Catholic University Journal of Law and Technology

Volume 26 | Issue 2 Article 3

2018

Privacy vs. Protection: Why Tracking Mobile-device Location Data Without a Warrant Requires a Fourth Amendment Exception

Andrew Stover
Michigan State University College of Law

PRIVACY VS. PROTECTION: WHY TRACKING MOBILE-DEVICE LOCATION DATA WITHOUT A WARRANT REQUIRES A FOURTH AMENDMENT EXCEPTION

Andrew J. Stover[+]

"*For time and the world do not stand still. Change is the law of life. And those who look only to the past or the present are certain to miss the future*."[1]
– John F. Kennedy

Imagine an America where the police and government were able to determine where people have been, or even where they currently are, just by looking at their mobile-device. An America where the government tracks the places one travels without limit; an America eerily reminiscent of George Orwell's *1984*.[2] That America could be fast approaching based on recent legal rulings.[3] If left unchecked, modern America may become fictional Oceania.[4]

On May 31, 2016, the Fourth Circuit Court of Appeals joined the Fifth, Sixth, and Eleventh Circuits in ruling that law enforcement's requests for mobile-device data records from service providers are not searches under the Fourth

[+] B.A. 2015, The Pennsylvania State University; J.D. 2018, Michigan State University College of Law.

1 John F. Kennedy, Address in the Assembly Hall at the Paulskirche in Frankfurt (June 25, 1963).

2 *See* GEORGE ORWELL, 1984 at 5 (Signet Classic 1961) ("[T]he eyes follow you about when you move. Big Brother Is Watching You.").

3 *See id.* at 6 ("[A] helicopter skimmed down between the roofs, hovered for an instant like a blue-bottle and darted away again with a curving flight. It was the Police Patrol, snooping into people's windows."); *see e.g.*, State v. Tate, 849 N.W.2d 798, 805–806 (Wis. 2014) (reasoning how a defendant does not have a reasonable expectation of privacy when one "is traveling down a public highway.").

4 *See* ORWELL, *supra* note 2, at 7 ("Winston kept his back turned to the telescreen. It was safer; though as he well knew, even a back can be revealing.").

Amendment and thus do not require a warrant.[5] While circuits to hear cases on this issue may all be in agreement, lower federal courts outside of those circuits' jurisdictions are not so united.[6] No circuit yet to rule on the issue controls a jurisdiction in which a district court has ruled in favor of privacy rights.[7] Although this particular issue is novel due to the growing use of mobile devices and Global Positioning System (GPS) tracking, it is part of a family of issues that have been proceeding through the courts since the turn of the century.[8]

Scholarship on tracking mobile-device location data has focused on the increased use of such data by law enforcement to deduce suspects' physical

---

5 *See, e.g.*, United States v. Riley, 858 F.3d 1012, 1018 (6th Cir. 2017) (holding the search of "an individual's location (or a cell phone's location), so long as the tracking does not reveal movements *within* the home (or hotel room), does not cross the sacred threshold of the home" and does not violate the Fourth Amendment); United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (reasoning the defendant did not have a reasonable expectation of privacy because when he registered his phone with the carrier, he voluntarily provided his personal information); *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 611 (5th Cir. 2013) (holding that compelling "cell phone service providers to produce the historical cell site information of their subscribers [were not] per se unconstitutional."); *see also* Jenna McLaughlin, *Appeals Court Delivers Devastating Blow to Cellphone-Privacy Advocates*, INTERCEPT (May 31, 2016), https://theintercept.com/2016/05/31/appeals-court-delivers-devastating-blow-to-cell-phone-privacy-advocates/; *No warrant needed to get cell phone location: US court*, PHYS.ORG (May 31, 2016), http://phys.org/news/2016-05-warrant-cell-court.html (explaining individuals who "voluntarily disclosed to a third party" and in those cases, "cell phone users 'voluntarily' give that data to carriers whenever they make a call or send a text message" and have no expectation of privacy).

6 *See, e.g.*, United States v. Graham, 824 F.3d 421, 427-28 (4th Cir. 2016) (holding the defendants "assumed the risk" when the phone company turned over the defendants' cell phone information); *In re* Application for Telephone Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1039, 1042 (N.D. Cal. 2015); United States v. Lambis, 744 F. Supp. 3d 606, 616 (S.D.N.Y. 2016).

7 *See, e.g.*, United States v. Davis, 785 F.3d 498, 507, 511 (11th Cir. 2015) (*en banc*); United States v. Guerrero, 768 F.3d 351, 358 (5th Cir. 2014); United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).

8 *See* Riley v. California, 134 S. Ct. 2473, 2477 (2014) (holding that police generally cannot search the contents of an arrested person's cell phone without a warrant); United States v. Jones, 565 U.S. 400, 402 (2010) (holding that attaching GPS devices to cars constitutes a search that requires a warrant). *See generally* Naomi LaChance, *At Supreme Court, Debate Over Phone Privacy Has A Long History*, NPR (Mar. 8, 2016), http://www.npr.org/sections/alltechconsidered/2016/02/29/468609371/at-supreme-court-debate-over-phone-privacy-has-a-long-history (explaining, for example, the Supreme Court has unanimously held attaching GPS devices to cars constitutes a search that requires a warrant); Alex Alben, *How to protect privacy in the digital age: a constitutional amendment*, SEATTLE TIMES (Apr. 20, 2015), https://www.seattletimes.com/opinion/how-to-protect-privacy-in-the-digital-age-a-constitutional-amendment/ (proposing for a new amendment to "safeguard privacy as a first principle of American law," given that "widespread deployment of GPS . . . our digital footprints are tracked and recorded.").

locations, usually without a warrant.[9] As is often the case, scholarship is divided as to the legality of law enforcement's compelling companies to disclose records—without a warrant—in order to track a suspect.[10] On one side is scholarship that recognizes the need for law enforcement to protect the general public, which agrees with the circuits that such information retrieval is not a search under the Fourth Amendment.[11] On the other side is scholarship that emphatically argues such use of mobile-device location data is a search and—without a warrant—is an unconstitutional invasion of privacy.[12] Some scholarship advocates for an approach from both the judiciary and society towards being more informed and not simply applying "blind justice," which is to say refraining from making gut reactions and uninformed decisions by taking into account data and evidence.[13]

This Comment advocates for the recognition of a new exception to the Fourth Amendment's warrant requirement. Law enforcement's tactic of arresting suspects by using location tracking data, obtained by compelling service

---

9 Martin Dolan, Noreen Lennon & Karen Munoz, *Use of Cell Phone Records and GPS Tracking*, 24 CBA REC. 38, 39 (2010); *see, e.g.*, Brian L. Owsley, *Cell Phone Tracking in the Era of United States v. Jones and Riley v. California*, 48 TEX. TECH. L. REV. 207, 227 (2015) (stating, under the third-party doctrine, mobile device users do not have a reasonable expectation of privacy to their location data); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 535 (2017).

10 *Compare* Shima Baradaran, *Rebalancing the Fourth Amendment*, 102 GEO. L.J. 1, 41 (2013), *with* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 715 (2011) (explaining how law enforcement can compel companies to turn over various phone data as permissible while others contend the constitutional implications of obtaining public data).

11 RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE (2014) (noting the third-party doctrine and compulsion of location data can be harmonized with Fourth Amendment case law); *see, e.g.*, William J. Stuntz, *Warrants and Fourth Amendment Remedies*, 77 VA. L. REV. 881, 885 (1991) (suggesting law enforcement should be able to search without a warrant because "[t]he reasons for requiring warrants are genuine, but not strong; it is entirely plausible that the system would function better without them.").

12 *See* Alessandra Suuberg, *Big Foot, Big Brother . . . and a Big Step Backwards for Your Fourth Amendment Rights: The Sixth Circuit Approves Warrantless Cell Phone Tracking in United States v. Skinner*, 15 TUL. J. TECH. & INTELL. PROP. 319, 330 (2012); *see also* Ian Herbert, *Where We Are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, 16 BERKELEY J. CRIM. L. 442, 448 (2011) (explaining GPS can "reveal the target's location every second of every day, while others only provide information when asked.").

13 Baradaran, *supra* note 10, at 3–4 ("Blind balancing" is "the process of decision making based simply on common sense and a gut assessment of risk, without consideration of data, evidence, or empirical studies" and ensures "important privacy rights enshrined in the Fourth Amendment are protected by individuals who are seen as criminals in the eyes of the court . . . [B]ecause the harmed party is identified as a criminal at the outset, the balance starts skewed in favor of the government.").

providers to disclose users' mobile-device information, may constitute a "search," yet it may be a "search" that is not unconstitutional under the Fourth Amendment.[14] The Supreme Court, due to recent lower court rulings, should take up the issue and create a new exception to the warrant requirement that protects privacy interests in electronic data contained on one's mobile device.[15] This exception must recognize a presumption of privacy in mobile devices, thus making it a search requiring a warrant to obtain location data.[16] The exception would then balance citizens' privacy interests against governmental interests, requiring the government to overcome the presumption of privacy through a strong showing of need.[17]

Part I discusses the evolving history of mobile devices in the United States, beginning with the rise of mobile devices, data networks, and modern "smart phones," and gives a general overview of differing approaches to location data protections.[18] Part II provides an overview of federal court jurisprudence on the issue of whether police's obtaining location data records without a warrant is an unconstitutional search.[19] Part III offers an overview of Supreme Court jurisprudence regarding similar issues pertaining to location tracking and data privacy.[20] Part IV analyzes how such uses of location tracking data by law enforcement are unconstitutional searches when conducted without a warrant in

---

14 *See* Jeremy H. Rothstein, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 530 (2012) (explaining how cell phone users "voluntarily disclose their location to third parties merely by carrying a cell phone that can be tracked with GPS."); *e.g.*, Charles Blain, *Police Could Get Your Data Location Without A Warrant. That Has To End*, WIRED (Feb. 2, 2017, 7:00 AM), https://www.wired.com/2017/02/police-get-location-data-without-warrant-end/ (describing how the victim was able to receive a restraining order because the defendant stalked her using his cell phone).

15 *See, e.g.*, David Smith, *Supreme court considers limits on police tracking via mobile phone data*, GUARDIAN (Nov. 29, 2017, 4:45 PM), https://www.theguardian.com/law/2017/nov/29/supreme-court-considers-limits-on-police-tracking-via-mobile-phone-data (discussing the implications of the government relying on a 1979 Supreme Court decision that distinguished between phone records and the actual conversations in this modern era).

16 *See* Henry F. Fradella, Weston J. Morrow, Ryan G. Fischer & Connie Ireland, *Quantifying Katz: Empirically Measuring Reasonable Expectations of Privacy in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 311 (2011) (arguing that the technological advancements of this era calls for updated outlooks of constitutional privacy concerns).

17 *See, e.g.*, Glenn Chatmas Smith, *We've Got Your Number (Is it Constitutional to Give It Out): Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145, 199 (1989); *see also* Suuberg, *supra* note 12, at 330 (explaining how many entities criticized United States v. Skinner because it denies "an expectation of privacy in cell phones.").

18 *Infra* Part I.

19 *Infra* Part II.

20 *Infra* Part III.

certain instances, but not others, and how the proposed exception would operate.[21]

I. EVOLVING HISTORY OF A MOBILE NETWORK SOCIETY

Over the past forty-three years, the United States has become increasingly reliant on mobile devices.[22] In under two generations, mobile technology has boomed, with over 64% of American adults owning a smartphone.[23] With the rise of mobile-device usage the ability of law enforcement to use such devices as a tool to track suspects has also risen.[24] The prevalence of mobile devices in everyday life has led to approaches for tracking location data,[25] ranging from allowing police to track without a warrant[26] to requiring police to obtain a warrant before tracking.[27] The issue of tracking suspects through their location

---

21 *Infra* Part IV.

22 *See* Freiwald, *supra* note 10, at 681, 702 (explaining location data provides law enforcement information about an individual's arrival and departure time and from where); *see also* Ellen Gibson, *Smartphone dependency: a growing obsession with gadgets*, USA TODAY (July 7, 2011), http://usatoday30.usatoday.com/news/health/medical/health/medical/mentalhealth/story/2011/07/Smartphone-dependency-a-growing-obsession-to-gadgets/49661286/1 (remarking that added dependence on mobile devices comes as Americans choose mobile phones over iPods, cameras, maps, and address books).

