# Rediscovering the Tracking Device Statute

Haley Amster*

24 STAN. TECH. L. REV. 344 (2021)

ABSTRACT

Tracking devices have long been staples in the government's investigatory toolkit. But law enforcement's tracking device of choice is now the suspect's own cell phone. In the burgeoning litigation after *Carpenter v. United States* over protections for prospective cell phone location information, the Tracking Device Statute (TDS)—enacted as a part of the 1986 Electronic Communications Privacy Act (ECPA)—has been overlooked as an avenue to regulate law enforcement usage of cell phones as investigative tools.

This Note first argues that cell phones are properly classified as tracking devices under ECPA and prospective location information can only be obtained under the provisions of the TDS. This Note then explains why the only federal appellate decision squarely addressing the issue, the First Circuit's 2019 decision in *United States v. Ackies*, is wrongly decided. This Note concludes with a consideration of other technologies,

* J.D. Candidate, Stanford Law School, 2021. My deepest thanks to Judge Stephen Smith and Professor Robert Weisberg for their encouragement, insights, and invaluable guidance. Many thanks as well to the editors of the *Stanford Technology Law Review*, especially Tanner Kuenneth.

applying the TDS to wearable health monitors, computers, and other devices in the smart home.

TABLE OF CONTENTS

## I. INTRODUCTION

In the early 1980s, law enforcement secretly placed location trackers on suspects' vehicles in order to follow their whereabouts in real time.[1] But today's investigators need not go through the trouble of securing such devices; they need only access a suspect's cell phone location information in order to conduct what the Supreme Court described in *Carpenter v. United States* as "near perfect surveillance."[2]

While mandating probable cause protections for *historical* location information, the *Carpenter* Court left open the question of protections for *prospective* location information.[3] Writing for the majority, Chief Justice Roberts issued a narrow decision with a series of caveats, explaining the decision "[did] not express a view on matters not before us," including "real-time [cell site location information]."[4]

With the Supreme Court punting the question of ongoing cell phone surveillance, the debate about protections for prospective location information continues.[5] But litigants have paid far too little attention to

---

[1] *See* United States v. Karo, 468 U.S. 705 (1984) (beeper placed in can of chemicals to track location); United States v. Knotts, 460 U.S. 276 (1983) (same).

[2] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

[3] Cell phone location information is categorized as either historical or prospective. Historical location information refers to records that "detail the location of a cell phone in the past (i.e.: prior to entry of the court order authorizing government acquisition)." *In re* Installation & Use of a Pen Reg., 402 F. Supp. 2d 597, 599 (D. Md. 2005). Prospective location information refers to "[location] information that is generated after the government has received court permission to acquire it." *Id.* "Real-time" location information and "ongoing surveillance" also refer to prospective location information. Real-time location information "refers to data used by the government to identify the location of a phone at the present moment," but this information is still prospective location information, as it is generally acquired after the issuance of a court order. *Id.* Ongoing surveillance refers to the regular acquisition of prospective location information, in contrast with one-time pings for location information.

[4] *Carpenter*, 138 S. Ct. at 2220.

[5] The question of constitutional protections for acquisition of prospective location

the maze of already-existing federal statutory regulations of electronic communications, dating back to the 1980s. Specifically, the statute governing tracking devices—the Tracking Device Statute (TDS), enacted as a part of the 1986 Electronic Communications Privacy Act (ECPA)—has been overlooked as an avenue for regulating law enforcement usage of cell phones as investigative tools.[6]

---

information was unresolved before *Carpenter*. *Compare* Jones v. United States, 168 A.3d 703, 713 (D.C. 2017) (holding that use of a cell-site simulator to track a suspect's phone in real-time "invaded a reasonable expectation of privacy and was thus a search"), *with* United States v. Riley, 858 F.3d 1012, 1018 (6th Cir. 2017) (holding that the "government did not conduct a search under the Fourth Amendment when it tracked the real-time GPS coordinates of" the suspect's phone outside of the home for seven hours). Some courts noted this issue was an open question. *See, e.g.*, United States v. Wallace, 866 F.3d 605, 609 (5th Cir. 2017), *withdrawn and superseded*, 885 F.3d 806 (5th Cir. 2018). The question of constitutional protections for obtaining prospective location information remains unresolved after *Carpenter*. *See generally* Eric Lode, Annotation, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1 (2015).

[6] Litigants have overlooked raising the TDS as an issue before courts, instead focusing on whether real-time location information from a cell phone is a search and whether the *Carpenter* holding extends. *See, e.g.*, Corrected Brief for Defendant at 25, Commonwealth v. Almonor, 120 N.E.3d 1183 (Mass. 2019) (No. SJC-12499) (asserting that real-time location pings "turns cellphones into tracking devices," but only arguing this violates constitutional rights, without mentioning statutory violations); Brief of Amici Curiae Elec. Frontier Found. et al. at 15, *Almonor*, 120 N.E.3d 1183 (No. SJC-12499) (same); Motion for Leave of Court to File a Supplemental Brief Based on *Carpenter v. United States* (handed down June 22, 2018) with the Supplemental Brief Included at 17, Sims v. State, 569 S.W.3d 634 (Tex. Crim. App. 2019) (No. PD-0941-17) (focusing on the constitutional question, mentioning the Stored Communications Act, but not mentioning the TDS); Appellant's Brief at 24-26, *Sims*, 569 S.W.3d 634 (No. PD-0941-17) (focusing on the constitutional question, mentioning the Wiretap Act, but not mentioning the TDS).

Prior to *Carpenter*, legal scholarship lightly explored the possibility of cell phones as tracking devices under the TDS, but this statute has received almost no attention in legal scholarship for many years. *See generally* Steven B. Toeniskoetter, *Preventing a Modern Panopticon: Law Enforcement Acquisition of Real-Time Cellular Tracking Data*, 13 RICH. J.L. & TECH. 16, 39 (2007) (briefly asserting the TDS is "irrelevant to determining the proper standard the government must meet in order

In order to access prospective location information from a suspect's cell phone, law enforcement has long sought non-TDS authorization within ECPA's statutory scheme, bobbing and weaving through

---

to obtain real-time cell site data"); Brian L. Owsley, *Cell Phone Tracking in the Era of* United States v. Jones *and* Riley v. California, 48 TEX. TECH L. REV. 207, 220-22 (2015) (agreeing with fellow magistrate judge decisions holding that a cell phone is a tracking device); M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1473 (2007) (primarily summarizing case law on government access to real-time information, and noting "[i]t would appear clear that on the statute's face, a cell phone easily fits within the term 'tracking device'").

Since *Carpenter*, Stephen Smith appears to be the only legal scholar to pay significant attention to the TDS. *See* Stephen Wm. Smith, *The Cellphone Donut Hole in the Tracking Device Statute*, FED. CT. L. REV. (forthcoming 2021); Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 208-11 (2018); Stephen Wm. Smith, *Trifling with the Courts*, CTR. INTERNET & SOC'Y BLOG (Jan. 30, 2020, 1:06 PM), https://perma.cc/SC93-TXAR; Stephen Wm. Smith, *Twisted Tracking Law Precedent Badly Needs Straightening Out*, CTR. INTERNET & SOC'Y BLOG (Jan. 14, 2020, 11:46 AM), https://perma.cc/V8VW-F2LB; Stephen Wm. Smith, *Why Are Precise Location Warrants a Thing?*, CTR. INTERNET & SOC'Y BLOG (Dec. 10, 2019, 4:50 PM), https://perma.cc/ZG6F-575B; Stephen Wm. Smith, *Losing Track of the Tracking Device Statute*, CTR. INTERNET & SOC'Y BLOG (Dec. 5, 2019, 11:11 AM), https://perma.cc/9HPF-GVVA.

Post-*Carpenter* scholarship has instead focused largely on the question of extending the *Carpenter* constitutional holding to prospective location information, neglecting questions of ECPA interpretation. *See, e.g.*, Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 375-76 (2019) (noting *Carpenter* should extend to real-time location information by its own reasoning, not addressing ECPA issues); Matthew DeVoy Jones, *Cell Phones Are Orwell's Telescreen: The Need for Fourth Amendment Protection in Real-Time Cell Phone Location Information*, 67 CLEV. ST. L. REV. 523, 524 (2019) (same); Michael Gentithes, *The End of* Miller*'s Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 GA. L. REV. 1039, 1072 (2019) (same); Daniel de Zayas, Carpenter v. United States *and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 AM. U. L. REV. 2209, 2243 (2019) (same); Lara M. McMahon, *Limited Privacy in "Pings:" Why Law Enforcement's Use of Cell-Site Simulators Does Not Categorically Violate the Fourth Amendment*, 77 WASH. & LEE L. REV. 981, 1027 (2020) (arguing *Carpenter* does not extend to real-time cell site location information).

This Note breaks new ground with a thorough account of ECPA legislative history, a direct refutation of the first court of appeals to consider the issue, an accounting of the government's recent divergent positions in the *Ackies* litigation and the Playpen litigation, and novel applications of the statute to other smart devices.

provisions to gin up legislative authority.[7] The Government has settled on arguing prospective location information from a cell phone can be obtained under Title II of ECPA, the Stored Communications Act (SCA), alone.[8]

This Note contends, contrary to the Government's position, that cell phones are properly classified as tracking devices under ECPA, and prospective location information can only be obtained under the provisions of the TDS. Part II explains the comprehensive ECPA legislative scheme by distilling its components: the Wiretap Act (WTA), the Pen Registers and Trap and Trace Devices Statute (PRTT), the SCA, and the TDS. Part III applies ECPA to cell phones, first detailing the various ways a cell phone tracks the location of its user, and confirming the TDS rightfully governs law enforcement access to cell phone prospective location information through an exploration of ECPA's text, structure, legislative history, and post-enactment developments. Part III.B explains why the only federal appellate decision squarely addressing the issue, the First Circuit's 2019 decision in *United States v. Ackies*,[9] is wrongly decided for holding that the SCA governs law enforcement access to cell phone prospective location information. Part IV concludes with a foray beyond cell phones to several close corollaries, applying my reading of the TDS to wearable health monitors, computers, and other devices in the smart home.

