurance—the SCA is notoriously the most secretive of ECPA's surveillance regimes, as discussed below.

B. Notice and Transparency

It is true that a PLI warrant and a Rule 41 tracking warrant both require a showing of probable cause. Beyond that similarity, however, lie several important differences.

One significant, possibly constitutional-level difference is notice. Unlike a normal search warrant, a PLI warrant issued under SCA section 2703(c) does not require notice to the target. Under SCA section 2703(c)(3), "[a] governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer."[280] The only party receiving notice of an SCA order or warrant for transactional records is the third-party provider, who is typically subject to a gag

---

[276] *See* 18 U.S.C. § 2511.

[277] 18 U.S.C. § 2510(4), (17).

[278] *In re* Order Authorizing Prospective & Continuous Release of Cell Site Location Recs., 31 F. Supp. 3d 889, 893 (S.D. Tex. 2014). *See also In re Application*, 396 F. Supp. 2d at 312.

[279] A similar "seven second delay" was invented for talk radio in the 1950s to guard against broadcast profanity. See Steely Dan's classic song "The Nightfly," in which a disc jockey cautions late-night callers to "turn your radio down/Respect the seven second delay we use." *Donald Fagen – The Nightfly Lyrics*, GENIUS, https://genius.com/Donald-fagen-the-nightfly-lyrics [https://perma.cc/LK5V-YM8X] (last visited Nov. 3, 2021).

[280] 18 U.S.C. § 2703(c)(3).

order forbidding them from telling customers that law enforcement has accessed their cell phone or email account records.[281]

By contrast, Rule 41 requires that, within ten days after the use of a tracking device, law enforcement "must serve a copy of the warrant on the person who was tracked or whose property was tracked."[282] Merely notifying the provider is insufficient. In addition, the officer executing the warrant must "enter on it the exact date and time the device was installed and the period during which it was used," before returning the warrant to the issuing judge.[283] None of these things are required by the SCA.

Lack of notice to the target is problematic for two reasons. First of all, it may be unconstitutional, especially now that the Supreme Court has ruled that cell site location data is protected by the Fourth Amendment.[284] A still-viable precedent from the Ninth Circuit holds that a warrant for surreptitious search and seizure of intangibles is "constitutionally defective" if it "fail[s] to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry." According to that court:

> [S]urreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed.[285]

The lack of a notice requirement is concerning on another, equally fundamental level—transparency in government. Federal court orders and warrants under ECPA make up the largest secret

---

[281] 18 U.S.C. § 2705(b).

[282] FED. R. CRIM. P. 41(f)(2)(C).

[283] FED. R. CRIM. P. 41(f)(2)(A)-(B).

[284] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[285] United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986). At least one circuit has declined to follow the Ninth Circuit's lead. *See* United States v. Pangburn, 983 F.2d 449, 455 (2d Cir. 1993) ("We prefer to root our notice requirement in the [implicit] provisions of Rule 41 rather than in the somewhat amorphous Fourth Amendment 'interests' concept developed by the *Freitas I* court.").

docket in our country.[286] The SCA is by far the least transparent of ECPA's three titles. Wiretap orders require subsequent notice to the target as well as detailed reports concerning each order; those reports are then aggregated and published by the Administrative Office.[287] Pen/trap orders do not require individualized notice, but the DOJ is required to publish annual reports on the number of pen/trap orders obtained.[288]

By contrast, there are no reporting requirements for SCA orders. That means there is no official tab of how many times the government has accessed our phone records and email accounts or how often law enforcement covertly monitors our daily movements via the tracking device we all carry in our pockets. If provider transparency reports are any indication, those numbers are large indeed. AT&T alone has reported 18,344 real-time location requests from U.S. law enforcement in 2020—more than nine times its volume of wiretap orders and twice the number of pen register orders during that same period.[289] T-Mobile (which recently merged with Sprint) reports 81,678 prospective location requests in 2020—more than eighteen times its number of wiretaps and nearly four times the number of pen registers.[290]

These numbers suggest that live cell phone tracking has now become the surveillance tool of choice for U.S. law enforcement. In fact, based on my own review of Houston docket records, it appears that cell phone tracking warrants are becoming nearly as common as ordinary search warrants:

---

[286] *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 314-15 (2012).

[287] 18 U.S.C. § 2519(2)-(3).