23 Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RES. CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/; *see also* Blain, *supra* note 14 ("[O]n average, American millennials check their phone roughly 82 times a day.").

24 *See, e.g.*, Mara Van Ells, *Law enforcement officers use cellphone tracking as a tool*, BISMARCK TRIB. (May 26, 2012), http://bismarcktribune.com/news/local/crime-and-courts/law-enforcem…racking-as-a-tool/article_23531016-a5c1-11e1-a957-0019bb2963f4.html (explaining how "cellphone information is a very useful tool for law enforcement and prosecutors."); *cf.* Jamie Condliffe, *Warrantless Tracking of Phone Location Data Could Get Harder*, MIT TECH. REV. (June 6, 2017), https://www.technologyreview.com/s/608042/warrantless-tracking-of-cell-phone-location-data-by-the-police-could-get-harder (tracking criminals could prove to be difficult despite the advent of cell phone use).

25 *See, e.g.*, *Cell Phone Location Tracking Laws by State*, ACLU, https://www.aclu.org/map/cell-phone-location-tracking-laws-state (last visited May 24, 2018); Charles Arthur, *iPhone keeps record of everywhere you go*, GUARDIAN (Apr. 20, 2011, 9:06 AM), https://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears ("Apple's iPhone keep track of where you go – and saves every detail of it to a secret file on the device which is then copied to the owner's computer when the two are synchronised [sic].").

26 *See* United States v. Skinner, 690 F.3d 772, 774, 777, 781 (6th Cir. 2012) (holding that the defendant "did not have a reasonable expectation of privacy in the GPS data and location on his cell phone.").

27 *See* Pub. Act 098-1104, § 10 ILL. GEN. ASSEMB. (Ill. 2014) ("[A] law enforcement agency shall not obtain current or future location information pertaining to a person or his or her effects without first obtaining a court order based on probable cause."); *see* Skinner, 690 F.3d at 774, 777, 781.

data is one that continues to grow and sow disagreement.[28]

A. Overview of Fourth Amendment Jurisprudence: A Primer

The Fourth Amendment is one of the most zealously coveted and protected parts of the United States Constitution.[29] It guarantees the right of Americans, "the people," to be free from searches of their homes, personal effects, and body, as well as seizure of their persons and property by the government without reasonable grounds.[30] Additionally, before the government may search or seize it must obtain a warrant, which is based on probable cause supported by statements, or evidence that describes the place being searched and the people or items being seized.[31]

One of the more important aspects of the Fourth Amendment is the "reasonable expectation of privacy" inquiry,[32] which is both a legal standard[33] and a constitutional safeguard.[34] As formulated by Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347 (1967), the existence of reasonable expectations of privacy in persons, places, and objects are determined using a two-part test.[35] That test has been applied for the past fifty years by United States courts to determine whether privacy rights attach to Americans' interactions, possessions, technologies, living quarters, and countless other areas.[36]

---

28 *See, e.g.*, *Cell Phone Location Tracking Laws by State*, *supra* note 25 (explaining how "the status of your privacy protections depends on where you are. For example, your location information is protected in Montana, but not in Georgia.").

29 U.S. CONST. amend. IV; *see, e.g.*, Barry Friedman & Orin Kerr, *The Fourth Amendment*, NAT'L CONST. CENT., https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv (last visited May 24, 2018) (understanding the Fourth Amendment "places restraints on the government any time it detains (seizes) or searches a person or property.").

30 *See* U.S. CONST. amend. IV.

31 *See id.*; *see, e.g.*, *Probable Cause*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("A reasonable ground to suspect that a person has committed or is committing a crime or that a place contains specific items connected with a crime.").

32 *Cf.* United States v. Jones, 565 U.S. 400, 404–05 n.3 (2012) (explaining how the Fourth Amendment values one's property rights and when the Government installs a GPS on a vehicle, they have physically intruded on a constitutionally protected area).

33 Katz v. United States, 389 U.S. 347, 360–61 (Harlan, J., concurring) (1967).

34 *Id.* (stating the infamous legal standard that there are places and objects in which a person has "a constitutionally protected reasonable expectation of privacy."). *Cf.* Jones, 565 U.S. at 404–05 n.3.

35 Katz, 389 U.S. at 361 (Harlan, J., concurring) (explaining Justice Harlan's test comprised an inquiry into (1) whether the person exhibited an actual expectation of privacy, and (2) whether society recognizes the expectation as reasonable).

36 *Cf.* Florida v. Jardines, 569 U.S. 1, 7, 9–10 (2013); Kyllo v. United States, 533 U.S. 27, 32, 35 (2001); United States v. Padin, 787 F.2d 1071, 1076 (6th Cir. 1986); United States v. Cabrera, No. 11–117–GMS, 2014 WL 3540894, at *14 (D. Del. July 15, 2014). In

The newest frontier for the Fourth Amendment's reasonable expectation of privacy inquiry is that of mobile-device user data.[37] Courts have been grappling with whether citizens have privacy rights to their data and whether those rights rise to the level of protection granted in *Katz*.[38] Even the Supreme Court has entered the fray, weighing in on the constitutionality of warrantless searches of cell phone videos and images, GPS tracking devices on cars, and pen registers on home phones.[39] Yet until recently, the Court has declined to address the issue of warrantless tracking of location data by law enforcement.[40] That decision, expected sometime in 2018, could definitively determine whether the Fourth Amendment applies to citizens' mobile device data.[41]

B. The Rise of Technology (GPS and Data) in the United States

Technology has quickly become present in almost every facet of American life, spurring a revolution of new portable devices that rely on mobile networks, which constantly communicate location data to service providers.[42] While the mobile-device may now be an everyday norm, it elicited ridicule when first released.[43] History proved even the most astute experts to be sensationally

---

fact, as of May 23, 2018, *Katz* has been cited 12,314 times by courts in the United States. *Citing References for* Katz v. United States, Westlaw KeyCite, https://1.next.westlaw.com/RelatedInformation/I64df71169c1d11d9bc61beebb95be672/kcCitingReferences.html?docSource=57694273439b4fb49d17ae3493cb2634&pageNumber=1&facetGuid=h562dbc1f9a5f4b0c9e54031a19076b9c&transitionType=ListViewType&contextData=(sc.DocLink) (search Katz v. United States; then click on the case; then click Citing References on menu bar and choose cases from the menu on the left).

37 *See, e.g.*, Jeremy Fogel, *From the Bench: A Reasonable Expectation of Privacy*, LITIG. J., Spring 2014, at 1.

38 *Cf.* Kyocera Wireless Corp. v. Int'l Trade Comm'n, 545 F.3d 1340, 1351, 1359 (Fed. Cir. 2008); United States v. Pierre, 435 Fed. Appx. 905, 908 (11th Cir. 2011).

39 *See* Riley v. California, 134 S. Ct. 2473, 2489–90 (2014) (reasoning that searching a phone's physical properties to determine danger is different from searching a phone's internal data, with the latter being unconstitutional without a warrant); United States v. Jones, 565 U.S. 400, 408–09 (2012) (holding that GPS tracking devices attached to vehicles outside the scope of a warrant are unconstitutional); Smith v. Maryland, 442 U.S. 735, 742 (1979) (ruling that there is no expectation of privacy in the numbers dialed from a home phones owned by the service provider).

40 *See* Lawrence Hurley, *U.S. Supreme Court to Settle Major Cellphone Privacy Case*, REUTERS (June 5, 2017), http://www.reuters.com/article/us-usa-court-mobilephone-idUSKBN18W1RY (explaining, in technology and criminal law cases, the Supreme Court has ruled that "a warrant is required to place a GPS tracking device on a vehicle" and "police need a warrant to search a cellphone that is seized during an arrest.").

41 *See* Carpenter v. United States, 819 F.3d 880 (6th Cir. 2015), *cert. granted*, 85 U.S.L.W. 3567 (U.S. June 5, 2017) (No. 16–402).

42 *See* Gibson, *supra* note 22 (remarking that added dependence on mobile devices comes as Americans choose mobile phones over iPods, cameras, maps, and address books).

43 *See* Will Oremus, *Forty Years Ago Today, Snarky Tech Journalists Made Fun of the First Cellphone*, FUTURE TENSE (Apr. 3, 2013, 2:10 PM), www.slate.com/blogs/

incorrect.[44]

That original device, the Motorola DynaTAC, had a battery that could last up to eight hours.[45] Jumping to 1993, Bellsouth and IBM released the "Simon personal communicator phone," which was touted as the first "smartphone."[46] In 2002, the next generation of technologically advanced smartphones was released into the market.[47] The world's first modern smartphone was born in 2007 with the release of the iPhone, Apple's venture into the mobile device market after previously concentrating on its Mac computers.[48] In the product release, Apple claimed the iPhone was three devices rolled into one: an iPod, a mobile phone, and a wireless communication device.[49]

With the dependency of Americans on mobile devices, and especially cellular devices, law enforcement has had to adapt and apply new approaches in response to the technology.[50] Service providers are able to assist law enforcement in

---

future_tense/2013/04/03/cell_phones_40th_birthday_skeptics_made_fun_of_first_mobile_phone.html (describing how Associated Press journalists compared the release of the first cell phone to the fictions in television series and while cellphones were too expensive for the average consumer, only 13% of the American business community would have been interested in purchasing such a device at that time).

44 *Cf.* Gibson, *supra* note 22 (providing that dependence on cell phones have increased in society as relevance to perform daily tasks like shopping have become more prevalent); Smith, *supra* note 23.

45 Oremus, *supra* note 43. Upon releasing its product, Motorola quipped that in its opinion, people would continue using their car phones and cell phones would not replace standard telephones. *See* Gibson, *supra* note 22.

46 *See* Doug Aamoth, *First Smartphone Turns 20: Fun Facts About Simon*, TIME (Aug. 18, 2014), http://time.com/3137005/first-smartphone-ibm-simon/ (describing that The Simon was designed as a phone first and computer second and demanded a $900 price on average with Bellsouth for features such as e-mail, on-screen writing (with a stylus), keypad with letters and numbers, and a calendar).

47 *See 5 major moments in cellphone history*, CBC NEWS, http://www.cbc.ca/news/technology/5-major-moments-in-cellphone-history-1.1407352 (last updated Apr. 3, 2013) (providing that The Nokia 7650 and the Sanyo SPC-5300, released in 2002 had the distinction of being the next-generation of smartphones. These phones were the first to incorporate built-in cameras, boasting large pixel color displays, user-controlled tones, white balance, and zoom while the Nokia 7650 had a 176x208 pixel display); *cf.* Michael Grothaus, *iPhone 7 vs Samsung Galaxy S7: The BIG Flagship Fight Rages On*, KNOW YOUR MOBILE (July 19, 2017, 4:34 PM), http://www.knowyourmobile.com/mobile phones/apple-iphone-7/23410/iphone-7-vs-samsung-galaxy-s7-edge-specs-features-price-detailed-ios-10-android-n (showing the even more advanced features in smartphones of the largest competing companies); *see also iPhone 7 Display*, APPLE, http://www.apple.com/iphone-7/specs/ (last visited Mat 24, 2018) (describing the iPhone 7's 1334 x 750 pixel resolution, which makes the 2002 smartphones seem like ancient history).

48 *5 major moments in cellphone history*, *supra* note 47.

49 *See id.* (describing the iPhone's advanced features, including a touch screen, visual voicemail box, touchpad keyboard, photo library, and a large display for watching movies or television).

50 *See* Van Ells, *supra* note 24 (quoting a North Dakota police officer as saying, "as

finding citizens' whereabouts through tracking location data.[51] While such methods of tracking suspects may not be used on a daily basis, there are times where such methods are used without a second thought, as is the case in tracking suspects of terrorism.[52] Police favor mobile device tracking because it provides nearly instantaneous results.[53]

While it may appear that law enforcement would always employ location data tracking methods, it is much more difficult to implement such techniques.[54] The policies of large service providers, such as AT&T and Verizon, allow expert analysts to determine if a true emergency exists[55] and whether to hand over information to police.[56] Once law enforcement obtains the information, through either compulsion or willing participation, the information can be sent to officers every five, fifteen, or thirty minutes depending on the urgency of the investigation.[57]

As the history of mobile device data, location tracking data, and Internet data progresses, there will be a constant balancing of public interests of privacy and government interests of security. One reason service providers may be reluctant to turn over location data is that the public—that is, their customers—sees mobile data as a privacy right to be protected.[58] The government no longer

---

cellphones become more and more sophisticated . . . we see more and more cases where they're being used in criminal attempts and criminal types of enterprises.").