---

[7] The Government has largely abandoned its previous theories of authority under ECPA. The most prominent prior argument was the "hybrid theory," invoking both the SCA and the PRTT as jointly granting authority to collect location information without a probable cause warrant. *See, e.g.*, *In re* Use of a Pen Reg., 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (rejecting the Government's hybrid theory as authority under ECPA to collect prospective location information); Lisa M. Lindemenn, Note, *From Cell to Slammer: Flaws of the Hybrid Theory*, 53 ARIZ. L. REV. 663, 687-88 (2011) (same).

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

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

## II. ECPA'S LEGAL LANDSCAPE

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA), comprehensive legislation governing law enforcement access to electronic communications.[10] ECPA is generally thought of in terms of its three titles: Title I, the Wiretap Act;[11] Title II, the Stored Communications Act;[12] and Title III, the Pen Registers and Trap and Trace Devices Statute.[13] The Tracking Device Statute—an oft-forgotten provision—is located within Title I.[14] As I explain further in Parts II.A through II.D, Congress's ECPA scheme reflects a comprehensive legislative plan. Access to prospective information is governed by Titles I and III, via the Wiretap Act, the Tracking Device Statute, and the Pen Registers and Trap and Trace Devices Statute. Title II, the Stored Communications Act, serves as the historical information corollary to the other titles. This understanding is critical to a proper application of ECPA.

---

[10] At the time, ECPA was a very forward-looking piece of legislation. It has since long needed updates, yet none are on the horizon. *See Lawful Access to Stored Content*: *Hearing on ECPA Part 1 Before the H. Judiciary Subcomm. on Crime, Terrorism, Homeland Sec. and Investigations*, 113th Cong. 48 (2013) (statement of Rep. Jim Sensenbrenner, Chairman, H. Judiciary Subcomm. on Crime, Terrorism, Homeland Sec. and Investigations) ("The Electronic Communications Privacy Act of 1986, or ECPA, is complicated, outdated, and largely unconstitutional."). Many of the lines drawn in ECPA no longer match the current state of the technology, but the framework continues to govern electronic communications. *See id.* (statement of Richard Salgado, Dir. L. Enf't & Info. Sec., Google, Inc.) ("The distinctions that ECPA made in 1986 were foresighted in light of technology at the time. But in 2013, ECPA frustrates users' reasonable expectations of privacy."); *see also* Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004) ("[ECPA] is a bit outdated and has several gaps in need of legislative attention, but by and large it reflects a sound approach to the protection of . . . [i]nternet communications.").

[11] 18 U.S.C. §§ 2510-2523.

[12] 18 U.S.C. §§ 2701-2713.

[13] 18 U.S.C. §§ 3121-3127.

[14] 18 U.S.C. § 3117.

*A. The Wiretap Act*

The Wiretap Act (WTA) was originally passed in 1968 as Title III of the Omnibus Crime Control and Safe Streets Act, predating ECPA.[15] The WTA regulates prospective surveillance of the content of communications, including the canonical example of law enforcement agents listening in on phone calls.[16] Because of the sensitive nature of the content of communications, the WTA represents the high-water mark of protections in ECPA. The WTA contains more restrictive requirements for issuance of a warrant as compared to the requirements for ordinary searches.[17] Because of these demanding requirements, the court order required to conduct a wiretap is often called a "super-warrant."[18]

The WTA contains a set of restrictions that repeat throughout ECPA wherever provisions grant law enforcement access to prospective information. These restrictions generally include a default maximum duration of surveillance, extensions, and a notice requirement. Under the WTA, the default maximum is set such that the investigation must terminate within thirty days unless an extension is granted.[19] The investigation cannot continue "for any period longer than is necessary to

---

[15] Title I of ECPA amended the WTA in 1986 to include interception of the contents of electronic communications. Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 13 n.22 (2004).

[16] *See, e.g.*, Berger v. New York, 388 U.S. 41 (1967).

[17] *See* Freiwald, *supra* note 15 at 25; Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 630 (2003).

[18] Freiwald, *supra* note 15 at 25; Kerr, *supra* note 17 at 630. To obtain a warrant to wiretap the content of prospective electronic communications, a reviewing judge must find probable cause to believe the target "is committing, has committed, or is about to commit" an offense, and that this surveillance will collect incriminating communications about the offense. 18 U.S.C. § 182518(3)(a). Only certain offenses can be the underlying offense for a wiretap. *Id.* Agents are also required to minimize the interception of non-incriminating communications. 18 U.S.C. § 2518(5). And law enforcement must certify that normal investigative procedures have been tried and have failed, reasonably appear to be unlikely to succeed if tried, or are too dangerous to try. 18 U.S.C. § 2518(1)(c).

[19] 18 U.S.C. § 2518(5).

achieve the objective of the authorization," so if the investigation is complete before thirty days have passed, the wiretap must terminate immediately.[20] Notice must be given to the targets of interception, but it may be delayed until the investigation is complete.[21]

And, perhaps most importantly, the WTA contains an exclusionary clause that repeats throughout each ECPA title, reinforcing the ECPA scheme. The definition of "electronic communications" specifically excludes information obtained from a tracking device.[22] Because of this clause, if there is any area where both the WTA and the Tracking Device Statute (TDS) could potentially apply, the TDS controls.[23] This clause, along with its counterparts in the various titles, serves to further the TDS's intended role within ECPA as the sole provision governing law enforcement access to prospective location tracking.

### *B. The Pen Registers and Trap and Trace Devices Statute*

Title III of ECPA created the Pen Registers and Trap and Trace Devices Statute (PRTT), which governs prospective surveillance of non-content information (dialing, routing, addressing, and signaling information) related to electronic communications.[24] The procedure for obtaining a pen register consists of two simple steps. First, the application must state the "identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the

---

[20] *Id.*

[21] *See* 18 U.S.C. § 2518(8)(d).

[22] 18 U.S.C. § 2510(12)(c).

[23] *Id.* This means that even if the location information obtained is *the content of an electronic communication*, it would nonetheless be governed by the TDS, not the WTA.

[24] Pen registers and trap and trace devices used to be two separate devices (one for recording *incoming* non-content information, and one for recording *outgoing* non-content information). *See* WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 4.7(a) (4th ed. 2019). Modern pen registers can do both of these tasks in one device and are now often referred to as pen/trap devices or as just pen registers. *Id.*

identity of the law enforcement agency conducting the investigation."[25] Second, the application must include a certification that "the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[26] If the application contains these required items, the judge must issue the order.[27]

As Wayne LaFave explains, the PRTT "acts as a non-content cousin" of the Wiretap Act (WTA).[28] The PRTT contains a similar set of the usual ECPA limits on prospective surveillance, but its limits are less strict than those found in the WTA, reflecting Congress's recognition that pen registers are less privacy-invasive than wiretaps because pen registers collect exclusively non-content information. Under the PRTT, a pen register order allows the government to receive prospective information for a period of sixty days, double the maximum duration of surveillance allowed by the WTA.[29] The surveillance period can be extended for similar durations upon application.[30]

And in 1994, the Communications Assistance to Law Enforcement Act (CALEA) amended the PRTT to add an exclusionary clause stating the statute does not authorize the acquisition of location information.[31] This clause, known as the CALEA proviso,[32] prohibits "information acquired solely pursuant to the authority for pen registers and trap and

---

[25] 18 U.S.C. § 3122(b).

[26] *Id.*

[27] LAFAVE ET AL., *supra* note 24, § 4.7(b).

[28] *Id.* § 4.7(a).

[29] 18 U.S.C. § 3123(c)(1).

[30] 18 U.S.C. § 3123(c)(2). And like the WTA, the PRTT contains a reporting requirement, so pen register numbers must be reported to Congress. 18 U.S.C. § 3126.

[31] Despite the CALEA proviso, the government has nonetheless attempted to acquire prospective location information via the PRTT. In order to get around the limitation imposed by the CALEA proviso, the government previously relied on their hybrid theory, arguing that the PRTT and the SCA combined (but neither in isolation) granted them authority to access prospective location information without a warrant. *See supra* note 7.

[32] *See In re* Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005).

trace devices" from including "any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."[33] Like the WTA, the PRTT makes clear that it does not authorize the collection of location information, again reinforcing the role of the Tracking Device Statute as the exclusive statute authorizing prospective location tracking.

### *C. The Stored Communications Act*

The Stored Communications Act (SCA) was enacted as Title II of ECPA.[34] Whereas the Wiretap Act and the Pen Registers and Trap and Trace Devices Statute regulate the acquisition of prospective communications data, the SCA regulates acquisition of historical information, "user account information stored in the ordinary course of business."[35] The SCA is a labyrinth of categories and distinctions, structured into a hierarchy of protections for various kinds of information: content, non-content records and other information pertaining to a subscriber or customer, and non-content basic subscriber information.

Unsurprisingly, the content of communications—"any information concerning the substance, purport, or meaning of that communication"—receives the most protection under the SCA.[36] To obtain this information, law enforcement must acquire a probable cause search warrant.[37] But while a standard Federal Rule of Criminal Procedure 41 search warrant limits "a search of property . . . [to] within the district,"[38] an SCA § 2703 warrant can be issued by any federal "court of competent jurisdiction,"[39]

---

[33] 47 U.S.C. § 1002(a)(2).
[34] Kerr, *supra* note 10, at 1208.
[35] LAFAVE ET AL., *supra* note 24, § 4.8(a).
[36] 18 U.S.C. § 2510(8).
[37] 18 U.S.C. § 2703.
[38] FED. R. CRIM. P. 41(b)(1).
[39] 18 U.S.C. § 2703.

creating broader jurisdiction and allowing searches of records held in another district.[40]

At the bottom of the hierarchy of protections is basic subscriber information, which can be obtained with a subpoena and the accompanying showing of relevance.[41]

In the middle of the protection hierarchy is "a record and other information pertaining to a subscriber to or customer of such service."[42] This "catch-all" category includes "all records that are not contents, including basic subscriber and session information, . . . transactional records, such as account logs that record account usage," and more. [43] To obtain records or other information, law enforcement must obtain a court order under 18 U.S.C. § 2703(d), requiring a showing of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[44] As the Tenth Circuit has noted, the "specific and articulable facts" standard for issuance of a § 2703(d) order is derived from the Supreme Court's decision in *Terry v. Ohio*.[45]

---

[40] *See* Smith, *Why Are Precise Location Warrants a Thing?*, *supra* note 6.