[288] 18 U.S.C. § 3126.

[289] *See AT&T February 2021 Transparency Report*, AT&T 4 (Feb. 11, 2021), https://about.att.com/ecms/dam/csr/2019/transparency/2021/2021-February-Report.pdf [https://perma.cc/SFM6-WJ42]; *AT&T August 2020 Transparency Report*, AT&T 4 (Aug. 20, 2020), https://about.att.com/ecms/dam/csr/2019/library/transparency/2020-August-Report.pdf [https://perma.cc/DJE5-APVA].

[290] *T-Mobile US, Inc. Transparency Report for 2020*, T-MOBILE 5-6, https://www.t-mobile.com/news/_admin/uploads/2021/07/2020-Transparency-Report.pdf [https://perma.cc/Q4ZE-EEU8] (last visited Nov. 4, 2021). T-Mobile's 2020 report also shows 109,534 requests for historical cell site information as well as 92,975 requests for "timing advance" information, which "identifies the historical location of a handset, delivered as longitude and latitude coordinates to a government requestor." *Id.* at 6.

FY	Standard Search Warrants	Cell Phone Tracking Warrants
2013	198	112
2014	284	87
2015	242	137
2016	200	195
2017	265	185
TOTAL	1,189	716

During this five-year period, the number of cell phone tracking warrants was more than half (60%) the number of search warrants for tangible property like homes, offices, autos, and mail packages.[291] In one of those years (FY 2016), the number of cell phone tracking warrants nearly equaled the number of standard search warrants – 195 to 200, a ratio of 97.5%.

There is no reason to believe that the Houston docket numbers are unrepresentative of federal courts nationwide. Unfortunately, similar statistics are not available from other district courts due in large part to the lack of reporting and notice requirements for SCA orders.[292] One of the troubling consequences of *Ackies* is a likely increase in court orders that will be routinely withheld not only from the public, but also the target himself.

C. Unbounded Tracking

As the *Ackies* case illustrates, an SCA warrant dramatically widens the geographical scope of law enforcement surveillance authority. Under Rule 41, a court sitting in Maine has no authority to issue a search warrant for a home in New York, no matter how much probable cause there is. Nor could that court issue a tracking warrant to place a GPS tracker on a vehicle in New York, even if the driver was a notorious drug lord. Yet, under *Ackies*, a Maine magistrate judge may authorize thirty-days of continuous GPS

[291] Numbers compiled by the author from the Southern District of Texas, Houston Division docket records (on file with the author and the Mississippi Law Journal).

[292] The Administrative Office does publish district-wide search warrant numbers in its annual Judicial Business Report. *See, e.g.*, *Table M-3: U.S. District Courts—Felony Preliminary Proceedings Handled by U.S. Magistrate Judges Under 28 U.S.C. § 636(a) During the 12-Month Period Ending September 30, 2019*, U.S. CTS. (Sept. 30, 2019), https://www.uscourts.gov/file/27632/download [Perma.cc link unavailable].

tracking of cell phones in New York or anywhere in the world within reach of a U.S. telecom carrier.

Like it or not, this is a big departure from the usual territorial restrictions on a magistrate judge's warrant authority. Normally, a magistrate judge "has authority to issue a warrant to search for and seize a person or property located within the district."[293] This territorial restriction is not a problem when the object of the search is fixed and unlikely to move outside the district of the issuing judge. A complication arises when the target of the search is mobile and likely to cross district or state lines after the warrant is issued but before it can be executed. The territorial principle might have required law enforcement to obtain multiple tracking warrants from courts in different jurisdictions.

To avert this venue problem, Congress and the Supreme Court settled on a compromise: a magistrate judge may authorize out of district monitoring so long as the installation occurs within the district.[294] Significantly, neither Rule 41(b)(4) nor section 3117(a) distinguishes between the tracking of persons or objects. The same rules apply to both. Yet, the SCA warrant would create a special venue rule for tracking of persons via the cell phones they carry. Because cell phone tracking is the predominant method used by law enforcement to track persons, this will mean one set of rules for tracking objects like vehicles and another set of rules for tracking persons.

Perhaps one could reasonably debate whether it might be good policy to carve out a special venue exception for tracking cell phones. The fact is that no such debate has occurred, whether in Congress or the Rules Committee. Instead, courts are being asked to create such an exception based on *ex parte* applications from law enforcement agencies with a history of pushing the outer limits of their statutory authority.[295] Nor are the territorial concerns about

---

[293] FED. R. CRIM. P. 41(b)(1).