51 *See id.* (stating that in 2012, a son was arrested and charged with his mother's murder and police were able to use cell phone tracking data provided by the cellular company to locate the son).

52 *See id.* (explaining in emergency situations, child pedophilia situations, and kidnapping situations tracking through cellular companies' data is oft-used).

53 *See id.* (quoting a North Dakota police officer as saying, "[t]echnology . . . is kind of a double-edged sword. More crimes are able to be committed since we have this technology but at the same time, we're able to investigate and successfully prosecute more cases because of this technology.").

54 *See id.* (explaining that police requests may be denied if the mobile provider does not believe that the situation constitutes an emergency and in such instances, law enforcement must obtain a warrant for the data whenever possible and otherwise hope that the situation constitutes an emergency that convinces the mobile service provider to turn over information willingly).

55 *See* Blain, *supra* note 14 (noting these policies are not just provided by cell phone service providers but companies such as Amazon have denied turning over data without a warrant where law enforcement requested such information from an Echo).

56 *See* Van Ells, *supra* note 24 (providing that without a showing by police of the existence of a true emergency, the analyst may transfer the request for data to a director who is responsible for determining whether to grant the request or inform the police they need a subpoena because service providers guard their customers' data information jealously, in part because the information can be used by law enforcement to pinpoint the exact location of the customer).

57 *Id.*

58 *See* Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (finding that 74% of Americans believe it is very important they are in control of

enjoys the support of public opinion that allowed for more invasive security measures like the PATRIOT Act and other post-9/11 measures.[59] The PATRIOT Act, which allowed the government to increase its surveillance of Americans' personal mobile and Internet data, was seen as a necessary protective measure from future terror attacks after the tragedy of September 11, 2001.[60]

C. General Information on Cell Towers and Tracking Technology

Modern mobile devices are amazing pieces of technology, yet they cannot function without the aid of a cell tower.[61] These towers serve as conduits for all mobile services, applications, and data emanating from mobile devices.[62] Service providers place towers in a hexagon pattern to increase the total service area and ensure that no holes in coverage exists.[63] By studying data traffic across networks in cell tower areas, carriers can determine whether there needs to be

---

who gets their information, and 65% say it is very important that they can control what information is collected about them); *see also* Smith, *supra* note 23 (stating that a majority of Americans own smartphones, which supports the proposition that privacy of these Americans' data is a major concern).

59 Sophia Rosenbaum, *Privacy vs. Protection: Public Wrestles with What's Most Important*, NBC NEWS (June 6, 2013, 10:01 AM), http://usnews.nbcnews.com/_news/2013/06/06/18802435-privacy-vs-protection-public-wrestles-with-whats-most-important?lite; *see The USA PATRIOT Act: Preserving Life and Liberty*, DEP'T OF JUSTICE, https://www.justice.gov/archive/ll/highlights.htm (last visited May 24, 2018) (describing that the PATRIOT Act was passed in response to the 9/11 attacks).

60 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (describing that the PATRIOT Act allowed the government to intercept communications, seize voicemail messages with warrants, and modify the law relating to pen registers); *see* David W. Moore, *Public Little Concerned About Patriot Act*, GALLUP (Sept. 9, 2003), http://news.gallup.com/poll/9205/public-little-concerned-about-patriot-act.aspx (noting that shortly after the 9/11 terrorist attacks, the public was not as concerned with loss of civil liberties in favor of counter-terrorism tactics and that two years later, the trend increased in favor of civil liberties over government interference).

61 Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 3 (2013); *see* MICHAEL HARRIS, HOW CELL TOWERS WORK 2 (2011), http://www.unisonsite.com/pdf/resource-center/How%20Towers%20Work.pdf (describing that cell towers are essentially elevated antennas that transmit and receive radio frequencies generated by mobile devices and the wires running from the antenna to cellular carrier equipment contain the mobile device information and wireless signals).

62 *See* Owsley, *supra* note 61, at 5 (describing that another purpose of the cell towers is to collect information for billing purposes).

63 Robert M. Bloom & William T. Clark, *Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information and the Need for Fourth Amendment Protections*, 106 J. CRIM. L. & CRIMINOLOGY 167, 172 (2016).

more or fewer towers in a specific location.[64] Cell towers in America run on a radio access network that essentially comprises of the tower connecting to all mobile devices in its range, the mobile devices sending data transmissions to the antenna, and the antenna providing those transmissions to the service provider.[65]

While cell towers communicate with, and track all activities of, mobile devices, a system of satellites provides the devices with the ability to give users directions to destinations and tell them their precise location anywhere in the world.[66] The Global Positioning System (GPS) sends radio signals from satellites orbiting the Earth to GPS devices that use the signals to pinpoint the devices' locations on the Earth's surface.[67] This advanced system allows Americans to always know where they are in the world simply by enabling the GPS functions on their mobile devices, which will then continuously monitor the device's global position.[68]

Mobile devices, by communicating with cell towers and using GPS capabilities have the ability to be monitored and tracked by the government and cellular service providers.[69] Cell towers receive data communications about a device's activities, which are then stored in the service provider's records.[70]

---

64 *See* Timothy Stapleton, *The Electronic Communications Privacy Act and Cell Location Data: Is the Whole More than the Sum of Its Parts*, 73 BROOK. L. REV. 383, 386 (2007) (describing that the number of cell towers is determined by how densely populated an area is such as rural areas have less cell towers than cities); *see also* HARRIS, *supra* note 61, at 1–3 (describing that modern cell towers come in varying sizes depending on the range required, with the largest typically covering 10 miles and the smallest covering under 250 yards and are also more frequently being camouflaged to blend into the surrounding landscape so as not to be eyesores).

65 Justin Hill, *Digital Technology and Analog Law: Cellular Location Data, the Third-Party Doctrine, and the Law's Need to Evolve*, 51 U. RICH. L. REV. 773, 777 (2017); *see also* HARRIS, *supra* note 61, at 3–4 (describing that these technical specifications and radio frequency transmissions are what people know as 3G, 4G, LTE, and other speeds that their mobile devices use to function).

66 Owen Murphy, *Commonwealth v. Augustine: The Supreme Judicial Court's Misapplication of Jurisprudence to Technology*, 98 MASS. L. REV. 39, 41 (2017); *GPS Overview*, GPS.GOV, http://www.gps.gov/systems/gps/ (last visited May 24, 2018).

67 *See How GPS Works*, GPS.GOV, http://www.gps.gov/multimedia/poster/ (last visited May 24, 2018) (describing that once a GPS-enabled device receives the radio signal, it notes the exact time of arrival and uses that information to calculate the distance from the device to each of the system's orbiting satellites calculates its distance from at least four satellites using geometry to determine its exact location on Earth).

68 *GPS Overview*, *supra* note 66; How GPS Works, GPS.GOV, http://www.gps.gov/multimedia/poster/ (last visited May 24, 2018).

69 *E.g.*, Ann O'Neill, *Tsarnaev Trial: Timeline of the Bombings, Manhunt and Aftermath*, CNN (May 15, 2015, 3:43 PM), http://www.cnn.com/2015/03/04/us/tsarnaev-trial-timeline/index.html (describing that the police were able to track the device of the kidnapped student which helped to locate the path the brothers were on, and ultimately led to their demise); *The Problem with Mobile Phones*, SURVEILLANCE SELF-DEFENSE, https://ssd.eff.org/en/module/problem-mobile-phones (last visited May 24, 2018).

70 Shannon Jaeckel, *Cell Phone Location Tracking: Reforming the Standard to Reflect*

Such incredible access to information, and near constant availability of cell tower signals, gives Americans the ability to always have their mobile devices up and running; however, it also allows law enforcement to track suspects by way of those same devices, such as used by the Boston Police to find Dzhokhar Tsarnev.[71] Technology can be both a boon for societal interconnection and a drawback for personal privacy.[72]

D. Different Strategies to Mobile Device Location Data Tracking Protections

Courts and legislatures have fallen behind the technological advancement of society, and have thus been attempting to play catch-up in regulating and protecting citizens' rights to their technological data.[73] One approach relies on the judicial system to determine what rights citizens have in their mobile location data.[74] Another approach places upon legislatures the impetus to create laws and statutes that outline citizen rights in the information.[75] Yet another approach has no binding authority from the courts or legislatures regarding the level of protection citizens can expect.[76]

In the first strategy, case law has determined that no warrant is required for law enforcement to obtain location-tracking data from service providers.[77] Following the Sixth Circuit's ruling in *United States v. Skinner*, 690 F.3d 774 (6th Cir. 2012), this strategy allows police to obtain data and signals from mobile devices without requiring a warrant to perform any tracking.[78] Tracking location data in such a manner is more efficient and uses fewer resources than a massive

---

Modern Privacy Expectations, 77 LA. L. REV. 143, 144 (2016).

71 O'Neill, *supra* note 69 (describing how Boston police officers were able to track Tsarnaev through a phone call he made on a hostage's mobile device, ultimately leading them to his location and ending the manhunt).

72 *See* Jaeckel, *supra* note 70; O'Neill, *supra* note 69.

73 *Cell Phone Location Tracking Laws by State*, *supra* note 25.

74 Jaeckel, *supra* note 70, at 155.

75 United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015).

76 *See Cell Phone Location Tracking Laws by State*, *supra* note 25 (providing that some states have yet to pass laws regarding this issue).

77 *Id.*

78 United States v. Skinner, 690 F.3d 774, 777 (6th Cir. 2012) (reasoning that if a tool used to transport contraband gives off a signal, and that signal's location can be tracked, police can track the signal; the court analogizes that to hold otherwise would prevent dogs from being used to track fugitives); Catherine Crump, *Appeals Court Rules Fourth Amendment Does Not Protect Cell Phone Location Data*, ACLU (Aug. 15, 2012), https://www.aclu.org/blog/national-security/appeals-court-rules-fourth-amendment-does-not-protect-cell-phone-location (highlighting that jurisdictions allow law enforcement to achieve the same level of surveillance through GPS monitoring in minutes as would be achieved through physical tailing of a suspect for numerous days).

surveillance operation.[79] Allowing warrantless tracking of mobile device location data is the strategy with the largest group of jurisdictions to follow similar policies.[80]

A second approach advocates requiring a warrant for all location information tracking by law enforcement.[81] This approach provides the highest level of protection to citizens' location data through legislatively enacted laws.[82] One example is the California Senate enacting the Electronic Communications Privacy Act in 2015, partially to ensure that Californians were protected from intrusions by law enforcement into their mobile data.[83] To guarantee privacy interests are protected, this approach allows citizens who have been targeted inconsistent with the law to move to suppress data information or petition for the destruction of the information.[84] Requiring warrants for any location data tracking is the most common approach today, while the second most common approach concerns state legislatures enacting state statutes.[85]

Another strategy arose where state legislatures chose to enact laws in harmony with, or above, federal court jurisprudence. Virginia is such a state that has enacted its own legislation regarding the issue of location data tracking.[86] Following the Fourth Circuit's decision in *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016), Virginia amended its state laws to weaken the protections afforded to individuals' mobile data.[87] Virginia's enacted law requires service providers to disclose information to government entities whenever they obtain a warrant, subpoena, court order, or consent of the consumer; yet it also provides avenues for law enforcement to obtain mobile data without a warrant.[88] Using

---

79 Crump, *supra* note 78.

80 *See generally Cell Phone Location Tracking Laws by State*, *supra* note 25 (showing the jurisdictional differences in cell phone tracking laws).

81 Blain, *supra* note 14.

82 S.B. 178, 2015 Leg., Reg. Sess. (Cal. 2015).

83 Cal. Penal Code § 1546.1(a) (2017) (providing that the only ways government entities may compel production of electronic communication is through a warrant, wiretap order, electronic reader records order, or subpoena pursuant to established California law); S.B. 178, 2015 Leg., Reg. Sess. (Cal. 2015) (prohibiting government entities from compelling service providers to produce electronic communication information, as well as accessing electronic devices physically or electronically without a valid warrant).

84 Cal. Penal Code § 1546.4(a) (2017).

85 *See generally Cell Phone Location Tracking Laws by State*, *supra* note 25 (showing the jurisdictional differences in cell phone tracking laws).