[41] 18 U.S.C. § 2703(c). Basic subscriber information is further broken down into six categories: (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number). 18 U.S.C. § 2703(c)(2).

[42] 18 U.S.C. §§ 2703(c)(1), (d).

[43] CRIM. DIV., U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 122 (2009).

[44] 18 U.S.C. § 2703(d).

[45] United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) (citing Terry v. Ohio, 392 U.S. 1 (1968)). This provision was found unconstitutional in *Carpenter* when used to acquire historical cell site location information. Carpenter v. United States, 138 S. Ct. 2206 (2018).

Additionally, the SCA contains its own exclusionary clause, as it cross-references the ECPA definition of "electronic communication," which explicitly excludes information from a tracking device.[46] The SCA cannot be used to obtain prospective location information from a tracking device, as defined by the TDS.[47] As is the case with the WTA and the PRTT, if there is any situation where a piece of information could plausibly be characterized as covered by either the TDS or the SCA, the TDS unequivocally governs.

### *D. The Tracking Device Statute and Rule 41(b)(4)*

The Tracking Device Statute (TDS) is housed within Title I of ECPA, and it contains two concise provisions: a definition and a venue restriction.[48] The two provisions are as follows:

> (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.

Federal Rule of Criminal Procedure 41, which governs the powers of the magistrate, incorporates the § 3117 definition of a tracking device and contains special provisions for tracking warrants.[49] The rule orders a magistrate judge to issue a warrant if there is probable cause to "install

---

[46] *See* 18 U.S.C. §§ 2510, 2711.
[47] 18 U.S.C. § 3117.
[48] *Id.*
[49] FED. R. CRIM. P. 41(b)(4).

and use a tracking device."[50] Such a warrant must "identify the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used."[51] Congress also included restrictions in Rule 41 mirroring the usual set throughout ECPA for law enforcement access to prospective information. Under Rule 41, a tracking device has a maximum duration of surveillance of forty-five days from the date of the issuance of the warrant.[52] The court may, for good cause, grant extensions for a further period of time not to exceed forty-five days each.[53] This forty-five-day limit on prospective surveillance places this provision squarely between the WTA and the PRTT in terms of strictness. And Rule 41 contains a notice requirement: Within ten days after the termination of the tracking device, "the officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked," but notice can be delayed upon the government's request.[54]

## III. APPLYING ECPA TO CELL PHONES

This Part explains how prospective location information from cell phones fits within ECPA regulation. Part III.A explains why the Tracking Device Statute (TDS) rightfully governs prospective location information from a cell phone, first by detailing the various ways a cell phone tracks the movements of its user, then by exploring the text, structure, and legislative history of the TDS. Part III.B refutes the First Circuit decision in *United States v. Ackies*, 918 F.3d 190 (1st Cir. 2019), which held that prospective location information can be obtained under the Stored Communications Act (SCA).

---

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

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

[52] *Id.*

[53] *Id.*

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

### *A. The Tracking Device Statute Rightfully Governs Cell Phones*

As discussed in the previous section, due to the ECPA exclusionary clauses, if access to certain electronic information falls under the jurisdiction of the TDS, it cannot be accessed under the Wiretap Act, the Pen Registers and Trap and Trace Devices Statute, or the Stored Communications Act. Thus, the threshold question is whether the TDS governs access to prospective cell phone location information. If the answer is yes, that ends the inquiry. This Part argues that a cell phone is a tracking device, meaning that when law enforcement seeks to gain prospective location information from a suspect's cell phone, they must obtain a warrant under the TDS. First, I discuss the technological mechanisms through which a cell phones tracks the movements of its user. I then apply ECPA. The text and structure of ECPA alone support classification as a tracking device, but the argument is even stronger when one considers ECPA's legislative history and post-enactment developments.

#### *1. How A Cell Phone Tracks the Movements of Its User*

A cell phone tracks location through a variety of methods. The most common methods are cell site location information (CSLI) and global positioning system (GPS) data collection.[55] CLSI refers to the data a cell phone conveys to cell towers. Cellular service providers maintain a network of cell towers, to and from which cell phones send and receive radio signals.[56] "Cell site" refers to the portion of the cell tower that

---

[55] NAT'L ASS'N CRIM. DEF. LAWYERS, CELL PHONE LOCATION TRACKING: A NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS PRIMER (2016).

[56] United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015); *In re* Tel. Info. Needed for a Crim. Investigation, 119 F. Supp. 3d 1011, 1013 (N.D. Cal. 2015) (citing *Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance: Hearing Before the H. Judiciary Subcomm. on Crime, Terrorism, Homeland Security, and Investigations*, 113th Cong. 50 (2013) [hereinafter *ECPA Hearing Part II*] (written testimony of Prof. Matt Blaze, Univ. of Pennsylvania)).

detects the radio signal from a cell phone and then connects that phone to the local cellular network or to the Internet.[57] While cellular service providers usually mount cell sites on cell towers, providers may also mount cell sites "on light posts, flagpoles, church steeples, or the sides of buildings."[58] As a user and her device move from location to location, the cell phone automatically and regularly scans nearby cell towers several times per minute in order to connect to the one with the strongest signal—allowing a user to gain access to the mobile network with the fastest possible service.[59] Every time a cell phone connects to a cell tower, the cell phone service provider records the time and duration of that connection.[60]

The precision of a trail of CSLI datapoints varies based on the number of nearby cell sites.[61] CSLI generally identifies the precise location of the connected site at any given time, and by extension, the location of the cell phone user within a few feet.[62] Information from multiple cell towers can be used to triangulate a cell phone's location, tracking the device with even greater precision.[63] Such information can be nearly as precise as GPS data, which is typically accurate to within roughly ten feet.[64] The greater

---

[57] *In re Tel. Info. Needed for a Crim. Investigation*, 119 F. Supp. 3d at 1014 (citing *ECPA Hearing Part II*, *supra* note 56 (written testimony of Prof. Matt Blaze, Univ. of Pennsylvania)); *see also Types of Cell Sites*, STEEL IN AIR, https://perma.cc/R8N8-XJBG.

[58] *See* Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

[59] *Id.* at 2211-12; ELEC. FRONTIER FOUND., CELL SITE LOCATION INFORMATION: A GUIDE FOR CRIMINAL DEFENSE ATTORNEYS (2019).

[60] ELEC. FRONTIER FOUND., *supra* note 59.

[61] Eric Pait, *Find My Suspect: Tracking People in the Age of Cell Phones*, 2 GEO. L. TECH. REV. 155, 157 (2017); *see also Carpenter*, 138 S. Ct. at 2211-12.

[62] *See* United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015); *In re Tel. Info. Needed for Crim. Investigation*, 119 F. Supp. 3d at 1014 (citing *ECPA Hearing Part II*, *supra* note 5656 (written testimony of Prof. Matt Blaze, Univ. of Pennsylvania)).

[63] *See* United States v. Stimler, 864 F.3d 253, 260 (3d Cir. 2017); *In re Tel. Info. Needed for Crim. Investigation*, 119 F. Supp. 3d at 1023 (citing *ECPA Hearing Part II*, *supra* note 56 (written testimony of Prof. Matt Blaze, Univ. of Pennsylvania)).

[64] *See In re Tel. Info. Needed for Crim. Investigation*, 119 F. Supp. 3d at 1015 (citing *ECPA*

the number and concentration of cell sites, the greater the tracking precision.[65]

GPS data, on the other hand, refers to the signals the cell phone receives from GPS satellites at set intervals of time. These signals are used to determine the device's location and provide highly accurate location data, typically within about ten to fifteen feet for GPS-enabled smart phones.[66] A cell phone's internal GPS locator thus can provide a catalog of the user's movements.[67]

Smart phones, cell phones with expanded functions that act as both phones and mini-computers, provide additional mechanisms to gather location information.[68] These phones can send location information via Bluetooth features.[69] For example, when an Android phone scans for nearby Bluetooth devices to connect to, a list of the nearby Bluetooth devices is sent to Google.[70] This can be incredibly specific tracking, as it "pinpoint[s] a device to a more specific locale" than GPS or CSLI can achieve.[71] Smart phones also allow location tracking through Wi-Fi connections. Google, for instance, keeps a "detailed map of known Wi-Fi networks and access points," and "[b]y knowing the exact location of

---

*Hearing Part II*, *supra* note 56 (written testimony of Prof. Matt Blaze, Univ. of Pennsylvania)); NAT'L ASS'N CRIM. DEF. LAWYERS, *supra* note 55; Pait, *supra* note 61, at 158.

[65] Cell site towers are up 8% from 2017, which was a record-breaking year in its own right. *2019 Annual Survey Highlights*, CTIA (June 20, 2019), https://perma.cc/7FSA-R9TP; Jones, *supra* note 6, at 530 (2019) ("A record number of cell sites were in operation at the end of 2017, providing increased precision of real-time CSLI.").

[66] *GPS Accuracy*, GPS.GOV, https://perma.cc/JAZ6-Z7KS (last modified Apr. 22, 2020).

[67] *Id. See also* Jones, *supra* note 6, at 528-29.

[68] Jones, *supra* note 6, at 526.

[69] Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant at 7, 10, United States v. Chatrie, No. 3:19-cr-00130-MHL (E.D. Va. Dec. 20, 2019).

[70] David Yanofsky, *Google Can Still Use Bluetooth to Track Your Android Phone When Bluetooth Is Turned Off*, QUARTZ (Jan. 24, 2018), https://perma.cc/L6YE-KBPT.