[294] FED. R. CRIM. P. 41(b)(4). *See also* FED. R. CRIM. P. 41(b)(4) Advisory Committee's Notes to 2006 Amendments ("Even where officers have no reason to believe initially that a person or property will move outside the district of issuance, issuing a warrant to authorize tracking both inside and outside the district avoids the necessity of obtaining multiple warrants if the property or person later crosses district or state lines.").

[295] *See* Hon. James Orenstein, Opinion, *I'm a Judge. Here's How Surveillance Is Challenging Our Legal System.*, N.Y. TIMES (June 13, 2019),

PLI warrants strictly a domestic matter. With the passage of the CLOUD Act in 2018, Congress extended the jurisdictional reach of the SCA. Under the new SCA section 2713, a provider can be compelled to disclose communication content and subscriber information within its possession, custody, or control, "regardless of whether such communication, record, or other information is located within or outside of the United States." For example, Microsoft Corporation can now be compelled by an SCA warrant to disclose emails held on foreign servers operated by its non-U.S. subsidiaries.

By the same logic, PLI warrants served upon U.S.-based global telecommunication conglomerates will now have international reach. For example, AT&T has affiliates in Canada, Mexico, Latin America, and in many countries throughout the Asia Pacific.[296] Under *Ackies*' expansion of the SCA to cover cell phone tracking, U.S. prosecutors will be able to leverage the global presence of U.S. multinational telecoms to enable real-time tracking of cell phones in foreign countries around the world. While some may cheer, there are significant causes for concern about such a development, particularly with regard to international law and foreign relations.

Under international law, while a state may have *prescriptive* jurisdiction to criminalize foreign conduct that has domestic effects, its *enforcement* jurisdiction "continues to be strictly territorial."[297] According to the ALI's Restatement of Foreign Relations Law, "[a] state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."[298] Under this rule, law enforcement's search and seizure authority does not generally

---

https://www.nytimes.com/2019/06/13/opinion/privacy-law-enforcment-congress.html [https://perma.cc/H7GB-FSRW].

[296] *See AT&T Around the World*, AT&T BUS., https://www.corp.att.com/worldwide/att-around-the-world/ [https://perma.cc/3MZX-3BEM] (last visited Nov. 4, 2021). Verizon Communications also has a worldwide presence with 132,200 employees in more than 150 global locations. S. O'Dea, *Number of Employees at Verizon from 2007 to 2020*, STATISTA (Mar. 17, 2021), https://www.statista.com/statistics/257304/number-of-employees-at-verizon/ [https://perma.cc/HT24-SSHL].

[297] FTC v. Compagnie de Saint-Gobain-Pont-a-Mousson, 636 F.2d 1300, 1316 (D.C. Cir. 1980).

[298] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 432(2) (AM. L. INST. 1987).

extend beyond the territorial United States.[299] An SCA order authorizing the government to continuously monitor a cell phone used by a foreign criminal suspect operating outside U.S. borders would arguably violate international law.[300]

Rule 41 follows the normal presumption against extraterritorial application of U.S. law and does not authorize searches and seizures on foreign soil.[301] This presumption is undergirded by important foreign relations imperatives, including mutual respect for national sovereignty. The Supreme Court has paid special heed to these concerns in the past. In 1990, the Court disapproved a proposed amendment to Rule 41 that authorized warrants to search property outside the United States.[302]

Of course, Congress has the power to override this presumption in particular circumstances, and the CLOUD Act did just that in a limited way—but only for content and subscriber information stored abroad under the control of a U.S. provider. Did the CLOUD Act Congress understand that it was permitting U.S. law enforcement to track cell phones in foreign countries? Nothing suggests that it did. At the time the law was passed in 2018, a majority of reported district court opinions had held cell phones to be Rule 41 tracking devices.[303] Nor had any appellate court held otherwise, save for the initial *Wallace* opinion withdrawn by the Fifth Circuit in August 2017.[304]

It is true that an SCA tracking warrant must clear the usual jurisdictional hurdles—competent jurisdiction by the court over the crime committed and sufficient contacts by the provider with the forum. As the swelling numbers of SCA tracking warrants demonstrate, these are not high hurdles. Given the continuing expansion of U.S. multi-national telecoms, the digital intrusion

---

[299] *See generally* Ghappour, *supra* note 106, at 1099-1105.