86 VA. CODE § 19.2-70.3(E) (1-4) (2017) (providing that law enforcement may obtain real-time location data without a warrant in certain emergencies).

87 United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016) (holding the government did not violate the Fourth Amendment by obtaining location information from a service provider without a warrant); VA. CODE § 19.2-70.3(E) (1-4) (2017) (providing that law enforcement may obtain real-time location data without a warrant in certain emergencies).

88 VA. CODE § 19.2-70.3(E) (1-4) (2017) (providing a warrant exception for certain exigent circumstances).

this approach, jurisdictions have amended their laws to either comply with guidelines handed down by the circuit courts or to provide other distinctive protections.[89]

A contrary state-based approach advocates enacting laws that prohibit police from obtaining current or future location information relating to a suspected citizen without a warrant based on probable cause.[90] This approach allows law enforcement agencies to obtain such information in times of emergency, with the consent of the device's owner, or when available to the general public.[91] This approach offers a hybrid scheme of policies protecting real-time location data by requiring warrants for data seizure by law enforcement, yet also allows law enforcement to obtain that information under a specified set of circumstances without a warrant.[92]

A contrasting strategy proposes offering protections to citizens' location data through the discretion of judges.[93] An example of this strategy comes by way of the Third Circuit.[94] The Third Circuit limits instances in which a government entity may require service providers to disclose customers' data.[95] Even though there is some form of protection from law enforcement's compelling service providers to turn over information, no absolute protection exists since courts can easily choose to order disclosure without a warrant with a sufficient showing of government need.[96] However, there are built-in protections in place that make disclosure orders different from a normal warrant based on probable cause; namely, law enforcement must meet certain requirements to convince courts to

---

89 *Id.* (allowing police to obtain mobile data in certain situations without a warrant).

90 Freedom from Location Surveillance Act, 725 ILCS 168/1 (Ill. 2014).

91 VA. CODE § 19.2-70.3(E)(1-4) (2017) (permitting exceptions to the warrant requirement in specific emergencies); *see* Commonwealth v. Rushing, 71 A.3d 939, 962 (Pa. Super. Ct. 2013) (recognizing that under the Pennsylvania Constitution, citizens do have legitimate expectations of privacy in their real-time location data and that tracking allows police to locate people inside their private dwellings, where privacy expectations are at the highest).

92 Freedom from Location Surveillance Act, 725 ILCS 168/1 (Ill. 2014).

93 *Cell Phone Location Tracking Laws by State*, *supra* note 25 (showing the jurisdictional differences in cell phone tracking laws).

94 *In re* United States for an Order Directing a Provider of Elec. Commun. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010) (holding that the government, in order to compel production of citizens' cell site location information, has a lesser burden to prove than probable cause; however, courts have the discretion to require a warrant prior to ordering service providers to turn over information).

95 *Id.* at 306–07 (explaining the various statutory circumstances that permit law enforcement to obtain cell phone data without a warrant while also distinguishing between the data stored on the phone and data stored remotely that the phone may access).

96 *Id.* (reasoning that there is a contradiction in the statute because warrants require probable cause, but there is no such burden when seeking a court order for disclosure).

compel disclosure without obtaining a warrant.[97] This mix of protections and pro-law enforcement policies has only attracted a small number of jurisdictions.[98]

Finally, in an approach that might be described as a lack of a strategy, the only uniting characteristic is that the jurisdiction has enacted no binding authority and thus defaults to the majority rule of unprotected location data.[99] This approach simply follows the overall model that location data information from mobile devices is unprotected.[100] Until a concrete answer is given to the question of warrantless tracking of location data, jurisdictions will continue to adhere to the current model of allowing such tracking.[101]

The arguments presented above represent differing approaches for determining what degree of protection to afford location data.[102] With differing strategies on the correct application of the Fourth Amendment to this issue, resolution will come down to either states enacting their own laws[103] or federal courts uniting behind one common legal rule.[104] However, even the federal courts have reached an impasse between differing approaches and resolutions to mobile device location data protections.[105]

II. FEDERAL COURT JURISPRUDENCE AND DIFFERING OUTCOMES

There is no recognized consensus on how to approach protection for mobile-device location data.[106] With the lack of agreement, the next step is to turn to the federal court system to deliver a legal rule that unites the differing approaches, yet that has not been forthcoming either.[107] At the district court level, there is a

---

97 *Id.*

98 *See generally* Crump, *supra* note 78 (showing the jurisdictional differences in cell phone tracking laws).

99 *See generally id.* (showing the jurisdictional differences in cell phone tracking laws).

100 *See generally id.* (highlighting the differences in various state's approach to cell phone data privacy).

101 *See* Carpenter v. United States, 819 F.3d 880 (6th Cir. 2015), *cert. granted*, 85 U.S.L.W. 3567 (U.S. June 5, 2017) (No. 16–402).

102 *Compare* VA. CODE § 19.2-70.3(E) (1-4) (2017), *with* Freedom from Location Surveillance Act, 725 ILCS 168/1 (Ill. 2014), *and* CAL. PENAL CODE § 1546.1(a) (2017).

103 *Compare* VA. CODE § 19.2-70.3(E)(1-4) (2017), *with* Freedom from Location Surveillance Act, 725 ILCS 168/1 (Ill. 2014), *and* CAL. PENAL CODE § 1546.1(a) (2017).

104 *Compare* VA. CODE § 19.2-70.3(E) (1-4) (2017), *with* Freedom from Location Surveillance Act, 725 ILCS 168/1 (Ill. 2014), *and* CAL. PENAL CODE § 1546.1(a) (2017). *See supra* Section I.D; *infra* Part II.

105 *See* Carpenter, 819 F.3d at 884 (6th Cir. 2015), *cert. granted*, 85 U.S.L.W. 3567 (U.S. June 5, 2017) (No. 16–402).

106 *See generally* Crump, *supra* note 78 (illustrating the differences between various states' laws regarding warrantless cell phone tracking).

107 *Compare* United States v. Lambis, 197 F. Supp. 3d 608, 616 (S.D.N.Y. 2016) (holding that the third party doctrine did not apply to cellular signals intercepted by the

split between courts that favor protecting location information and courts that favor law enforcement conducting warrantless tracking.[108] Contrastingly, the circuit courts offer unified results.[109] However, even that unity is showing signs of cracking.[110]

A. Split District Court Decisions Further the Uncertainty Surrounding Location Data Rights

On the lower end of the federal courts, there is disagreement between supporting law enforcement's use of location data without obtaining a warrant and adamantly refusing to allow such data to be obtained without a warrant.[111] In *United States v. Ledbetter*, 2015 WL 7758930 (S.D. Ohio Dec. 2, 2015), the District Court for the Southern District of Ohio had to determine whether citizens are protected from having their mobile devices' records disclosed to police investigating certain crimes.[112] Upon analyzing the devices found in Ledbetter's vehicle, police issued subpoenas to obtain the devices' records from service providers in connection with multiple murder investigations.[113]

---

government), *with* United States v. Chavez, No. 3:14-cr-00185, 2016 WL 740246, at *1–2 (D. Conn. Feb. 24, 2016) (denying the defendant's motion to suppress cellular records obtained from via the third party doctrine), *and* United States v. Ledbetter, No. 2:15-CR-080, 2015 U.S. Dist. LEXIS 161693, at *41–42 (S.D. Ohio 2016) (holding the defendant lacked a reasonable expectation of privacy for cellular records in the possession of a third party), *and In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1023–24 (N.D. Cal. 2015) (holding that the large amount of data collected and stored of a customer's movement was within the reasonable expectation of privacy and in violation of the 4th Amendment).

108 *Compare* Lambis, 197 F. Supp. 3d at 616 (holding that the third-party doctrine did not apply to cellular signals intercepted by the government), *with* Ledbetter, No. 2:15-CR-080, 2015 U.S. Dist. LEXIS 161693, at *41–42 (holding the defendant lacked a reasonable expectation of privacy for cellular records in the possession of a third party).

109 *Compare* Chavez, No. 3:14-cr-00185, 2016 WL 740246, at *1–2, *with In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1023–24 (N.D. Cal. 2015).

110 United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (upholding the third-party doctrine and ruling that the defendant had no reasonable expectation of privacy for information given to a third party).

111 *Compare* Chavez, No. 3:14-cr-00185, 2016 WL 740246, at *1–2, *with In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d at 1023–24.

112 United States v. Ledbetter, No. 2:15-CR-080, 2015 WL 7758930, at *41–42 (S.D. Ohio Dec. 2, 2015) (describing an undercover police surveillance operation where upon initiation of police stop the defendant only yielded after roughly one-tenth of a mile giving probable cause to police to search and find $5,500 in cash, a small amount of marijuana, three grams of cocaine, eight grams of marijuana, a 9mm handgun, $51,302 in cash, and five mobile devices).

113 *See* United States v. Ledbetter, No. 2:15-CR-080, 2015 WL 7758930, at *1 (S.D.

Ultimately, the court held that Ledbetter lacked a reasonable expectation of privacy in the records on the mobile devices obtained by law enforcement.[114]

Agreement soon came from the District of Connecticut in *United States v. Chavez*, 2016 WL 740246 (D. Conn. Feb. 24, 2016).[115] In *Chavez*, the issue was whether a magistrate judge's order to compel Verizon to disclose Chavez's location data was an unconstitutional search and seizure.[116] The court found that there was no Fourth Amendment violation of the search and seizure principle because the third-party doctrine applied.[117] The third-party doctrine states persons do not have reasonable expectations of privacy in their phone conversations with others because the other party is free to reveal the contents of the conversation to police.[118] Applying the rule of law found in the third-party doctrine, the court held that it was irrelevant that a suspect disclosed information while in the privacy of the home and that disclosure reveals something the user said or did in the home.[119] The court also found no need to suppress the obtained information because there was no violation of the Fourth Amendment or the Stored Communication Act.[120]

A case on the opposite end of the protection spectrum is *In re Application for Telephone Information Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015).[121] The Northern District of California, like California in

---

Ohio Dec. 2, 2015) (challenging the subpoenas contending that without valid search warrants, "the police were not entitled to obtain those records because they might contain historical cell-site location information.").

114 United States v. Ledbetter, No. 2:15-CR-080, 2015 WL 7758930, at *1 (S.D. Ohio Dec. 2, 2015) (holding that suppression is not a remedy that is available for a violation of the Stored Communications Act, and for that additional reason his motions to suppress failed).

115 United States v. Chavez, No. 3:14-cr-00185, 2016 WL 740246, at *1 (D. Conn. Feb. 24, 2016).

116 *Id.* (stating that the government obtained Chavez's data records through a valid order because the reasons stated in the application were seen to satisfy probable cause).

117 United States v. Chavez, No. 3:14-cr-00185, 2016 WL 740246, at *2 (D. Conn. Feb. 24, 2016) (defining the third-party doctrine as, "a person does not have a right or interest that is protected under the Fourth Amendment to prevent the Government from obtaining information about a person that is in the custody of a third party and including information that the person has voluntarily disclosed to a third party.").

118 THOMPSON, *supra* note 11, at 7–9 (stating that when parties are invited to the conversation or accept the use of devices, any person who has the information or is party to that agreement may report to the authorities).

119 *See* Chavez, No. 3:14-cr-00185, 2016 WL 740246, at *1 (holding a customer's preferences or wishes are not a controlling consideration for determining whether information has been voluntarily given under the third-party doctrine).

120 *Id.* at *4.

121 *In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1040 (N.D. Cal. 2015).

general,[122] came down in favor of individual rights to location data.[123] The court gave a thorough analysis on mobile device information, often called "historical cell site location information" (CSLI).[124] CSLI includes the exact location of the service provider's tower that serves the mobile device's call, text, or data transfer.[125] With the precise nature of base stations, it is now possible to know a device's location to within a relatively small geolocation.[126] Analyzing the government's request for CSLI for a sixty-day retroactive period, the court found that mobile devices clearly qualify as "effects" under the Fourth Amendment.[127] Under that premise, the court ultimately held that individuals have an expectation of privacy in CSLI associated with their mobile devices.[128] Since the individual's privacy interest was reasonable and protected by society, the court ruled that the government must obtain a warrant for any CSLI data.[129]

Finally, mere months after *Chavez* was decided, the Southern District of New York held that to track location data a warrant must be received, with the scope

---

122 *See* DeMassa v. Nunez, 770 F.2d 1505, 1506 (9th Cir. 1989) (holding that an individual has a reasonable expectation of privacy against searches of their attorney's office under the Fourth Amendment).