[71] *Id.*

these networks, and your proximity to them, its location services can gauge your location with roughly 30 feet of accuracy."[72]

*2. The Text and Structure of ECPA*

Starting with the plain text of the Tracking Device Statute (TDS), cell phones clearly fall within the statute's coverage. Congress defined a tracking device broadly, as an "electronic or mechanical device which permits the tracking of the movement of a person or object."[73] As discussed in Part III.A.1, cell phones enable their users' movements to be tracked. A cell phone can use a variety of mechanisms to track the movements of its user, including CSLI, GPS, Bluetooth, and Wi-Fi connections.[74] In fact, the cell phone's ability to track its user's movements is precisely why law enforcement officers seek cell phone location data: They want to track the suspects of crimes.[75] Because cell

---

[72] Christina Bonnington, *How Google Uses Wi-Fi Networks to Figure Out Your Exact Location*, SLATE (June 20, 2018, 10:30 AM), https://perma.cc/92D9-EWUM. The current COVID-19 pandemic provides another example of the power of location tracking, and the ability of technology providers to track movements and movement patterns with startling breadth and precision. New Google reports have relied on users' location data to show how movement patterns are changing based on COVID-19 (for example, showing who complied with stay-at-home orders), and their reporting reveals the extent to which cell phones can chronicle, to an unsettling degree, a user's every move. Casey Newton, *Google Uses Location Data to Show Which Places Are Complying with Stay-at-Home Orders — and Which Aren't*, VERGE (Apr. 3, 2020, 2:00 AM), https://perma.cc/8UY9-6Q9K.

[73] 18 U.S.C. § 3117.

[74] *See supra* Part III.A.1.

[75] *See, e.g.*, Petition for Writ of Certiorari at 10, Ackies v. United States, 140 S. Ct. 662 (2019) (No. 19-6602) ("Indeed, a cell phone's ability to track a person is precisely why the law enforcement officers in this case sought PLI warrants. The warrants 'directed AT&T to provide "specific latitude and longitude or other precise location information"' for a specific cell phone for 30 days . . . . The government used the precise information obtained pursuant to the warrants to literally 'follow[]' a phone as the PLI showed it 'moving down' a road . . . . Thus, the cell phone 'permit[ted]' the government to 'track[] . . . the movement' of an 'object' (the phone) and 'a person' (Mr. Ackies).").

phones permit location tracking over time, they clearly fall within the plain meaning of the term tracking device in § 3117.

And Congress chose a broad and facially technology-neutral definition of tracking device.[76] The decision whether to have a broad or narrow definition in a statute is ultimately up to Congress.[77] Here, Congress chose a wide-reaching and flexible definition, without enumerated limits on the kind of technology the statute could apply to. Had Congress wanted to limit the coverage of the TDS to the preferred tracking devices of the 1980s,[78] it would have done so—when Congress wants to impose such limits, it uses limiting mechanisms such as an enumerated list.[79] Yet, Congress conspicuously chose not to do so in the TDS, indicating its intent to create a broad and flexible definition that could add future or unforeseen technologies to its jurisdiction based on their functions and capabilities. The inclusion of the word "installation" does not change this, as installation encompasses both the installation of hardware, such as the placement of a beeper under a vehicle, as well as the installation of software, such as a tracking application onto a cell phone.[80]

---

[76] Text should be construed "reasonably, to contain all that it fairly means." ANTONIN SCALIA, A MATTER OF INTERPRETATION: FEDERAL COURTS AND THE LAW 23 (1997); *see also* Conn. Nat'l Bank v. Germain, 503 U.S. 249, 253-54 (1992) ("[C]ourts must presume that a legislature says in a statute what it means and means in a statute what it says there.").

[77] United States v. Rodgers, 466 U.S. 475, 484 (1984) ("Resolution of the pros and cons of whether a statute should sweep broadly or narrowly is for Congress.").

[78] The preferred tracking devices of the 1980s were beepers, one-way radio transmitters of location information that were attached to an object. *See* United States v. Karo, 468 U.S. 705, 707 (1984); United States v. Knotts, 460 U.S. 276, 277 (1983).

[79] *See*, *e.g.*, 16 U.S.C. § 1532(19) ("The term 'take' means to harass, harm, pursue, hunt, shoot, wound, kill, trap, capture, or collect, or to attempt to engage in any such conduct."); Babbitt v. Sweet Home, 515 U.S. 687 (1995) (analyzing throughout the limited applicability of "take" in § 1532(19) in light of the list).

[80] This argument is addressed further in Part III.B. *See infra* notes 146-73 and accompanying text.

Congress further indicated its intent to have a broad, technology-neutral definition by defining a tracking device as a device that "*permits* the tracking" of a person.[81] Such language broadens the applicability of § 3117: Not only does the TDS apply to technology created for the sole and express purpose of tracking location and movements,[82] but it also applies to technology that permits the tracking of its user *among its other uses*. In other words, technology can qualify as a tracking device without *solely* being a tracking device. And as the Supreme Court recognized in *Riley v. California*[83] and *Carpenter v. United States*,[84] cell phones do many things at many points in time. They are multifunctional devices that handle phone calls, manage banking, provide directions to destinations, and much more, all the while tracking movements with such precision that it is "as if [the government] had attached an ankle monitor to the phone's user."[85]

Viewed structurally, ECPA further supports the conclusion that prospective location information from a cell phone is regulated by the TDS. Taken as a whole, ECPA consists of a coherent legislative scheme, with protections based on the kind of data at issue. ECPA authorizes

---

[81] 18 U.S.C. § 3117 (emphasis added). I disagree with the decision of *In re Smartphone Geolocation Data Application*, in which the court said "the [Tracking Device] 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." 977 F. Supp. 2d 129, 149 (E.D.N.Y. 2013). By the text of § 3117, the intended purpose of a device is irrelevant to the determination of whether it is a tracking device. The plain language contains no such limit regarding purpose and defines tracking device based exclusively on functional capabilities, specifically whether it permits the tracking of the movements of a person or object.

[82] For example, a beeper placed in a container, *Knotts*, 460 U.S. at 277, or a GPS tracker placed on a car, United States v. Jones, 565 U.S. 400, 403-04 (2012).

[83] 573 U.S. 373, 393 (2014) ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

[84] 138 S. Ct. 2206 (2018).

[85] *Id.* at 2218.

three different kinds of prospective surveillance: content under the WTA, location information under the TDS, and non-content information under the PRTT. These statutes share a set of similar, forward-looking provisions (e.g., maximum duration of surveillance, extensions, and notice) that ECPA pairs with ongoing law enforcement activity.[86]

The SCA, on the other hand, serves as the historical information corollary to the WTA, TDS, and PRTT, governing "what law enforcement must do to obtain electronic communications or records from third-party providers that *already exist* in 'electronic storage.'"[87] But while historical records of all kinds can be obtained under the SCA, the SCA itself does not authorize ongoing surveillance. For one, the SCA was modeled on the Right to Financial Privacy Act (RFPA),[88] which governed law enforcement access to bank records.[89] As the RFPA does not allow monitoring of bank account transactions in real-time, neither does the SCA allow for monitoring of information in real-time.[90] Furthermore, as explained by Judge Stephen Smith, "[t]he SCA's only nod to prospective data gathering is section 2703(f), which authorizes the government to require a provider 'to preserve records and other evidence in its possession pending the issuance of a court order.'"[91] This provision indeed allows the government to acquire a set of location information in

---

[86] *See In re* Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 760-61 (S.D. Tex. 2005).Congress added the duration and renewal requirements for tracking warrants in the 2006 amendments to Rule 41. *See* FED. R. CRIM. P. 41(b)(4).

[87] *See* Petition for Writ of Certiorari, *supra* note 75, at 12 n.4 (emphasis added); *see also In re* Use of a Pen Reg., 396 F. Supp. 2d 294, 309 (E.D.N.Y. 2005) ("[T]he profound structural differences between [§ 2703] and [§ 3117] suggest that Congress did not intend the former to be a vehicle for allowing prospective, real-time surveillance of a mobile telephone user's physical location and movements . . . .").

[88] S. REP. NO. 99-541, at 3 (1986).

[89] *See In re* Prospective & Continuous Release of Cell Site Location Recs., 31 F. Supp. 3d 889, 895 (S.D. Tex. 2014) (discussing the history of the SCA).

[90] *Id.*

[91] *Id.* (quoting 18 U.S.C. § 2703(f)).

the future, "albeit not contemporaneously, [but rather] pursuant to a *retrospective* 2703(d) order."[92] Section 2703(f) directs the preservation of records to be disclosed to the government, but disclosure must come later in response to a 2703(d) order, issued *after the records are created*.[93]

*3. Legislative History*

The legislative history of ECPA further supports that cell phones should be considered tracking devices for the purposes of § 3117. A congressional report and testimony from ECPA hearings indicate that Congress contemplated its broad, technology-neutral definition of a tracking device could include a cell phone.

The ECPA legislative record includes the Office of Technology Assessment (OTA) 1985 report, which brought to Congress's attention that cell phones could be used to track the movements of their users.[94] In the first paragraph of the report, the OTA led with the issue of cell phones as a law enforcement investigative tool, explaining that "new electronic technologies in use by individuals, such as cordless phones" can be "easily monitored" for investigative purposes.[95]

And in the first paragraph of the report's Telephone Surveillance chapter, the OTA again led with an explanation of the potential for monitoring location information: Technological innovation had led to easier ways to monitor "phone transactions," the data other than content that was associated with telephone calls.[96] The OTA explicitly flagged

---

[92] *Id.*

[93] *Id.*

[94] U.S. OFF. OF TECH. ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985).

[95] *Id.* at 3.