[300] *See generally* Stephen W. Smith, *Clouds on the Horizon: Cross-Border Surveillance Under the US CLOUD Act*, *in* DATA PROTECTION BEYOND BORDERS: TRANSATLANTIC PERSPECTIVES ON EXTRATERRITORIALITY AND SOVEREIGNTY (Federico Fabbrini, Edoardo Celeste & John Quinn eds., 2021).

[301] *See* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 261 (2010) ("[W]e apply the presumption in all cases.").

[302] FED. R. CRIM. P. 41 Advisory Committee's Notes to 1990 Amendments.

[303] *See* Smith, *supra* note 300.

[304] *See supra* notes 254-57 and accompanying text.

upon the territorial sovereignty of other countries will continue to grow.

Consequently, *Ackies* may have inaugurated a new form of global surveillance without any consideration of the serious implications for U.S. foreign relations or of settled international law principles limiting the operations of domestic law enforcement on foreign soil.

D. "Strategic Duplicity"

A commonplace among law enforcement critics is the lack of candor in warrant applications, particularly those involving new investigative techniques.[305] Anodyne terms like "network investigative technique" and "precise location information warrant" seem calculated to minimize the intrusiveness of the surveillance to be conducted. Without an adequate grasp of the particular technology to be employed and the privacy risks involved, a magistrate judge may well authorize a search or seizure of far greater scope than is intended or justified.

A case in point is the NIT warrant underlying the Operation Playpen investigation. Pursuant to this single warrant, the FBI installed malware on more than 8,000 computers in 120 countries around the world.[306] The warrant was challenged in dozens of courts around the country with many judges pointing to the defective warrant application. Probably the severest critic was Judge Gerald Tjoflat of the Eleventh Circuit, who charged the government with breaching its duty of candor in submitting a jurisdictionally defective and misleading NIT warrant application. In a partial dissent, he charged that law enforcement:

---

[305] *See, e.g.*, *In re* Application for an Order Authorizing the Installation and Use of a Pen Reg. & Trap & Trace Device, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012).

[306] *See* Brief of the United States, *supra* note 107, at 6-8.

> knew or should have known that there was an issue with jurisdiction and that the search would occur outside the district. Yet, the officials told the magistrate repeatedly that the search would take place in the district. If the law condones this conduct, it makes a mockery of the warrant process.[307]

Responding to the government's contention that a single passage buried at page 29 of a 31-page affidavit somehow "cured" the warrant of ambiguity, Judge Tjoflat was unforgiving:

> This sets too low a bar. It essentially gives officials permission to try to hoodwink magistrates: they can make false statements to the court so long as they include enough information to uncover their chicanery. . . . I refuse to invite such gamesmanship.[308]

> I cannot believe that the law expects so little of law enforcement, or so much of magistrates. . . . This is a system designed to encourage mistakes.[309]

> Instead, we should demand the utmost candor in warrant applications. Before today, I thought we did. . . . Otherwise, we excuse conduct, like the conduct at issue here, which invites strategic duplicity into the warrant process.[310]

Strong words indeed. One wonders how much stronger they would have been had Judge Tjoflat been aware that the government's tracking device argument directly contradicted its legal position simultaneously taken before another federal appellate court.

As shown, this is not the only reversal of position by the government in arguing for PLI warrants. The government has previously opposed four of the key legal propositions it successfully proposed to the *Ackies* panel:

Reversal #1. The TDS requires physical installation of hardware. While government prosecutors vigorously pursued this line of argument in the *Ackies* litigation, federal prosecutors in ten

---

[307] United States v. Taylor, 935 F.3d 1279, 1293 (11th Cir. 2019) (Tjoflat, J., concurring in part and dissenting in part) (footnote omitted).

[308] *Id.* at 1300.

[309] *Id.* at 1303.