123 *See In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d at 1013.
(holding that users' expectations of privacy in location information associated with cellular devices were reasonable).

124 *See id.* at 1013–14 (discussing how mobile device data is sent and received, and how it can be monitored by service providers and the government, and discussing that to facilitate better mobile device use, service providers maintain a network of radio base stations (cell towers) with varying coverage areas).

125 *See id.* at 1014 (stating how a special agent from the FBI informed the court that CSLI can be generated in the absence of any user interaction with the mobile device). Many modern devices have applications that continuously run in the background, generating a constant stream of incoming and outgoing data and additional testimony revealed that a mobile device that is turned on will "ping" the nearest cell tower every seven to nine minutes, and service providers keep track of CSLI generated in such fashion. *See id.*

126 *See id.* at 1015 (stating that at times the location can be so accurate that service providers can identify individual floors and rooms within buildings).

127 *See id.* at 1019 (citing the Fourth Amendment's guarantee of the right of the people to be secure in their persons, homes, papers, and effects against unreasonable searches and seizures).

128 *See In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1022–23 (N.D. Cal. 2015) (applying the following three principles: "(1) an individual's expectation of privacy is at its pinnacle when government surveillance intrudes on the home; (2) long-term electronic surveillance . . . implicates an individual's expectation of privacy; and (3) location data generated by cell phones . . . can reveal a wealth of private information about an individual.").

129 *See In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1023, 1040 (N.D. Cal. 2015) (finding that since CSLI, like GPS, can provide a comprehensive record of a person's movements and individual preferences, protection was warranted, and the government has to obtain a search warrant before compelling disclosure of CSLI and location information from service providers).

of the tracking limited to only those records specifically requested.[130] In *United States v. Lambis*, 197 F. Supp. 3d 606 (S.D.N.Y. 2016), the issue was whether the use of a cell-site simulator, a device that mimics cell tower frequencies, constituted an unreasonable search prohibited under the Fourth Amendment.[131] The court found that use of such a device was an unreasonable search because the forced "pings," a ping being each time a device connects to a cell tower,[132] constituted technology not available to the public.[133] Additionally, the simulator gave the DEA details of the home constituting a physical intrusion.[134] Ultimately, the court found that the "pings" picked up by the simulator were forced transmissions of electronic data identifying the phone's exact location until the DEA found the apartment.[135]

The district court decisions above show disagreement over the applicability of the third-party doctrine to location information tracking cases.[136] They also show disagreement over whether mobile devices and data information are protected.[137] Interestingly, the district courts siding with law enforcement are usually from jurisdictions in which the circuit court has ruled in favor of warrantless tracking, whereas courts not in those jurisdictions have held the opposite.

B. United States Circuit Court Opinions

Unlike the disagreement at the district court level, circuit courts currently agree that there is no constitutional requirement for law enforcement to obtain a warrant to gather location data from service providers.[138] In the first circuit

---

130 United States v. Lambis, 197 F. Supp. 3d 606, 611, 614 (S.D.N.Y. 2016).

131 *Id.* at 610 (distinguishing between CSLI and "ping" data by describing CSLI as the aggregate data that is obtained by cell towers, including general location, device usage, and numbers dialed while "pings" on the other hand are a means by which the police force the mobile device to emit a data signal to pinpoint location).

132 *Id.* at 609.

133 *Id.*

134 *Id.* at 610-11 (holding, in a direct divergence from its sister court in Connecticut, that without a search warrant, the government cannot turn citizens' mobile devices into tracking instruments).

135 *Id.* at 615–16 (holding the forced pings violate the Fourth Amendment's search protection because they are outside the normal operation of the mobile device).

136 *In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1023, 1040 (N.D. Cal. 2015); United States v. Chavez, No. 3:14-cr-00185, 2016 WL 740246, at *2 (D. Conn. Feb. 24, 2016).

137 United States v. Ledbetter, No. 2:15-CR-080, 2015 WL 7758930, at *1 (S.D. Ohio Dec. 2, 2015). *See generally In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1019–20 (N.D. Cal. 2015).

138 United States v. Skinner, 690 F.3d 772, 781 (6th Cir. 2012); United States v. Guerrero, 768 F.3d 351, 358–59 (5th Cir. 2014); United States v. Davis, 785 F.3d 498, 500 (11th Cir. 2015) (*en banc*).

decision on this issue, the Sixth Circuit had to determine whether the government's use of real-time location tracking of two phones belonging to the defendant constituted a violation of the Fourth Amendment.[139] The court stated that when criminals use modern technological devices to carry out criminal acts, they cannot complain when law enforcement uses those same devices to apprehend them.[140]

It held that when a tool being used to transport contraband gives off location data signals, the law does not prevent police from tracking those signals.[141] Similarly, there is no difference between physically trailing a suspect and tracking the suspect through technological means.[142] The government strengthened its case by obtaining multiple orders to compel the disclosure of GPS location information from Skinner's phones.[143] Ultimately, Skinner had no reasonable expectation of privacy in his location data and records suppression was not warranted.[144]

Two years after *Skinner*, the Fifth Circuit decided *United States v. Guerrero*, 768 F.3d 351 (5th Cir. 2014).[145] On the relevant CSLI and cell towers facts, the court focused on the third-party doctrine and the Stored Communications Act.[146]

---

139 *See* Skinner, 690 F.3d at 774–76 (showing how the communications between two phones belonging to the leader of the smuggling ring identified the defendant allowing law enforcement to obtain new orders to compel the phones' service provider to disclose subscriber information, CSLI, GPS real-time location, and "ping" data from the phones which in turn allowed law enforcement to track defendant's movements throughout Texas without any visual or physical surveillance).

140 *Id.* at 774 (reasoning that Skinner had no reasonable expectation of privacy in the data being transmitted from his mobile device).

141 *Id.* at 777 (reasoning that the law "cannot be that a criminal is entitled to rely on the expected untrackability [sic] of his tools.").

142 *See id.* at 778 (stating that law enforcement must be allowed to adapt its tactics to modern technology in order to prevent criminals from taking advantage of the criminal justice system).

143 *Id.* at 779.

144 *Id.* at 781 (reasoning that no physical intrusion occurred because defendant obtained the mobile devices for the purpose of communication, and GPS capabilities are included in a phone's function and elaborating that since authorities tracked a known cellular number, which was voluntarily used during travel on public roads, the GPS location information was public knowledge).

145 United States v. Guerrero, 768 F.3d 351, 355 (5th Cir. 2014) (describing how CSLI was introduced at trial regarding five phone calls made on the afternoon of a murder, and the location information was used by law enforcement to put defendant at the scene of the crime).

146 *See id.* at 358 (reasoning that data revealing the cell tower and sector to which the mobile device sent its signals was only available from third-party service providers). The SCA requires service providers to maintain records of transmissions and communications made by devices on their networks and prohibits the government from obtaining that information without following certain procedures outlined in statute. *Id.*

It found the government in violation of the procedures outlined in the SCA,[147] yet determined that suppressing the information was not appropriate; for suppression to be granted, Guerrero would need to show the CSLI was obtained in violation of the Fourth Amendment.[148]

With regard to the Fourth Amendment, the court restated that mobile-device users voluntarily convey information to service providers, knowing that the service providers record location information.[149] Since users have implied recognition that their information is recorded to the same extent that landline users understand numbers dialed are recorded, the court held that expectations of privacy were unreasonable.[150] Accordingly, the Fifth Circuit determined there was no Fourth Amendment violation and no reason to suppress the CSLI.[151]

Shortly after *Guerrero*, the Eleventh Circuit heard the case of *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015), and was faced with the question of whether a court order authorized by the SCA to compel production of records pertaining to CSLI violated Davis's Fourth Amendment rights.[152] The court relied on the third-party doctrine and an unreasonable belief in the right to location information privacy to deny the motion to suppress CSLI records.[153] It found that the cell tower records and CSLI belonged to MetroPCS, were stored in electronic form in MetroPCS servers, and were stored by it as a third-party, thereby preventing Davis from having any interest in the records' ownership.[154] Therefore, the court held the government obtained a valid court order to compel production of the service provider's records and even if production constituted a search, obtaining records without a warrant was reasonable.[155]

These circuits have been the battleground for challenges to police use of location data obtained by means of warrantless compulsion of service providers to disclose records.[156] They are a small, but united, portion of the federal circuit

---

147 *Id.*

148 *Id.*

149 *Id.*

150 *Id.*

151 *See id.* (explaining the court's determination for not requiring the grant of a motion to suppress because the government's violation of the Stored Communications Act did not amount to a Fourth Amendment violation).

152 *See* United States v. Davis, 785 F.3d 498, 500, 502 (11th Cir. 2015) (explaining a case where the government produced telephone records obtained through court order from MetroPCS, showing all the information from cellphone towers those calls were "pinged" off).

153 *See id.* at 511 (reasoning that Davis could not assert ownership or possession over the business records sought to be suppressed).

154 *See id.* (holding that Davis had no reasonable expectation of privacy in the business records because users are aware that their phones do not work when they are outside the service provider's cell tower network).

155 *Id.* at 509.

156 *Id.* at 502; United States v. Guerrero, 768 F.3d 351, 358 (5th Cir. 2014) (explaining a

courts. However, no circuit to rule on this issue controls a jurisdiction in which a district court has ruled in favor of a user's right to location data.[157]

C. The Fourth Circuit Anomaly

In an interesting twist of jurisprudence, the Fourth Circuit became the first federal court of appeals to rule in favor of a citizen's right to privacy in location data.[158] However, in an *en banc* rehearing it promptly reversed the earlier decision in favor of the individual.[159] This case offers an analysis of how undecided circuits may come to disagree with their sister circuits in the future based on individual cases' fact patterns.

The facts presented to the Fourth Circuit in the two *Graham* cases remained the same.[160] Aaron Graham and Eric Jordan were implicated in a string of robberies perpetrated in Baltimore County, Maryland and police obtained warrants for items found on the men or in their residences.[161] However, the government only obtained warrants for the physical mobile devices, and later sought to compel the devices' service providers to disclose CSLI pertaining to text messages and call records.[162] The Fourth Circuit determined that the government's obtaining the CSLI was an unreasonable search in violation of the Fourth Amendment.[163] It reasoned that users of mobile devices have an objectively reasonable expectation of privacy in the information their devices transmit.[164] Yet the ruling was not a complete win for mobile device users because the court affirmed the district court's denial of the defendants' motions to suppress because the government acted in good faith in obtaining the

---

scenario where the acquirement of information without a search warrant does not violate Fourth Amendment rights); United States v. Skinner, 690 F.3d 772, 775 (6th Cir. 2012).

157 Davis, 785 F.3d at 500, 502; Guerrero, 768 F.3d at 358; Skinner, 690 F.3d at 775.

158 *See* United States v. Graham, 796 F.3d 332, 349 (4th Cir. 2015) (recognizing the court's own originality in Fourth Amendment privacy).

159 Graham, 824 F.3d at 424.

160 Graham, 796 F.3d at 342; *see also* Graham, 824 F.3d at 424 (showing similar holdings that were consistent to the two *Graham* cases).

161 *See* Graham, 796 F.3d at 338.

162 *See id.* at 341 (explaining how the government sought two court orders for disclosure of CSLI relating to calls and text messages for a 221-day span even after wireless services' initial denials).

163 *Id.* at 343–45 (reasoning that absent subscriber notice and consent, the government must secure a warrant or court order for the individual's records after defining search "within the meaning of the Fourth Amendment occurs where the government invades a matter in which a person has an expectation of privacy that society is willing to recognize as reasonable.").