[96] *Id.* at 30.

that these innovations would make it possible to collect transactional information such as location information.[97]

Later in the report, the OTA noted the potential for monitoring of location over time, explaining that "[n]ew information technologies have also greatly increased the ability to collect and access transactional information about telephone calls," including, for example, the "places dialed."[98] Per the report, "[a]ccess to this information makes it possible to determine patterns and interconnections in phone transactions."[99] The report then linked the use of "[t]ransactional information about phone calls (e.g. numbers and places dialed)" to investigative uses, indicating that "access to such information represents a significant threat to civil liberties and a significant potential benefit to investigators."[100] Per the OTA, "[t]ransactional information is becoming more valuable as more of it is available and can be cross-referenced,"[101] and "[i]nformation on phone transactions is potentially of great interest to investigative authorities"[102] such as the "Justice Department and other investigative agencies [that] use such information primarily in the initial investigation of a case."[103]

The OTA report ends with another such statement, explaining "[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."[104] The report's continual references to investigative uses of non-content information to determine the user's

---

[97] *Id.* at 29 ("[T]echnological innovations now make it easier to electronically monitor both the content of phone calls and phone transactions (e.g., number called, time, and place called).").

[98] *Id.* at 40.

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.* at 42.

[103] *Id.*

[104] *Id.*

location put Congress on notice that cell phones could be used to track the movements of persons.

Furthermore, this report was not an isolated or forgotten part of the legislative record. During a hearing specifically designated to discuss the TDS provisions in ECPA, Representative Robert Kastenmeier, one of the primary authors of ECPA, explicitly referenced the OTA report while questioning a testifying witness, communications executive John Stanton.[105] Indeed, in his testimony, Stanton linked the findings of the OTA report to a potential application of the TDS to cell phones.

Stanton's testimony flagged the potential use of cell phones to track the movements of their users, and he explicitly mentioned that this could mean cell phones fall within the definition of a tracking device. To illustrate this concern, Stanton brought to the hearing "a cellular telephone that can be mounted either in a vehicle or carried around" and "a portable cellular telephone that can be conveniently carried around in a pocket."[106] He explained that both devices could "easily access the telephone network, making calls locally, national, over the interstate or State long-distance network, or international."[107] After explaining how transactional information from such phone calls could include location information, Stanton confirmed "the definition of the term 'tracking device' in the current bill is broad enough that it could be read as including paging or cellular equipment."[108]

After the release of the OTA report and the hearings in which Stanton explicitly brought the issue of cell phones as tracking devices under § 3117 to the attention of the legislators and primary ECPA drafters, Congress did not make a single change to the definition of a tracking

---

[105] *Electronic Communications Privacy Act: Hearings Before the H. Judiciary Subcomm. on Courts, C.L., and the Admin. of Just.*, 99th Cong. 101 (1985) ("Mr. Kastenmeier: The OTA report assessing the impact of emerging technologies on privacy obviously did include cellular telephones.").

[106] *Id.* at 92.

[107] *Id.*

[108] *Id.* at 99.

device before ECPA's passage.[109] Congress was on notice that its definition could include cell phones, and they chose to leave the § 3117 definition broad enough to do so. This evidence, while imperfect, may indicate an intent to include cell phones in the definition. At a minimum, it indicates there was no intent to *exclude* cell phones from § 3117 coverage.

Finally, ECPA's post-enactment history further supports that cell phones are properly classified as tracking devices. In 2006, Congress amended Rule 41 of the Federal Rules of Criminal Procedure to add the tracking warrants provisions detailed in Part II, incorporating the same broad and technology-neutral definition of a tracking device originally enacted by the 1986 Congress.[110] Needless to say, technology tracking the

---

[109] *See* Smith, *Losing Track of the Tracking Device Statute*, *supra* note 6. A Senate Report recommending the passage of ECPA included its own explanations of some key terms. S. REP. NO. 99-541 (1986). In the report, the Senate describes "electronic tracking devices (transponders)" as "one-way radio communication devices that emit a signal on a specific radio frequency," *id.* at 10, cutting-edge tracking technology at the time that has since become obsolete. The Government referenced this report in 2014 in front of the Southern District of Texas. *In re* Prospective & Continuous Release of Cell Site Location Recs., 31 F. Supp. 3d 889, 897-98 (S.D. Tex. 2014). Judge Smith rightfully rejected the argument because "[t]he descriptive passage in the Senate Report could not, and did not purport to, displace the statutory definition of 'tracking device' enacted by Congress." *Id.* As Judge Smith noted, "[w]hen Congress unambiguously defines a term in the United States Code, a reviewing court has no power to redefine that term based on extraneous sources of 'plain meaning.'" *Id.* (citing 2A N. SINGER & S. SINGER, STATUTES AND STATUTORY CONSTRUCTION § 45.8 at 53 (7th ed. 2014) (noting that the popular meaning of words in a statute may be consulted only "in the absence of a statutory definition"). Furthermore, Judge Posner discussed this same report's definition of "mobile interception device[s]," as the report similarly provides a narrower explanation than the broad language of the statute, narrowing this discussion to vehicles. United States v. Ramirez, 112 F.3d 849, 852 (7th Cir. 1997). Judge Posner explained that this Senate Report's descriptions should be taken as "illustrative rather than definitional because there is no [such] limitation" in the statute. *Id.*

[110] *See* Smith, *Losing Track of the Tracking Device Statute*, *supra* note 6.

movements of persons looked very different in 2006 than it did in 1986.[111] Nonetheless, Congress saw no need to alter the two-decades-old definition, indicating approval of its broad and technology-neutral reach. And this was not an issue ignored in public discourse or the courts: Prior to the 2006 amendments, several magistrate judges and district courts issued high-profile opinions holding that a cell phone is a tracking device under § 3117 when it is used to track the user's location in real time.[112] While the issue had not yet reached the courts of appeals, a growing number of opinions regulated prospective cellular location information under § 3117. Yet Congress felt no need to dispute these holdings in the 2006 rules or Advisory Committee Notes.[113]

In sum, the text, structure, and legislative history support a reading of ECPA as regulating prospective cell phone location information under its tracking device provisions. Tracking device authorization can only

---

[111] *See, e.g.*, *In re* Use of a Pen Reg., 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (law enforcement sought to track suspect through cell phone location information).

[112] These decisions were dubbed the "Magistrate's Revolt," garnering much attention. *See* Ann E. Marimow & Craig Timberg, *Low-level Federal Judges Balking at Law Enforcement Requests for Electronic Evidence*, WASH. POST (Apr. 24, 2014), https://perma.cc/78X7-QXWC. Judge Smith's 2005 opinion, prior to the Rule 41 amendments, is credited as a high-profile inflection point in the movement. *Id.* ("Magistrate Judge Stephen W. Smith, based in Houston's federal court, is often credited with touching off the insurrection among his colleagues with a 2005 ruling in which he denied a government request for real-time access to the detailed location information that cellphones emit. He ruled that requiring a telecommunications company to provide subjects' ongoing data amounted to placing a tracking device on them — something permitted only with the issuance of a search warrant, which the government had not requested.")

[113] *See, e.g.*, *In re* Installation & Use of a Pen Reg., 402 F. Supp. 2d 597 (D. Md. 2005); *See In re* Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005); *In re Use of a Pen Reg.*, 396 F. Supp. 2d at 309. *See generally* Bob Jones Univ. v. Simon, 416 U.S. 725 (1974) (holding that there was a strong case for legislative acquiescence through Congress's failure to act to overturn IRS conclusions); Flood v. Kuhn, 407 U.S. 258, 283-84 (1972) (relying on Congress' implicit acquiescence, or "positive inaction," to justify adherence to prior judicial interpretation of a statute).

come from the TDS and the associated Rule 41 provisions, and no other provision of ECPA.[114]

### *B.* Ackies *Was Wrongly Decided: Acquisition of Prospective Location Information Should Not Be Authorized Under the Stored Communications Act*

My argument implies that the only federal court of appeals decision to squarely address this question was wrongly decided. In *United States v. Ackies*,[115] the First Circuit held that prospective location information could be obtained under the SCA.[116] The opinion made a series of mistakes that other courts should not repeat.

As background on the case, in January 2016, law enforcement applied to a federal magistrate judge in Maine for two warrants under the SCA, each to provide prospective location information from a cell phone.[117] The magistrate judge approved the warrants, directing AT&T to provide law enforcement with ongoing location information from the two cell phones—in particular, continuous latitudinal and longitudinal information for a period of thirty days.[118] The prospective location information obtained indicated that the cell phones were initially located at a residence in New York.[119] The defendant, Carey Ackies, was never seen at the residence; however, law enforcement continued to track the cell phones' locations throughout the city and eventually to a parking lot, where investigators discovered a vehicle matching a description from a

---

[114] *See supra* Part II (detailing provisions of the WTA, PRTT, and SCA that grant exclusive authority to the TDS for location information from a tracking device).

[115] 918 F.3d 190 (1st Cir. 2019).

[116] *Id.* at 200.

[117] *Id.* at 195.

[118] Petition for Writ of Certiorari, *supra* note 75, at 4.

[119] *Id.*

cooperating defendant.[120] Ackies was arrested as he approached the vehicle.[121]

Ackies filed motions to suppress the evidence obtained from the issuance of the prospective location information warrants, arguing the warrants were "jurisdictionally void."[122] Ackies argued that a cell phone is a tracking device under the § 3117 definition; therefore, the § 3117 territorial restriction forbade the magistrate in Maine from authorizing a warrant to track a cell phone located in New York.[123] The district court denied Ackies' motion, and the jury found Ackies guilty of one count of conspiracy to possess with intent to distribute heroin and cocaine base.[124]

In an opinion by Judge Sandra Lynch, a three-judge panel of the First Circuit affirmed the lower court's decision, holding that the prospective location information warrants were properly issued under § 2703 of the SCA.[125] The court's analysis of this issue was cursory, but the opinion explained its reasoning as follows. According to the First Circuit, a cell phone is not a tracking device because it is incompatible with § 3117 language requiring "installation" of a "device."[126] The court further held that applying § 3117 would be improper because of the practical difficulties of determining the proper venue when the present location of a cell phone is unknown.[127] The court then concluded that law enforcement could obtain ongoing location information under the provisions governing stored electronic communications because the data sought was information pertaining to a subscriber or customer of AT&T's services.[128]

---

[120] *Id.*

[121] *Id.* at 4-5.

[122] *Id.* at 5.

[123] *Id.*

[124] *Id.*

[125] United States v. Ackies, 918 F.3d 190, 200 (1st Cir. 2019).

[126] *Id.* at 199.

[127] *Id.*

[128] *Id.* at 200.