[310] *Id.* at 1303-04.

circuit courts and dozens of district courts were busy pressing the opposing line with equal vigor—i.e., that remotely installed software via a NIT warrant *was* a tracking device within the meaning of TDS section 3117(b).[311] The near-verbatim language in government briefs filed in ten different circuits leaves no doubt that the DOJ itself was coordinating the government's legal arguments in these cases.[312]

Reversal #2. The TDS covers only homing devices. Federal prosecutors have taken full advantage of GPS tracking technology since it became available for civilian use over two decades ago. The GPS cell phone-based tracking device which gave rise to the Supreme Court decision in *Jones* was installed in 2005.[313] Another highly-publicized, non-homing device case was *United States v. Rigmaiden*, in which the government obtained a tracking device warrant for a cell site simulator.[314] Neither GPS trackers nor cell site simulators are homing devices, yet the government routinely applies for tracking warrants to authorize their use.[315]

Reversal #3. GPS pings are provider records. A prominent DOJ spokesman told Congress in 2011 that GPS ping data are not

---

[311] *See supra* text accompanying note 109.

[312] *See* Government's Opening Brief, *supra* note 111, at 27 ("As applied to newer technologies, the Rule envisions that a tracking device may be an electronic device used to track the movement of information – e.g., computer instructions embedded in digital content traveling on data highways, like the NIT in this case."); Brief for the United States, *supra* note 105, at 22 (same); Brief for Appellee United States of America, *supra* note 109, at 31 (same); Brief for Appellee United States at 13, United States v. Moorehead, 912 F.3d 963 (6th Cir. 2019) (No. 18-5216), 2018 WL 3526403, at *13 (same); Brief of Plaintiff-Appellee at 22, United States v. Kienast, 907 F.3d 522 (7th Cir. 2018) (No. 17-1840), 2017 WL 4315962, at *22 (same); Government's Opening Brief at 21-22, United States v. Horton, 863 F.3d 1041 (8th Cir. 2017) (Nos. 16-3976 & 16-3982), 2016 WL 6905741, at *21-22 (same); Brief for the United States at 17, United States v. Henderson, 906 F.3d 1109 (9th Cir. 2018) (No. 17-10230), 2018 WL 1136328, at *17 (same); Brief for the United States at 20, United States v. Workman, 863 F.3d 1313 (10th Cir. 2017) (No. 16-1401), 2016 WL 7536312, at *20 (same); Brief of the United States at 15, United States v. Taylor, 935 F.3d 1279 (11th Cir. 2019) (No. 17-14915), 2018 WL 1635452, at *15 (same). In another Playpen appeal, the government's brief is unavailable on Westlaw, but the defendant's reply brief leaves no doubt that the government had made the NIT tracking device argument. *See* Reply Brief of the Appellant at 2, United States v. McLamb, 880 F.3d 685 (4th Cir. 2018) (No. 17-4299), 2017 WL 3394910, at *2.

[313] United States v. Jones, 565 U.S. 400, 402-03 (2012).

[314] *See* discussion *supra* Section I.B.3.

[315] During my fourteen years as a magistrate judge, I issued dozens of such tracking warrants.

maintained by the provider in the ordinary course of business and cautioned that courts should not conflate such data with cell site records which are maintained by providers. Similar instructions were given to FBI agents in their domestic investigation manual. In 2017, federal prosecutors apologized to the Fifth Circuit for failing to clarify this distinction in an earlier brief, which led to the court's withdrawal of its initial opinion.[316]

Reversal #4. The SCA authorizes ongoing surveillance. During its first quarter-century of existence, the SCA was understood as a record-production regime, aimed at retrospective rather than prospective electronic surveillance.[317] Even when, post-PATRIOT Act, the government began pushing the hybrid theory as justification for prospective CSLI, it was conceded that the SCA alone was inadequate to the task due to its retrospective orientation.[318] In 2009, DOJ appellate advocates told the Third Circuit that the SCA did not regulate prospective ongoing surveillance.[319] The DOJ advised agents that the proper legal mechanisms to obtain future communications data were the Wiretap Act and the Pen/Trap Statute rather than the SCA.[320]

This is a remarkable set of U-turns to find in a single case; even more remarkably, none of these reversals of position are addressed, much less justified, in the government's briefing. Ordinarily, courts take a dim view of litigants advancing inconsistent legal positions in court. The Fifth Circuit has a disparaging term for such litigation tactics—"trifl[ing] with the [c]ourt."[321] The practice is especially disturbing when the trifling party is the government itself. An oft-cited First Circuit opinion, joined by then-Circuit Judge Stephen Breyer, explains why:

> This inconsistency is troubling where its source is the prosecutorial arm of the federal government. . . . The criminal trial should be viewed not as an adversarial sporting contest,

---

316 *See supra* note 256 and accompanying text.