164 *See id.* at 345 (holding that inspection of such information by the government requires a warrant unless one of the few established exceptions to the warrant requirement apply).

information.[165]

Upon an *en banc* rehearing, the entire panel of the Fourth Circuit held that the government did not violate the Fourth Amendment by obtaining CSLI from mobile devices without a warrant.[166] Unlike the earlier decision, the *en banc* panel determined that the third-party doctrine applied to this case.[167] Under the third-party doctrine, the court reasoned that the defendants had no legitimate expectation of privacy to information voluntarily turned over to a third party.[168]

The now-united stance of circuits, compared to the disagreeing stance of district courts, shows that the debate over whether law enforcement may obtain location data without a warrant should be settled by the Supreme Court.[169] Clearer guidance from the Supreme Court would bring a sense of finality to the issue, or at least allow for a more uniform application of law. However, achieving a bright-line ruling from the Court may prove to be more challenging than expected.[170]

III. CLOSE, BUT NOT EXACT: PAST SUPREME COURT CASES DEALING WITH GPS TRACKING AND USE OF PHONE CONTENTS

The United States Supreme Court has not directly addressed the issue of mobile device location data.[171] However, the Court has taken cases dealing with major surveillance and technological issues in the past.[172] Since its first landmark technology surveillance decision in 1979,[173] the Supreme Court has slowly waded through the uncharted waters of modern technology, privacy expectations, and police's responses to technological advances.[174]

---

165 *See id.* at 362 (finding that the government relied on the Stored Communications Act and two court orders in obtaining the CSLI from service providers and recognizing that citizens have an inherently reasonable expectation to the privacy of their mobile communications, but that the government can overcome that expectation if it relies in good faith on statutes or court orders).

166 *See* United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016).

167 *See id.* at 425 (holding that the third-party doctrine applies even when the information is revealed to a third party "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

168 *See id.* (showing that since the government acquired the records from the service providers in the normal course of business, and did not view, listen to, record, or engage in direct surveillance of defendants to obtain the information, there was no constitutional violation).

169 *Id.*

170 *See infra* Part III.

171 *See infra* Sections III.A-E.

172 *See infra* Sections III.A-E.

173 *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 745–46 (1979) ("The installation and use of a pen register, consequently, was not a 'search,' and no warrant was required.").

174 *See also* Arizona v. Hicks, 480 U.S. 321, 323 (1987) (holding that a mere recording of serial numbers of stereo equipment in plain view does not constitute a "seizure"); City of

A. *Smith v. Maryland*: Acceptable Surveillance when Risk is Assumed

The first landmark decision by the United States Supreme Court came in *Smith v. Maryland*, 442 U.S. 735 (1979).[175] This case set the tone that surveillance is acceptable, especially when the person assumes the risk that information could be given to police.[176] The facts of *Smith* are simple; a man driving a 1975 Monte Carlo robbed Patricia McDonough in Baltimore, Maryland and shortly after, McDonough began receiving phone calls from the robber and one day saw the Monte Carlo slowly driving past her front porch.[177] Police had the telephone company install a pen register at its office to monitor the calls being dialed from Smith's phone.[178] After installing the pen register, without a warrant, police learned that Smith dialed McDonough's home phone on several occasions.[179]

The Supreme Court stated that application of the Fourth Amendment depended upon whether an individual could claim a justifiable, reasonable, or legitimate expectation of privacy that had been invaded by government action.[180] The Court found that with the pen register installed on telephone company property, Smith had no claim that his property was invaded.[181]Additionally, Smith had no expectation of privacy in the numbers dialed from his home phone.[182]

The Court stated that even if individuals expect some level of privacy in the

---

Ontario v. Quon, 560 U.S. 746, 764–65 (2010); United States v. Jones, 565 U.S. 945, 948 (2010); Riley v. California, 134 S. Ct. 2473, 2486 (2014).

175 *See* Smith, 442 U.S. at 745–46 (holding the use of a pen register by a telephone company does not constitute a "search" within the meaning of the Fourth Amendment).

176 *See id.* at 745; *see also* LaChance, *supra* note 8.

177 Smith, 442 U.S. at 737 (describing a scenario where police found a man matching the description given to them by McDonough in her general neighborhood, who was driving a 1975 Monte Carlo).

178 *Id.* at 736 (explaining a pen register is a mechanical device that records the numbers dialed on a telephone; it does not record conversations or completed calls, only the numbers dialed into the phone).

179 *Id.* at 740 (explaining a scene where the police then received a warrant to search Smith's home, which revealed a telephone book with McDonough's page folded downwards).

180 *Id.* at 740 (presenting the new analysis into two questions: first, whether the individual has shown he sought to preserve something as private, and second, whether the individual's expectation of privacy was justifiable under the circumstances).

181 *Id.* at 741 (reasoning that the pen register differed from a listening device, because pen registers cannot record contents of communications per court findings in previous cases; pen registers "disclose only the telephone numbers that have been dialed . . . Neither the purport of any communication between the caller and the recipient of the call . . . is disclosed by pen registers.").

182 *Id.* at 742 (reasoning that all telephone users realize they must give phone numbers to the telephone company to complete the desired call).

numbers they dial, society is not prepared to recognize such expectations as reasonable.[183] Even with some expectation of privacy, it is not legitimate and does not satisfy the test for a "search."[184] This early landmark decision paved the way for future Supreme Court cases dealing with surveillance.[185]

B. *Arizona v. Hicks*: Seizing an Object Must Be Based on a Standard Similar to that of a Warrant

Eight years after *Smith*, the Court weighed the interests of the public against the individual's expectations of privacy, with a heavy emphasis on not depriving citizens of their liberty from unreasonable government searches.[186] *Arizona v. Hicks*, 480 U.S. 321 (1987) did not involve the use of mobile devices, but it has been instrumental in formulating the Supreme Court's Fourth Amendment jurisprudence in the almost thirty years since it was handed down.[187] Justice Antonin Scalia presented an analytical and thorough dissection of the case in accord with the Fourth Amendment.[188] Justice Scalia stated that taking action unrelated to the objectives of the authorized entry into the apartment, which revealed new portions of the apartment's contents, produced a new invasion of privacy unjustified by the original circumstances validating the entry.[189]

Turning to the reasonableness of the search, the Court bluntly stated there would be no doubt the search would be covered under the "plain view" doctrine if the officers had probable cause to believe that the equipment was stolen.[190] Yet, a lack of probable cause turned this into a case of first impression for the Court.[191] Ultimately, it held that probable cause is required, thereby requiring a standard as high as that of obtaining a warrant.[192] The Court made sure to

---

183 *Id.* at 743–44 (arguing that because society was not willing to recognize this privacy right, there is a presumption against its reasonableness; therefore, Smith assumed the risk that the telephone company would reveal to police any numbers he dialed).

184 *Id.* at 745–46.

185 Katz v. United States, 389 U.S. 347, 353 (1967).

186 *See* Arizona v. Hicks, 480 U.S. 321, 329 (1987) (holding that there is nothing new in the realization that the Constitution may sometimes insulate the criminal acts of a few to protect the privacy interests of the majority).

187 LaChance, *supra* note 8.

188 *See, e.g.*, Hicks, 480 U.S. at 323–25.

189 *See, e.g.*, *id.* at 325 ("A search is a search, even if it happens to disclose nothing but the bottom of a turntable.").

190 *See, e.g.*, *id.* at 323–25 (explaining that the State conceded that the officers involved in the entry of the apartment had only a reasonable suspicion, meaning that it was less than probable cause).

191 *See, e.g.*, *id.* (arguing that the Court had never ruled on the question of whether probable cause is required to invoke the "plain view" doctrine; in fact, earlier Court decisions had explicitly mentioned that the issue was unresolved).

192 *See, e.g.*, *id.* at 326 (highlighting that dispensing of the need for police to obtain a warrant is not the same as settling for a lesser standard than a warrant would require).

reinforce the point that just because an object can be seized without a warrant does not mean that it may be seized without probable cause, the same standard for obtaining court-authorized warrants.[193]

C. *City of Ontario v. Quon*: Work-Related Mobile Devices and Diminished Privacy Expectations

Following a lull in location-tracking jurisprudence, the Supreme Court decided *City of Ontario v. Quon*, 560 U.S. 746 (2010).[194] *Quon* focused on whether an employer has the right in certain circumstances to read the text messages sent and received from company-owned mobile devices.[195] Jeff Quon, a SWAT team member for the City of Ontario, California, was issued a pager capable of sending and receiving text messages.[196] With officers exceeding imposed limits, the police looked into whether officers were using the devices for non-work-related purposes.[197]

The Supreme Court had to determine whether an unreasonable search under the Fourth Amendment occurred, and importantly, whether individuals have a reasonable privacy interest in their mobile device data.[198] It found that the police department made clear from the beginning that the mobile devices were not considered private, their messages were subject to audits, and they were to be used solely for work-related purposes.[199] Yet, Justice Kennedy's opinion advocated caution and refrained from issuing a sweeping decision.[200] Accordingly, such decisions must be made in light of the expectation of privacy

---

193 *See, e.g.*, *id.* at 323–25 (reasoning that the mere fact that an object came within an officer's plain view does not, by itself, do away with the requirement of probable cause or a warrant).

194 City of Ontario v. Quon, 560 U.S. 746, 750 (2010).

195 *Id.*

196 *See id.* at 751 (demonstrating how the Ontario Police Department held a meeting where it was explained that the messages sent on the pages were considered e-mail and were eligible for auditing by the City).

197 *See id.* at 752 (showing that due to Quon's excessive overage each month, the police department asked Arch Wireless to provide it with transcripts of his messages sent and received).

198 *See id.* at 766–67 (holding that the police did not violate the Fourth Amendment because the audit was ordered to determine the result of the character limits while determining that the search was not reasonable in its scope, and that there were other means to go about the search that were less intrusive).

199 *Id.*

200 *See id.* at 759 ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear" because "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.").

society places upon the use of such technology and, as of *Quon*, there was no satisfactory gauge of society's attitude to issue a broad opinion.[201]

The Court found that Quon did have a reasonable, but minimal, expectation of privacy in his text messages.[202] As a police officer, he should have known his actions and work-related communications were subject to scrutiny.[203] In determining the reasonableness of the search, the Court stated that even though warrantless searches are *per se* unreasonable, specifically established exceptions exist.[204] Ultimately, the search was found to be motivated by legitimate work-related purposes, limited in scope, and reasonable under precedent, thereby making it constitutional.[205] This decision was one of the last significant developments in mobile device surveillance that did not deal with GPS and location-specific tracking of enabled smart devices.[206]

D. *United States v. Jones*: Tracking of Citizens' Vehicles by Means of GPS is a No-Go

Delving deeper into technology and the GPS capabilities of modern devices, the Court issued a landmark ruling in 2012 that protected individuals' rights to privacy of their vehicles and against searches.[207] *United States v. Jones*, 565 U.S. 400 (2010), is a rare unanimous opinion for a major issue case.[208] It marks the first time that the Court ruled against the government and police on a major tracking decision.[209] Antoine Jones owned a nightclub and was under

---

201 *See id.* at 758–60 (opining how it was not known whether society expressed a greater expectation of privacy because of self-identification and ubiquity of mobile device usage, or whether the devices had become so mainstream that employees could purchase their own if they did not want their employers to search the content).

202 *See id.* at 760 (highlighting that while Quon may have had a reasonable expectation of privacy in the text messages, the police department did not necessarily violate his Fourth Amendment rights by obtaining and reviewing the records).

203 *See id.* at 760 (holding that even if Quon could assume some level of privacy, it was not reasonable to believe that the text messages were immune from scrutiny under all circumstances).

204 *See id.* (describing one such exception is the "special needs" of the workplace to justify employers searching company-owned devices).

205 *See generally* Suuberg, *supra* note 12 (noting that for over two decades of decisions, only 20% of Supreme Court opinions on criminal procedure matters have individual rights trumping government interests and expressing that needs for law enforcement appears to persuade the Court more than any other governmental interest).

206 *City of Ontario v. Quon*, EPIC.ORG, https://epic.org/privacy/quon/ (last visited May 24, 2018) (outlining the case as one of workers' employment privacy rights, not necessarily one of electronic rights in location).

207 *See* United States v. Jones, 565 U.S. 400, 412 (2012) (ruling that individuals have a reasonable expectation in privacy in vehicles).