The First Circuit erred in granting the warrant under the authority of the SCA because, first and foremost, real-time surveillance is plainly not a stored communication.[129] Stored communications are historical information, not prospective information.[130] As discussed in Part II, the SCA is structurally incompatible with an interpretation that it authorizes ongoing surveillance. And, as Judge Smith has flatly put it, "SCA 2703(c) was intended to provide the means for government to compel disclosure of existing communications and transaction records in the hands of service providers," and "[n]othing in the SCA contemplates a new form of ongoing surveillance in which law enforcement uses co-opted provider facilities to track cell phone users in real-time."[131] According to Judge Smith, "[t]here really is no such thing as a [prospective location information] warrant under the SCA."[132]

Furthermore, as discussed in Part II, the SCA contains a provision explicitly excluding coverage of information from a tracking device, explaining that "information from a tracking device is not a wire or electronic communication."[133] Thus, the question of which provision of

---

[129] *See* Kerr, *supra* note 10, at 1231 ("A stored communication rests on a network server in a permanent or semipermanent state. If the government wishes to obtain a copy of a stored communication, the government obtains an order compelling the system administrator of the server to locate the file and copy it. It is a one-time event.")

[130] As a further problem, GPS data is plainly not the kind of data *stored* in the ordinary course of business by the provider at issue, AT&T. *See infra* notes 146-149 and accompanying text.

[131] Smith, *Why Are Precise Location Warrants a Thing?*, *supra* note 6.

[132] *Id.* Some have argued that the line between prospective and historical stored information is meaningless because the information becomes "stored" information the second the provider has access to it, known as the "instantaneous storage theory." *In re* Prospective & Continuous Release of Cell Site Location Recs., 31 F. Supp. 3d 889, 893 (S.D. Tex. 2014). This argument leads to absurd results, as it would obviate the need to, for example, obtain a wiretap order for anything that could be obtained under the SCA as stored content. *See* Smith, *Why are PLI Warrants a Thing?*, *supra* note 6 ("It would be no different than a 2703(a) order purporting to allow the government real-time access to your emails over a 30-day period. Such an order would be rightly condemned as an illegitimate circumvention of the Wiretap Act.").

[133] *See supra* notes 46-47 and accompanying text.

ECPA governs this law enforcement tactic ultimately turns on the applicability of the TDS. If there is any seeming overlap, Congress made clear that the TDS, and the TDS alone, must apply.

Turning to the determinative application of the TDS, Judge Lynch's opinion concluded that prospective location information from a cell phones is not governed by the TDS. Judge Lynch focused primarily on the use of two terms in the TDS: "installation" and "device."[134] First, the court concluded that "[a] reading of § 3117(b) which includes cell phones as 'tracking device[s]' ignores the relevant textual context in § 3117(a),"[135] the statute's reference to "installation of a mobile tracking device."[136] According to Judge Lynch, "[b]y their plain meanings, 'installation' and 'device' refer to the physical placement of some hardware or equipment (such as [a] GPS device installed on a car . . . )."[137]

However, the First Circuit's textual reading of the tracking device definition as limited to physical placement of hardware was overly narrow. First, "installation" plainly refers to software as well as hardware. This is clearly colloquially true—it is common to, for instance, speak of installing a software application, like Microsoft Word, onto a computer. Common-use dictionaries further support that installation does not solely refer to the physical placement of hardware. Merriam-Webster defines "install" very broadly as "to set up for use or service," and, critically, it provides two examples to illustrate the definition.[138] First, it gives the example of installing a fan in the kitchen, in line with the First Circuit's hardware understanding.[139] But it provides a second example—none other than to "install software."[140] It is by no means a

---

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

[135] *Id.*

[136] *Id.*

[137] *Id.*

[138] *Install*, MERRIAM-WEBSTER, https://perma.cc/Q86N-EPU3 (last visited Apr. 9, 2021).

[139] *Id.*

[140] *Id.*

stretch for installation to refer to software as well as hardware, and the First Circuit's limited understanding of the term was surprising for an opinion written in 2019.[141]

Furthermore, contrary to the First Circuit's assertion that "software is not a 'device' under its plain meaning," [142] the definition of device is also not limited to hardware.[143] To illustrate that software is not a device

---

[141] The First Circuit asserted that installation means "the physical placement of some hardware or equipment," noticeably lacking dictionary support for this definition it invented. *Ackies*, 918 F.3d at 199. Installation does not mean this, and did not mean this at the time of ECPA's enactment. *See* MERRIAM-WEBSTER, INC., WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 626 (1983) (defining "install," in one usage, broadly as "to set up for use or service"). And arguments that, despite a broad dictionary definition, Congress in the 1980s did not *intend* installation to refer to software are irrelevant to the analysis. The Supreme Court explained in *University of Texas Southwest Medical Center v. Nassar* that courts must take care to apply the text itself and not any extratextual "infer[ence]" about what "Congress meant." 570 U.S. 338, 356 (2013); *see* Wis. Cent. Ltd. v. United States, 138 S. Ct. 2067, 2074 (2018) ("While every statute's *meaning* is fixed at the time of enactment, new *applications* may arise in light of changes in the world."); Bostock v. Clayton Cnty., 140 S. Ct. 1731, 1737 (2020) ("Those who adopted the [statute] might not have anticipated their work would lead to this particular result. . . . But the limits of the drafters' imagination supply no reason to ignore the law's demands. . . . Only the written word is the law, and all persons are entitled to its benefit."); *see also* Penn. Dep't of Corr. v. Yeskey, 524 U.S. 206, 212 (1998) (finding "irrelevant" that "Congress did not 'envision that the ADA would be applied to state prisoners'" (quoting Brief for Petitioners at 13-14, *Yeskey*, 524 U.S. 206 (No. 97-634))).

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

[143] In the alternative, if a court is committed to a hardware understanding of the word "device," a more holistic understanding of the underlying technology reveals this not to be a problem. Software does not exist or operate in a vacuum; it relies on hardware in order to be functional. *See The Relationship Between Hardware and Software*, SOPHIA, https://perma.cc/HA8C-PLJW ("Essentially, computer software controls computer hardware. These two components are complementary and cannot act independently of one another. In order for a computer to effectively manipulate data and produce useful output, its hardware and software must work together. Without software, computer hardware is useless. Conversely, computer software cannot be used without supporting hardware."). Installing tracking software onto an already-existing device (the hardware, such as the cell phone or a data server) can be interpreted as turning that device into a tracking device. Thus, regardless of whether

under its plain meaning, Judge Lynch cited to the 1993 edition of Webster's Third New International Dictionary, defining "device," in one usage, as a "piece of equipment or a mechanism designed to serve a special purpose or perform a special function."[144] But even this definition alone does not facially limit the term to hardware—"a piece of equipment" certainly refers to hardware, but "a mechanism" does not. Mechanism is, in turn, defined as both "a piece of machinery" (hardware), or as "a process, technique, or system for achieving a result."[145] This latter definition, "a process, technique, or system," is not limited to hardware: Software that runs on a piece of hardware is clearly a system that achieves an intended result. Take the example of a recording device. Where law enforcement once may have needed an informant to wear a wire or carry a recorder, now all that is needed is an informant to install a recording device (a software application) onto his or her cell phone. Both scenarios, the hardware and the software, involve recording *devices*, and it would be merely formalistic to distinguish between the two.

Such is the case with a tracking device: Where law enforcement once may have needed to place a beeper in a vehicle, now all they need to do is install software onto the target's phone to collect identical information. And law enforcement generally does need to install software in order to access prospective location information from a cell phone because GPS data is not the kind of data cell service providers collect in the ordinary

---

one wants to refer to the software application as the tracking device (meaning the software is the device) or the cell phone with the tracking software downloaded onto it as the tracking device (meaning the hardware is the device), either understanding appears to suffice under the TDS's language requiring "installation of a mobile tracking device." 18 U.S.C. § 3117(a).

[144] *Ackies*, 918 F.3d at 199 n.5 (quoting MERRIAM-WEBSTER, INC., WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 618 (1993)).

[145] *Mechanism*, MERRIAM-WEBSTER, https://perma.cc/C5A4-6ZPA (last visited Apr. 9, 2021).

course of business.[146] The U.S. Department of Justice has explicitly acknowledged this to at least one federal court of appeals.[147] The FBI's *Domestic Investigations and Operations Guide* also attests to this fact, explaining that "[i]n the ordinary course of providing service to the customer, the provider does not typically use this GPS location data," and because of this, "the data may not constitute a 'record or other information' in the provider's custody within the meaning of [the Stored Communications Act]."[148] For records that are collected in the ordinary course of business, such as a hypothetical request solely for transmitting real-time CSLI (and no GPS data), this may turn on a more fact-intensive inquiry, exploring whether the provider must install *anything* in order to make such transmission possible. For example, if the provider needed to install software in order to give law enforcement automatic access to this data (even though the provider regularly collects such data anyway), this would sufficiently meet the statutory installation requirement. But this is a highly unlikely scenario given that modern cell phone location information requests generally seek the cell phone's GPS coordinates over time, or, at least GPS coordinates *in addition* to CSLI coordinates. The requested warrant in *Ackies* directed AT&T "to initiate a signal to determine the location of [the devices] at such times and intervals as directed by law enforcement for a period of 30 days."[149] Thus, not only did the SCA warrant in *Ackies not* compel the production of *stored*

---

[146] *See* Smith, *Why Are Precise Location Warrants a Thing?*, *supra* note 6 ("As the FBI correctly instructed its agents, cell site location data (CSLI) is typically generated and kept by providers in the ordinary course of its business, while more precise GPS data is not.")

[147] Gov't Response to Petition for Rehearing En Banc at i, United States v. Wallace, 866 F.3d 605 (2017) (No. 16-40701) ("E911 [GPS] location information is different from cell-site data, in part because cellular-service providers [including AT&T] typically do not collect and maintain E911 [GPS] location information in the ordinary course of business.")

[148] FBI, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE § 18.6.8.4.2.5.3 (2011).