317 *See, e.g.*, Mulligan, *supra* note 65, at 1567 ("The SCA covers retrospective surveillance of both content and noncontent information.").

318 *See supra* note 264 and accompanying text.

319 Brief for the United States, *supra* note 262, at 16.

320 *See* United States v. Warshak, 631 F.3d 266, 335 (6th Cir. 2010) (Keith, J., concurring) (quoting OFF. OF LEGAL EDUC., *supra* note 263, at 140).

321 United States v. Cuevas-Sanchez, 821 F.2d 248, 250 (5th Cir. 1987).

> but as a quest for truth. . . . Thus, it is disturbing to see the Justice Department change the color of its stripes to such a significant degree, . . . depending on the strategic necessities of the separate litigations.[322]

The *Ackies* courts, both trial and appellate, were simply not well served by the government advocates before them. Rather than candidly acknowledge the flaws in their novel legal theory, these prosecutors made arguments that contradicted official DOJ pronouncements to other courts and even to Congress. Whatever you call it—strategic duplicity, strategic necessity, or trifling with the courts—this approach to investigative powers may bring success in the short term. But prosecutors reflexively pushing the most aggressive tack on surveillance authority will eventually pay a hefty toll in the coin of professional credibility. Losing the benefit of judicial doubt in warrant applications would be a serious loss indeed for agents and prosecutors.

CONCLUSION

For many years now, a standard refrain in judicial opinions, when forced to confront the widening gap between law and new surveillance technology, has gone something like this: "The law is wildly behind the times and must be updated. But this is not a job for courts, for we are institutionally ill-equipped to grasp the nuances of technology and make the most rational policy choices. This is a job for Congress, which has neglected its duty far too long."[323] Academic voices often join the swelling chorus for modernizing legislation.[324]

Yet, in the case of tracking devices, Congress did its duty. The 1986 Congress, anticipating the communications technology revolution by then already underway, passed a technology-neutral law placing territorial limits on their use. Subsequently, Congress approved amendments to Rule 41 elaborating the procedures for such tracking warrants. The regulatory scheme for handling cell

---

[322] United States v. Kattar, 840 F.2d 118, 127 (1st Cir. 1988).

[323] *See, e.g.*, United States v. Jones, 565 U.S. 400, 429-30 (2012) (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.").

[324] *See, e.g.*, Freiwald, *supra* note 65, at 79-84.

phone tracking warrants was now complete with plenty of flexibility to cover future advances in technology like smartphones and satellite-based geolocation gear.

It is no small irony then to find an appellate court sweeping aside unambiguous legislation and procedural rules, replacing them with provisions from a different law serving a different purpose. While government advocates might fairly be apportioned some of the blame, ultimate responsibility must lie with the court. The legal missteps detailed here might have been avoided if the court had not endorsed the fiction that a cell phone is not a tracking device.

Appellate decisions make easy targets for academic critics, writing at leisure, unconstrained by incomplete factual records, inadequate briefs, lazy lawyers, or hazy precedents. This is especially true for cases construing ECPA, a notoriously complex statute, challenging to understand, let alone master. Having wrestled with this statute for fourteen years as a magistrate judge, I sympathize.

But sympathy has its limits. *Ackies* is, in my view, not just incorrectly decided. Even more troubling, it is a case of first impression at the appellate level. Most circuits make a practice of avoiding circuit splits absent a compelling reason,[325] a policy some might uncharitably describe as the "Lemming Rule." If the initial circuit to rule on a question gets it wrong, then other circuits are more likely to hurl themselves headlong onto the same beach, long before the Supreme Court is able to set matters straight.[326]

Those circuits can avoid the fate of lemmings by taking a critical look at the rickety legal architecture of the PLI warrant. They should also hold government attorneys to account for opportunistic advocacy. Otherwise, our electronic surveillance laws will become less coherent and less privacy-protective, not simply due to the relentless march of technology, but because courts create donut holes that swallow up entire statutes.

---

[325] *See* United States v. Thomas, 939 F.3d 1121, 1130-31 (10th Cir. 2019) (collecting cases).

[326] This was the case in *Carpenter*, where the Supreme Court reversed the unanimous view of the five circuits who had ruled on the historical cell site issue. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).