208 *See generally id.*

209 *See id.* (deciding whether attaching a GPS device to a citizen's vehicle and subsequently using the device to monitor the vehicle's movements constituted a search).

investigation by the FBI and District of Columbia Police for trafficking narcotics.[210] The police obtained a warrant to install a GPS device on Jones's car within ten days and within the District of Columbia.[211] However, the police did not install the device until the eleventh day, and it was installed in Maryland.[212]

Using the device attached to Jones's car, the government was able to record his movements to within fifty feet, all of which was relayed to government computers.[213] On appeal of his conviction, the Court of Appeals for the D.C. Circuit reversed the conviction, holding that the admission of evidence obtained through warrantless use of GPS tracking violated the Fourth Amendment.[214] The Supreme Court, after granting certiorari, found that the government physically occupied private property for the sole purpose of obtaining information, which would have been considered a search under the Fourth Amendment when it was originally adopted.[215] The Supreme Court affirmed the ruling of the D.C. Circuit in favor of Jones because the warrantless encroachment on property was unreasonable and unconstitutional.[216] *Jones*, and the Court's decision in *Riley v. California*, 134 S. Ct. 2473 (2014), are the basis for much of the current debate on location data tracking and whether police need to obtain warrants for such information.

E. *Riley v. California*: Mobile Devices Are Much More than Mere Wireless Telephones

The most recent decision on warrantless location data tracking struck a blow

---

[210] *See id.* at 402 (describing how the joint task force employed different techniques to watch Jones, including visual surveillance, installing cameras to watch the nightclub, and adding a pen register and wiretap on Jones's cell phone).

[211] Jones, 565 U.S. at 402–03.

[212] *See id.* (2012) (explaining how the government tracked the car of the defendant for the twenty-eight days, and the ensuing information produced over 2,000 pages of data).

[213] *See id.* at 403–04 (demonstrating that during Jones's first trial, the district court granted a suppression motion for the data relating to the times the vehicle was at Jones's residence and parked in his garage but admitted all data as to when the vehicle was traveling on public roads while during a second trial, the government admitted the entirety of the tracking data, and a guilty conviction was rendered, placing Jones in prison for life).

[214] *Id.*

[215] *See id.* at 408 (reasoning that the text of the Fourth Amendment reflects a close connection to property, defining a reasonable expectation of privacy as, "an expectation 'that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.'").

[216] *See id.* at 412 (finding that the attachment of GPS tracking devices to vehicles, and the subsequent tracking of the vehicle's movements, constituted an unconstitutional search under the Fourth Amendment).

to law enforcement and gave a win to privacy advocates.[217] *Riley v. California* revolved around the traffic stop of David Riley and culminated in the seizure of his mobile-device.[218] The issue arose from the officer's actions at the scene of the arrest, and later at the police station, of accessing information on Riley's phone without a warrant.[219] With the information, Riley was convicted of firing into an occupied vehicle, assault with a semiautomatic firearm, and attempted murder, which carried enhanced penalties of fifteen years to life in prison.[220]

Chief Justice Roberts wrote the opinion of the Court, in which seven Justices joined, and one Justice entered a concurring opinion.[221] Chief Justice Roberts began by stating that, "[o]ur cases have determined that '[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant.'"[222] That reiteration of clearly established law was followed by the mandate that in the absence of a warrant, searches are only reasonable if they fall within one of the specifically recognized exceptions to the warrant requirement.[223] The question that the Court sought to resolve was whether the search incident to arrest doctrine applies to information stored on modern mobile devices.[224] Noting that there was little guidance from earlier Court jurisprudence, the standard for determining whether to exempt a search from the warrant requirement lies in a balancing test.[225]

---

217 Riley v. California, 134 S. Ct. 2473, 2494 (2014); LaChance, *supra* note 8. 02/29/468609371/at-supreme-court-debate-over-phone-privacy-has-a-long-history (citing Jones and Riley as the latest in succession of cases on expectation of privacy).

218 *See, e.g.*, Riley, 134 S. Ct. at 2480 (holding that an individual has a reasonable expectation of privacy in a mobile phone).

219 *See, e.g.*, *id.* at 2480–81 (describing how the officers at the scene accessed information on the device that identified other members of the "Bloods" gang, contact lists, and text messages when a detective who specialized in gangs explicitly examined files that "caught his eye" such as videos, photographs, and messages relating to possible gang activity).

220 *Id.*

221 *Id.* at 2481.

222 *See, e.g.*, *id.* at 2482.

223 *Id.* at 2494; *see* United States v. Robinson, 414 U.S. 218, 236 (1973) (holding that a suspect arrested for driving with a revoked license could be searched incident to arrest); Evans v. Solomon, 681 F. Supp. 2d 233, 248-49 (E.D.N.Y. 2010) (holding that a search of a suspect stopped for a traffic violation was legitimate because probable cause to arrest existed at the time of the search and the search was valid as a search incident to arrest); *see also* Drew Liming, *Calling for a Standard: Why Courts Should Apply a New Balancing Test in Cell Phone Searches Incident to Arrest*, 51 AM. CRIM. L. REV. 715, 729 (2014) (discussing officer's search of your cell phone would frequently be permitted under the search incident to arrest exception to the warrant requirement of the Fourth Amendment).

224 *See, e.g.*, Riley, 134 S. Ct. at 2484 (noting the Court made the point that modern mobile devices are a pervasive and insistent part of Americans' daily lives).

225 *See, e.g.*, *Riley*, 134 S. Ct. at 2484 (noting the balancing test employed assesses "on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other,

After a lengthy consideration of the balance between individual privacy interests and the government's interest in protecting society, the Court held that officers must generally secure a warrant before conducting a search like in *Riley*.[226] In regards to the search incident to arrest exception, the Chief Justice Roberts recognized its validity and that it rests both on the heightened governmental interests at stake as well as on the arrestee's reduced privacy interests once in custody.[227] However, with the advent of modern mobile devices such as cell phones, privacy concerns implicated are far beyond those of the traditional wallet, cigarette pack, or purse.[228]

The opinion then moved on to a general description of the difference between mobile devices and traditional objects normally kept on an arrested person's body.[229] Many cell phones are in fact minicomputers, cameras, video players, calendars, recorders, libraries, and maps.[230] Additionally, storage capabilities of modern mobile devices have several important consequences for individual's privacy interests.[231] Like previous courts, the Supreme Court touched on CSLI, but to a much different effect. It recognized that CSLI is a standard feature on modern mobile devices, often able to track a person's movements down to specific locations and the exact time data was collected, all of which warrant some level of privacy protection.[232] Consequently, the Court explained that a search of a mobile device in today's age reveals much more to the government than a traditional search of a house because the device contains the digital form

---

the degree to which it is needed for the promotion of legitimate governmental interests.").

226 *See, e.g.*, *id.* at 2493; *cf.* Liming, *supra* note 223, at 729 (contending that balancing tests weigh legitimate interests of both law enforcement and suspected citizens; additionally, bright-line rules do not give courts enough flexibility to respond to new developments in technology).

227 *See, e.g.*, Riley, 134 S. Ct. at 2488 (reiterating that law enforcement officers are still free to examine the physical aspects of a phone in order to ensure that it cannot be used as a weapon, yet the interest of protecting officers from harmful objects does not justify dispensing with the warrant requirement in totality).

228 *See, e.g.*, *id.* at 2488–89 (stressing that while searches of arrested persons' pockets for physical items implicate privacy interests, it is not coextensive to that of digital data).

229 *See, e.g.*, *id.* at 2489.

230 *See, e.g.*, *id.*

231 *See, e.g.*, *id.* at 2489–90 (illustrating that (1) mobile devices collect many distinct types of information in one place that reveals much more than any isolated record, such as addresses, notes, prescriptions, bank statements, and videos; (2) the devices' capacities allow one piece of information to convey far more than previous devices were capable of, through photographs with dates, locations, and descriptions; and (3) data on devices can date to the purchase of the device, which could potentially include months' worth of data on one conversation, and fourth, unlike physical records, mobile devices have an element of pervasiveness that makes it possible to carry on one's person a cache of sensitive personal information on a daily basis).

232 *See, e.g.*, *id.* at 2490 (citing United States v. Jones, 565 U.S. 400, 414 (2012)).

of sensitive records that would be found in a home, as well as private information that is never kept in a home.[233]

The Court recognized that the data stored on these devices can contain incriminating information regardless of when the crime occurred.[234] Additionally, call logs on mobile devices can include information that identifies other individuals or special names that the owner might give to loved ones.[235] Finally, the Court admitted its decision will undoubtedly impact the ability of law enforcement to combat crime, yet it rationalizes that consequence by the fact that privacy comes at a cost.[236] In its final ruling, the Court made sure to state that mobile device data is not always immune, only that warrants are generally required for police to obtain the information contained in these devices.[237] From such a lengthy and detailed analysis of mobile-device usage and data information contained therein, the Court came to a rather simple holding: when police seize a mobile-device *incident to arrest*, they must obtain a warrant before searching the device.[238]

Background material and legal jurisprudence show that strong opinions by district courts on both sides of the issue exist.[239] Circuit courts have formed a united front on the pro-law enforcement side.[240] Even Supreme Court case law

---

233 *See, e.g.*, *id.* at 2491 (distinguishing between data that is stored on the device itself and data which is stored in remote servers such as "cloud computing" and service provider servers).

234 *See, e.g.*, *id.* at 2492 (reasoning that devices will contain location data or texting data that is indicative of past crimes or illegal acts that were never contemplated by police when performing a simple traffic stop or citation).

235 *See, e.g.*, *id.* at 2493.

236 *See id.* at 2493–94 (noting Chief Justice Roberts discussion on how mobile devices have become important tools in the coordination of criminal enterprises and can provide incriminating information about criminals to police and about how these devices are so pervasive in society that to allow for their search without a warrant or an exception to the warrant requirement would subject the vast majority of innocent citizens to unconstitutional searches).

237 *See, e.g.*, *id.* at 2493.

238 *See, e.g.*, *id.* at 2495.

239 United States v. Ledbetter, No. 2:15-CR-080, 2015 WL 7758930, at *1 (S.D. Ohio Dec. 2, 2015) (discussing the motion to suppress all evidence seized as a result of a traffic stop on December 18, 2007, as well as various cell phone records obtained without search warrants); United States v. Lambis, 197 F. Supp. 3d 608, 610 (S.D.N.Y. 2016) (discussing the DEA's use of the cell-site simulator to locate Lambis's apartment was an unreasonable search); *In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1013, 1026 (N.D. Cal. 2015) (concluding that cell phone users have an expectation of privacy in the historical CSLI associated with their cell phones, and that society is prepared to recognize that expectation as objectively reasonable); United States v. Chavez, No. 3:14-cr-00185, 2016 WL 740246, at *2 (D. Conn. Feb. 24, 2016) (concluding that the Government's acquisition of this information was neither a "search" nor "seizure" that is subject to the requirements of the Fourth).

240 *See, e.g.*, United States v. Guerrero, 768 F.3d 353, 358 (5th Cir. 2014); United States v. Skinner, 690 F.3d 774, 777 (6th Cir. 2012); United States v. Davis, 785 F.3d 500, 518

does not set a clear precedent to follow.[241] With such opinions on whether law enforcement can compel mobile device location data to be turned over without a warrant, the Court must settle the dispute with a clear, precedential decision.

IV. WARRANTLESS USE OF MOBILE LOCATION TRACKING DATA IS A SEARCH . . . SOMETIMES: CREATING AN EXCEPTION TO THE WARRANT REQUIREMENT THROUGH AN ADAPTED TEST

With all of the differing approaches taken by states, federal courts, and the Supreme Court, it seems nearly impossible to reconcile the differences in order to make one coherent legal policy.[242] The proposed solution is to do away with the competing court rulings and implement a balancing test that will combine Supreme Court precedent with concepts from the differing lower court rulings.[243] This solution is necessitated by the fact that warrantless use of mobile location data to track suspects by law enforcement can be constitutional under certain circumstances, but may be highly unconstitutional under others.[244]

A. Location Data Taken Without a Warrant Are, and Are Not, Searches Depending on Each Case

In the evolving world of technology, Americans are immersing themselves to greater depths in mobile devices and their associated risks.[245] Due to the increase in mobile device use, law enforcement has adapted tracking methods to incorporate the data emanated from those devices.[246] However, the combination

---

(11th Cir. 2015); United States v. Graham, 824 F.3d 424, 438 (4th Cir. 2016).

241 Dolan, Lennon & Munoz, *supra* note 9, at 40–41 (discussing the history of relevant precedents set by the Supreme Court).

242 *See* Lauren E. Babst, *No More Shortcuts: Protect Cell Site Location Data with a Warrant Requirement*, 21 MICH. TELECOMM. & TECH. L. REV. 363, 383 (2015) (discussing the different conclusions reached throughout the United States federal jurisdiction).