[149] United States v. Ackies, No. 2:16-cr-20-GZS, 2017 WL 3184178, at *2 (D. Me. July 26, 2017).

information, but it also compelled the provider to *create* GPS data that would not otherwise exist.

Furthermore, the PRTT is not interpreted to refer only to the physical installation of hardware, even though it includes the same language as the TDS. Under the PRTT, law enforcement must similarly obtain a court order before "install[ing]" a pen register "device,"[150] but modern-day pen registers are also electronically-installed software, not physical hardware.[151] Despite using the same words, "install" and "device," the PRTT is not construed as narrowly as the First Circuit would construe the TDS.

Perhaps surprisingly, neither does the government seem to believe that "installation" and "device" are limited by their plain meaning to hardware. This is clear from the Government's filings in recent litigation over the FBI's Operation Playpen, during which the agency took control of a dark web child sexual exploitation imagery site.[152] As part of the investigation, a magistrate judge in the Eastern District of Virginia granted a Rule 41 warrant authorizing a Network Investigative Technique (NIT).[153] The Eleventh Circuit described the NIT as "government-created malware—specifically, a computer code" that "transmit[s] user information back to the FBI."[154] When a Playpen user downloaded images, "the NIT would essentially 'hitchhike' along, invade the host computer, and force it to send to the FBI (among other

---

[150] 18 U.S.C. §§ 3121-3125.

[151] *See In re* Prospective & Continuous Release of Cell Site Location Recs., 31 F. Supp. 3d 889, 898 n.46 (S.D. Tex. 2014). (citing Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 982-89 (1996) (describing the evolution of the pen register from mechanical device to computer system)).

[152] *See* United States v. Taylor, 935 F.3d 1279, 1283 (11th Cir. 2019).

[153] *Id.*

[154] *Id.*

information) the computer's IP address, the computer's host name, and the username associated with the computer."[155]

The Government argued that this remotely-installed piece of software was a tracking device under 18 U.S.C. § 3117, the TDS.[156] In its briefing, the Government asserted that a device is "simply 'a thing made or adapted for a particular purpose,' such as software."[157] The Government asserted that the NIT fit within the definition of a tracking device because Rule 41(b)(4) and § 3117 contemplate multiple kinds of devices:

> 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., like the beeper attached to a container of chloroform 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 through the internet.[158]

At least nineteen district courts agreed with the Government, holding that the NIT warrant was authorized as a tracking warrant under Rule 41(b)(4) and § 3117.[159]

On appeal, the four circuit courts considering the merits of this argument rejected the claim, but not on *Ackies* grounds that installation of software cannot constitute a tracking device.[160] The courts of appeals

---

[155] *Id.*

[156] *Id.* at 1285-86.

[157] Brief of the United States at 15, *Taylor*, 935 F.3d 1279 (No. 18-11852) (citing Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 940 (2005) (referring to "the device, the software in this case")).

[158] *Id.* at 16.

[159] *See* Smith, *Trifling with the Courts*, *supra* note 6.

[160] *Id.* The other seven courts that rejected challenges to the Playpen warrant declined

rejected the argument in the Playpen cases because the NIT did not track *movements*—it only received one-time location information identifying the targeted computers.[161] And if the device does not track movements, it is not a tracking device under § 3117. The courts of appeals also rejected the argument because the NIT was installed on computers outside of the district of the Virginia judge, so it would have violated the § 3117(a) venue limitation and been void nonetheless.[162]

The Playpen cases left open the question of whether the TDS tracking definition encompasses tracking software.[163] But the Government has only argued in front of one court of appeals that software *cannot* be a tracking device under the TDS.[164] It has argued in front of eleven others that it can.[165]

Briefly addressing policy concerns, the *Ackies* opinion also endorsed the district court's view that § 3117 cannot govern prospective cell phone location data because of its venue restriction: "'[I]t 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.'"[166] However, the First Circuit

---

to consider the merits of the argument that the NIT was a tracking device, assuming arguendo that the warrant was not validly issued. *Id.*

[161] *Id.* For more on the status of computers and other smart devices as tracking devices, see *infra* Part IV.

[162] *Id.*

[163] *Id.* ("The Third, Eighth, Ninth and Eleventh Circuits have all tacitly endorsed this proposition; only the First Circuit in *Ackies* has expressly rejected it.").

[164] *Id.*

[165] *Id.*

[166] United States v. Ackies, 918 F.3d 190, 199 (1st Cir. 2019) (quoting United States v. Ackies, No. 2:16-cr-20-GZS, 2017 WL 3184178, at *11 (D. Me. July 26, 2017)). The Government in the Playpen cases argued installation occurs on their site and not on the suspect's laptop, another budding legal issue in the digital era. Questions of where a search or installation occurs are beyond the scope of this piece. My instinct is with the First Circuit—the installation or search occurs at the location of the suspect's device, not at the FBI office, the provider's office, or elsewhere. *See generally*

has created a problem where there is none. The question of one-time location pings is an open question, but certainly is not restricted by the TDS. As the *Taylor* court rightfully held, a one-time ping for location does not constitute tracking *movement*.[167] Insofar as a one-time location ping may not require a high degree of process (or, at least lesser than a tracking warrant), this diminishes the issue of determining venue when, initially, law enforcement does not know the location of the phone. But an issue with the preliminary question of where the device is located in order to satisfy the venue restriction is not a persuasive reason to interpret away from the TDS and towards the SCA.[168] In fact, the First Circuit creates a bigger policy problem—the judicial crafting of a new ongoing surveillance regime where Congress did not create one.[169]

---

Geneva Ramirez, Note, *What* Carpenter *Tells Us About When a Fourth Amendment Search of Metadata Begins*, 70 CASE W. RES. L. REV. 187, 207 (2019).

[167] 935 F.3d 1279, 1283 (11th Cir. 2019).

[168] Union Bank v. Wolas, 502 U.S. 151, 158 (1991) (noting the mere fact "that Congress may not have foreseen all of the consequences of a statutory enactment is not a sufficient reason for refusing to give effect to its plain meaning").

[169] The First Circuit also briefly argued several provisions of Rule 41 are inconsistent with cell phones—the maintenance and removal provisions, and the daytime requirement. *Ackies*, 918 F.3d at 200. Maintenance and removal provisions apply just as well to software as to hardware. Software needs updates and maintenance, often to fix bugs. @sanjoy_62, *Software Engineering: Software Maintenance*, GEEKSFORGEEKS (Oct. 11, 2018), https://perma.cc/QLC7-TURT. Removal too applies to software: As law enforcement cannot leave a beeper permanently affixed to a past suspect's vehicle, they cannot leave the software linked to a suspect's phone indefinitely. For an example of a software removal application, see *Stanford Software Removal Tool*, STANFORD UNIVERSITY IT, https://perma.cc/FH5H-ZHCY. Neither is the daytime requirement necessarily inconsistent—while it reflects the somewhat outdated Rule 41 understanding of notice, there is no reason why law enforcement cannot comply and merely install the software during the day. This one odd but easily satisfiable restriction holds little weight.

### *C. Different Protections for Prospective Location Information Under the Tracking Device Statute and the Stored Communications Act*

The *Ackies* decision frustrates congressional purpose in the ECPA scheme while leading to the loss of statutorily-provided protections for suspects and criminal defendants. These concerns have broad reach given the SCA's recent extraterritorial extension under the Clarifying Lawful Overseas Use of Data (CLOUD) Act.

First, by ignoring Congress's deliberate choice to use a broad and technology-neutral definition, following *Ackies* frustrates the remedy to the problem Congress intended to address.[170] Congress created a scheme to regulate ongoing surveillance through ECPA, via the WTA, the PRTT, and the TDS. It chose to include characteristic ongoing surveillance protections, including prospective time limits, venue restrictions, reporting requirements, and more.[171] The SCA has no such protections.[172] Allowing this information to be gathered under the SCA fundamentally upsets Congress's intention that standard protections apply to prospective location information.

Furthermore, reading in an artificial technology limitation to hardware frustrates Congress's deliberate choice of a tech-neutral definition. Congress chose to adopt a broad definition, allowing the TDS to avoid going obsolete in the face of advancing technology. And the resulting loss of statutory protections was plain in *Ackies*: If governed by § 3117, then the magistrate judge in Maine would not have been able to issue a warrant to track a device initially located in New York.[173] The SCA allowed this kind of far-reaching magistrate power because it does not contain similar limits on jurisdiction.

---

[170] *See generally* United Steelworkers of Am. v. Weber, 443 U.S. 193 (1979) (interpreting statutory text with a view toward the particular problem that the legislation was meant to remedy).

[171] *See supra* note 86 and accompanying text.

[172] *See id.*

[173] Petition for Writ of Certiorari, *supra* note 75, at 3.

In fact, this jurisdictional issue has the potential to become a bigger controversy in light of Congressional passage of the CLOUD Act in 2018, which broadened the jurisdiction of the SCA extraterritorially.[174] The CLOUD Act amended the SCA to instruct a provider to disclose information and communications "regardless of whether such communication, record, or other information is located within or outside of the United States."[175] Thus, with the amended SCA and the reasoning of *Ackies*, a magistrate judge in Maine could not only authorize real-time tracking of a device in New York, but also the real-time tracking of a device in New Guinea.

Beyond the *Ackies* issues, other statutory protections are lost when prospective location information is obtained under the SCA instead of the TDS. A defendant loses statutorily-required notice when a warrant is issued under the SCA instead of the TDS and the related Rule 41 tracking warrant provisions.[176] The only party that receives notice of an SCA warrant is the provider (e.g., AT&T in *Ackies*), but providers are generally subject to non-disclosure orders precluding providing notice to customers that the government has sought access to their records.[177] The statutory right of a maximum limit on duration of the surveillance is also lost under the SCA. Rule 41 imposes a forty-five-day limit on prospective location information acquisition.[178] The duration of surveillance is limitless under the SCA.

## IV. BEYOND CELL PHONES: APPLICATIONS OF THE TRACKING DEVICE STATUTE TO OTHER SMART DEVICES

Since the TDS contains a technology-neutral definition, there is a question about how far the statute extends. This Part contains a brief

---

[174] 18 U.S.C. § 2523.
[175] 18 U.S.C. § 2713.
[176] FED. R. CRIM. P. 41(f)(2)(C).
[177] 18 U.S.C. § 2705(b).
[178] FED. R. CRIM. P. 41(e)(2)(C).

delineation of the boundaries of the TDS's reach. All of the technologies in this Part are less ubiquitous than cell phones, so it is perhaps unlikely law enforcement would seek a tracking warrant for one of these devices instead of or in addition to one for a cell phone.[179] Nonetheless, this Part covers wearable health monitors such as Fitbits and Apple Watches, and some non-wearable, less mobile technologies like laptop computers and smart home devices.

### *A. Wearable Devices: Fitbits and Apple Watches*

The TDS likely applies to wearable health monitors such as Fitbits and Apple Watches. A Fitbit, a health monitor resembling a bracelet that tracks heart rate and other physiological signals, could be co-opted to transmit real-time location information to law enforcement, as was the cell phone in *Ackies*.[180] Focusing on the language of the § 3117 technology-neutral definition, Fitbits can certainly track the movements of its user.[181] The same installation and device arguments discussed in Part III apply, as this technology would need software installed in order to start transmitting location in real-time to law enforcement.

The only argument against applying the TDS to a health monitor such as a Fitbit is that the technology came to be so long after 1986 that the enacting Congress could not have intended the TDS to govern it.[182] However, just as discussed above, the technology-neutral definition ought to trump these concerns. Furthermore, an appendix contained in the written records of the ECPA hearings includes a discussion of health

---

[179] Fitbit location data has been used in a criminal investigation. *See* Justin Jouvenal, *Commit a Crime? Your Fitbit, Key Fob or Pacemaker Could Snitch on You.*, WASH. POST (Oct. 9, 2017), https://perma.cc/W7D7-M7TC (detailing the case of Richard Dabate, in which the Fitbit location information of his dead wife's device was used to implicate him in her murder).

[180] *Id.*

[181] *Why Is the Fitbit App Prompting Me to Turn On Location Services?*, FITBIT HELP, https://perma.cc/97DQ-K8AY.

[182] *See supra* note 141.

monitors as potential location tracking devices.[183] Fitbits are, in some sense, the modern incarnation of the health monitors discussed in these hearings, so if the health monitors of the 1980s would have fit in the definition of a tracking device, Fitbits should not be excluded from coverage solely on the grounds that the technology has advanced such that it can provide health monitoring non-invasively.

Apple Watches should certainly fall under the ambit of the TDS. Apple Watches, while also health monitors, are properly classified as cell phones. Many Apple Watches are equipped with a SIM card, so the watch itself can make phone calls and send text messages via cell towers.[184] Apple Watches without cell chips generally have onboard GPS, or are tethered to an underlying iPhone, using the iPhone's GPS and SIM card to carry out functions.[185] An Apple Watch, while also a health monitor, is functionally also a cell phone (or an extension of a cell phone), and should not be distinguished from it.

### *B. Computers and Other Relatively Static Smart Devices*

Many other devices also track location information but are not as mobile as wearable Fitbits and Apple Watches. This consists of essentially three categories of devices: movable devices the owner occasionally moves (like a laptop computer), movable devices the owner infrequently moves (like a device equipped with Amazon's Alexa software), and immovable devices (like smart thermometers).

---

[183] *See First Session on the Matter of Wiretapping, Electronic Eavesdropping, and Other Surveillance: Before H. Judiciary Subcomm. on Courts, C.L., and the Admin. of Just.*, 94th Cong. 794 (1975) ("But the same electronic sensors that can warn us of an impending heart attack can locate us, track our movements, and expose our emotions and our thoughts.").

[184] Christine Chan & Lory Gil, *Apple Watch Cellular vs GPS: What's the Difference?*, IMORE (Feb. 24, 2021), https://perma.cc/4ZVL-6827 ("Apple Watch LTE coverage lets you do anything solo on the Apple Watch that you can do when tied to your iPhone's data. That includes placing calls, receiving messages, using Siri, navigating via Maps, playing with third-party apps, and just about anything else.").

[185] *Id.*

First, consider movable devices, such as a laptop computer. This computer could hypothetically be a tracking device, as it could track the movements of its user. As was clear from the Playpen cases, there are many ways to get location information from a computer.[186] However, as explained by the Eleventh Circuit in *Taylor*, a tracking device must track the *movements* of a user.[187] If law enforcement seeks to use a laptop for a one-time ping to get location information, this does not transform the device into a tracking device. However, if law enforcement seeks to get location information from the laptop periodically to track the movements of the user, it would then squarely fit the definition in § 3117. The application of the TDS then turns on the nature of the government's request.

The next category of smart devices consists of ones that the user can move, but due to the nature of the object, the user infrequently does so—as such, these devices are relatively static. This category consists of devices such as Google Home or an Amazon Echo equipped with Alexa. An Alexa equipped device could certainly be used to track its user's movements if the user tends to pick it up and carry it around,[188] but the user generally places the speaker in a particular area of the home and infrequently moves it from there.[189] Like the computer, the classification of a relatively static smart device turns on its intended use. If law enforcements seeks one-time location information from an Alexa equipped device, this is not within the jurisdiction of the TDS; however,

---

[186] For a particularly creative one, the warrant in the Playpen cases was used to "activate the computer's camera over a period of time and capture latitude/longitude coordinates of the computer's physical location." *In re* Warrant to Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753, 758 (S.D. Tex. 2013).

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

[188] *See* Khari Johnson, *Amazon Alexa Skills Can Now Access User Location for Services Such As Food Delivery*, VENTUREBEAT (Apr. 5, 2017, 8:17 AM), https://perma.cc/P37L-UEBT.

[189] *See, e.g.*, Katie Conner, *4 Best Uses for Alexa in Every Room of Your Home*, CNET (Nov. 5, 2020), https://perma.cc/HLW8-N6B4 (illustrating the typical user practice for smart speakers—selecting a room to place the device, and leaving it there indefinitely).

if the government seeks location information from the device every few minutes for forty days because law enforcement suspects the user regularly brings the device to an area of investigatory interest, the Alexa equipped device is a tracking device.[190] However, because a user tends to move her smart speaker less frequently than she tends to move, for example, her laptop computer, it seems far less likely that an Alexa equipped device will, in practice, fall under the jurisdiction of the TDS.

The last category of smart devices are immovable devices, such as smart thermostats,[191] smart door locks,[192] and other truly static smart devices. In this category, some devices may fall under the jurisdiction of the TDS, while others do not. Their ECPA classification turns on the difficult question of whether they capture *movement*. A smart thermostat, for example, never itself moves *with* the user, but it can detect *when a user is and is not home.* For instance, Stanford University recently installed smart thermostats into on-campus graduate housing—these thermostats consist of a main control device located in the common area, and then smaller connected sensors located in each room (one in the common area, and one in each individual bedroom).[193] Through this system, the smart thermostat senses whether anyone is home, and, if so, which room they are in.[194] If someone moves from the common area into a bedroom, the smart thermostat senses this and then begins temperature control in the newly-occupied bedroom.[195] This system allows Stanford to track a

---

[190] *See* 18 U.S.C. § 3117.

[191] *Nest and Google Home. Now Under One Roof.*, GOOGLE STORE : NEST, https://perma.cc/B5E6-KQUW.

[192] *See* Jon Chase, *The Best Smart Locks*, WIRECUTTER, https://perma.cc/8F7T-JPRB (last updated Dec. 13, 2019).

[193] *See New Smart Thermostats at Munger*, SUSTAINABLE STANFORD (Aug. 20, 2019), https://perma.cc/TUE3-FEH4.

[194] *Id.* ("The system includes an online dashboard, which tracks 200 smart thermostats and 360 sensors that work synergistically to detect occupancy . . . . The Ecobee smart thermostat allows the heating and cooling system to go into an energy-saving mode when rooms are unoccupied . . . .").

[195] *See id.*

resident's movements throughout her apartment, historically or in real-time. Even though the immovable device in this instance does not move with the user, it is spread out through many components in a system that allows it to track movement throughout a home. This is indeed a tracking device, and if law enforcement wanted access to this data, it would need a Rule 41 tracking warrant.

However, a less-complex smart thermostat that does not capture movement is not a tracking device. For example, a smart thermostat installed in one place in the home may track when people are or are not home, but it does not track movements within the home. This is not a tracking device, because this device does not permit law enforcement to track the movements of people. This system more closely resembles a singular location ping. When someone is home, the smart thermostat reveals the location of the user as within the square footage of the home. However, when no one is home, the smart thermostat reveals only that—the user is *not* within the square footage of the home, but may be anywhere else. Pieced together with other sources of information, this kind of data can suggest to law enforcement the whereabouts of the user; for example, if the smart thermostat reflects no one is home, and another smart device reflects the user is at their usual place of work, this data can support a location tracking effort. Yet, the static thermostat alone does not capture this movement the way a cell phone or beeper can. Therefore, the smart thermostat, smart door lock, or other immovable smart device, while providing rough indications of location, is not a tracking device for purposes of the TDS.

## V. CONCLUSION

As law enforcement continues to rely on cell phones to track the prospective location and movements of suspects, the statutory classification of these devices demands resolution. Because a cell phone permits the tracking of the movements of its user, this device squarely falls within the plain language of the technology-neutral definition of

tracking devices, and thus under the jurisdiction of the TDS. Lower courts should not repeat the interpretive mistakes of the First Circuit.

*Carpenter* certainly was not the last word on the use of cell phones as law enforcement location tracking tools, but litigants and criminal defendants ought not wait to see if the Supreme Court will extend constitutional protections to prospective location information. Neither should they wait for the day Congress decides to finally update ECPA after decades of growing calls to do so. Congress already had the foresight to use a definition of tracking devices in § 3117 that would adapt to changing technology, and it should be taken seriously. Litigants should start challenging statutorily invalid SCA warrants purporting to authorize access to prospective cell phone location information, and courts should start engaging in ECPA analysis that does not forget the TDS.