243 *See* Oliver v. United States, 466 U.S. 170, 178 (1984) (discussing the different factors, courts have given weight to including the uses to which a person has put a location).

244 *See* United States v. Jones, 565 U.S. 400, 430–31 (2012) (noting that the court need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4–week mark).

245 *See* Smith, *supra* note 23 (noting that over 68% of American adults now own smartphones); James M. Lucas, *The Fourth Amendment - Are Mobile Phones Now Governmental Tracking Devices*, 67 S.M.U. L. REV. 211, 216 (2014) (noting in 1986, there were only 340,213 mobile phone subscribers in the United States and there were approximately 315 million mobile phone subscribers in 2011).

246 Dolan, Lennon & Munoz, *supra* note 9, at 41 (stating that wireless technology has become a powerful tool in criminal investigation and prosecution as well as law enforcement); Babst, *supra* note 242, at 383 (quoting Justice Sotomayor's concern about protecting location information, as she questioned the "appropriateness of entrusting to the

of mobile device use and law enforcement location data tracking creates serious concerns as to the amount of personal information being turned over to police, coupled with many suspects being tracked without a warrant.[247]

1. Competing Strategies, Federal Court Rulings, and Supreme Court Jurisprudence

Courts across the United States have been unable to agree on what kind of protection to give citizens, if any protection at all, in their mobile location data.[248] Courts that follow the *Skinner* line of reasoning base protections on the fact that federal courts have determined no warrant is necessary for police to obtain location tracking data.[249] Other courts follow California's stance that a warrant is necessary for law enforcement to obtain any location data information from service providers, a stance that is often achieved through state legislation.[250] Yet others have put citizens and law enforcement in the position of protecting privacy interests in some cases and not protecting those interests in other cases.[251] With no clear consensus among lower courts, it would be logical to rely on the higher federal courts to sort out the matter because of their jurisdictional authority.

However, higher federal courts have been no better at dealing with the problem. District courts have refused to follow circuit court rulings unless they

---

Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercise of police power to [sic] and prevent 'a too permeating police surveillance.'").

247 *See* Dolan, Lennon & Munoz, *supra* note 9, at 41 (positing that the increased use of wireless technology as a law enforcement tool has lowered the barriers for acquiring any type of personal information from individuals' devices); Babst, *supra* note 242, at 380 (discussing that in order to properly analyze the scope of the privacy interests at stake, courts must account for the fact that modern technology can store vastly greater amounts of data and disclose much more revealing personal information than past technology); *cf.* Riley v. California, 134 S. Ct. 2473, 2491 (2014).

248 *See* Babst, *supra* note 242, at 383 (discussing the choices courts face when deciding whether to follow Supreme Court Fourth Amendment precedent from an era before modern cell phones, or instead consider what legal standards should apply in light of the dramatic changes in technology).

249 *See* United States v. Skinner, 690 F.3d 774, 775 (6th Cir. 2012) (holding that individuals do not have reasonable expectations of privacy in location data); Carpenter v. United States, 819 F.3d 880, 895 (6th Cir. 2015), *cert. granted*, 85 U.S.L.W. 3567 (U.S. June 5, 2017) (No. 16–402).

250 *See* S. 178, 2015 Leg., Reg. Sess. (Cal. 2015).

251 *See In re* Application of the United States for an Order Directing a Provider of Elec. Communic'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 306–07 (3d Cir. 2010) (discussing a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity obtains a warrant).

are in their jurisdiction; while not required to adopt circuit decisions outside their jurisdiction, this may tend to support the general disagreement between district courts over the proper application of Fourth Amendment law.[252] *Ledbetter* came out of the District of Ohio, within the Sixth Circuit, and like its parent circuit, it determined that there was no reasonable expectation of privacy.[253] Yet, *In re Application for Tel. Information Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) rejected the Sixth Circuit's ruling and since its parent the Ninth Circuit has no controlling precedent, held that the individual's expectation of privacy was reasonable.[254] Therefore, the ultimate decision must come from the Supreme Court, for only it can settle division among the lower federal courts.

Even the Supreme Court is not entirely enlightening on this issue because it has a history of rulings that lead to different conclusions.[255] In *Smith v. Maryland*, 442 U.S. 735 (1979), the Court set the tone for police surveillance being permissible when the individual assumes the risk that their information could be turned over to police.[256] Yet, the *Jones* ruling flipped the tables and held that it is unconstitutional for law enforcement to use GPS tracking on personal property to track suspects' movements.[257] The problem is that the Court has never taken a case where the issue solely revolved around CSLI and location data tracking; the closest is arguably *Riley*, but even that does not entirely fit into the mold of warrantless CSLI and location data tracking.[258]

Perhaps the Court will use *Carpenter v. United States*, 819 F.3d 880 (6th Cir. 2015), *cert. granted*, 85 U.S.L.W. 3567 (U.S. June 5, 2017) (No. 16–402), to settle the issue once and for all.[259] *Carpenter* asks the Court to consider whether

---

252 *See supra* Part II.

253 United States v. Ledbetter, No. 2:15-CR-080, 2015 WL 7758930, at *1 (S.D. Ohio 2015 Dec. 2, 2015).

254 *See In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1020 (N.D. Cal. 2015) (finding that individuals have an expectation of privacy in the historical CSLI associated with their cell phones, and that such an expectation is one that society is willing to recognize as reasonable).

255 *See also supra* Part III.

256 *See* Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that it would be unreasonable for the depositor to expect for his financial records to remain private).

257 *See* United States v. Jones, 565 U.S. 400, 404 (2012) (holding that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a "search").

258 *See* Riley v. California, 134 S. Ct. 2473, 2480–81 (2014) (focusing on the physical inspection of Riley's mobile device for pictures, text messages, videos, and other forms of CSLI contained on the phone itself).

259 *See* Hurley, *supra* note 40 (recognizing the need for the Supreme Court to make clear that Fourth Amendment protections apply with undiminished force to sensitive cellphone digital records).

the warrantless seizure and search of 127 days of CSLI data to track Carpenter's movements is constitutional.[260] However, while this may be the timeliest and most relevant case to reach the Court, there is no guarantee the Court will address the underlying issue of privacy rights in one's CSLI data considering how the Court has avoided the issue at almost every turn or chose to rule on other points of law.[261]

2. Individual Privacy Rights, The Fourth Amendment, and Balancing

Individual privacy and the rights guaranteed under the Fourth Amendment should be protected to the fullest extent of the law. Yet the protections should not interfere with the police's duty to protect the public.[262] Courts need to undertake a balancing of public interest against personal privacy expectations extending beyond the traditional secure-in-one's-home analysis.[263] This would be different from the traditional reasonableness test because it builds upon, and expands, the test already in place to cover electronic devices.[264] As discussed in *Quon*, legal jurisprudence has not caught up to expanding use of mobile devices.[265] The American legal landscape has changed in the six years since *Quon*, as there are now more research studies, public opinion polls, and legal jurisprudence on Americans' use of mobile devices and privacy expectations society attaches to information on the devices.[266]

---

260 *See* Carpenter v. United States, 819 F.3d 880, 886 (6th Cir. 2015), *cert. granted*, 85 U.S.L.W. 3567 (U.S. June 5, 2017) (No. 16–402).

261 Hurley, *supra* note 40. The Court is just as likely to punt the issue by merely deciding another point of law as it is to decide the issue of CSLI privacy rights. It may choose to follow the Smith approach that this culmination of days is unconstitutional without a warrant, without even touching the underlying issues. *See, e.g.*, United States v. Jones, 565 U.S. 400, 404 (2012); *In re* Application of United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Tel., 460 F. Supp. 2d 448, 462 (S.D.N.Y. 2006).

262 *See* Rosenbaum, *supra* note 59 (discussing the public's opinions on privacy protections and national security); Moore, *supra* note 60; Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 238 (1993) (discussing the balance between Fourth Amendment protections and responsibilities and duties of police officers in maintaining law and order in American society).

263 *See* Rosenbaum, *supra* note 59 (discussing the public's opinions on privacy protections and national security).

264 *See id.* (detailing how Americans are torn between protecting their mobile devices and allowing the government to protect the entire society); Maclin, *supra* note 262, at 211.

265 *See* City of Ontario v. Quon, 560 U.S. 746, 748 (2010) (recognizing that the Court did not have enough information or expertise to gauge whether society was in favor of protecting mobile device information or if it was willing to allow the government leeway in searching the information).

266 *See* Rainie, *supra* note 58 (finding that 74% of Americans believe it is very important they are in control of who gets their information, and 65% say it is very important they be able to control what information is collected about them).

In a Pew Research Center study, 5% of Americans surveyed were "very confident" the records kept by their mobile device's service provider were private and secure, whereas 31% were "not at all confident."[267] Additionally, when asked how confident they were that their search engine history records, social media site records, and online video site records would be kept secure and private, 1% of Americans were "very confident."[268] While the survey may show that Americans are very skeptical about the security of CSLI and location data searches, it more likely shows that they have a very low expectation of privacy for their information in those mediums.[269] There is something inherently disturbing when considering that Americans do not feel that their private and sensitive information are protected from the prying eyes of their own government.[270]

The current reasonableness test has been used by every circuit court to rule in favor of law enforcement,[271] yet that test is outdated and does not take into account the modern development of mobile-device technology and sentiment that Americans attach to their devices.[272] In 1903, Edgar Kinkead stated, "Next to the security of one's person, life and health, the safety of his belongings and possessions from disturbance is the most valuable of all his civil rights."[273] That statement is as relevant today as it was in 1903, and perhaps even more relevant. Americans value their mobile devices like they value jewelry, watches, and their passports.[274] In fact, 62% of Americans get information about health conditions

---

267 *Id*.

268 Rainie, *supra* note 58 (stating for search engine history, 41% were "not at all confident"; for social media records, 45% were "not at all confident"; and for online video site records, 42% were "not at all confident").

269 *See id.*

270 *Id*. (stating that America is meant to be a "free" country in which its citizens are not harassed by the government and can live in a manner that is free from the oversight of Big Brother at every turn); Ms. Smith, *Americans feel they have no privacy, don't trust government or advertisers*, CSO (Nov. 12, 2014, 3:55 PM), https://www.csoonline.com/article/2846048/microsoft-subnet/americans-feel-they-have-no-privacy-dont-trust-government-or-advertisers.html.

271 Graham v. Connor, 109 S. Ct 1867, 1871 (1989) ("[A]ll claims that law enforcement officers have used excessive force– deadly or not– in the course of an arrest, investigatory stop, or other 'seizure' of a free citizen should be analyzed under the Fourth Amendment and its objective 'reasonableness' standard.").

272 *Id.*; s*ee* Riley v. California, 134 S. Ct. 2473, 2484 (2014) (stating that modern mobile devices are a pervasive part of Americans' daily lives, and that any test must take that factor into account).

273 *See* 2 EDGAR KINKEAD, COMMENTARIES ON THE LAW OF TORTS: A PHILOSOPHICAL DISCUSSION OF THE GENERAL PRINCIPLES UNDERLYING CIVIL WRONGS EX DELICTO 983 (1903) (highlighting the importance of feeling confident in one's personal privacy rights).

274 *Cf.* Smith, *supra* note 23 (showing that over half of Americans with mobile devices use them on a daily and constant basis).

on their mobile devices, 57% do online banking, 40% look up government information, and 43% find information about jobs.[275]

Most informative is that Americans in 2016 overwhelmingly felt that it is "very important" to control who can get information on them and what information is collected.[276] Coupled with 46% saying they "couldn't live without" their mobile devices,[277] there is an expectation of privacy in the information and CSLI that mobile devices emit on a near-constant basis.[278] It stands to reason that Americans now, more than ever, value their mobile data and location information privacy.[279]

While it may appear that location data can be included under the data protected by the Court in *Riley*,[280] a distinction must be made.[281] The data searched on Riley's mobile device was akin to data that might be found on a camera, laptop, iPod, tablet, or other device containing personal information and memories.[282] Yet, location data was not seized from his mobile device, and the Court did not explicitly include location data in its holding.[283] Location data is an extremely specific subset of information data that is stored on mobile devices.[284] Location data, which is technically known as "cell site location information" (CSLI), encompasses any signals or location-specific information transmitted from a device to a cell tower.[285]

Searches and seizures of this data need to be protected through warrants because they are the modern equivalent of one's most personal secrets.[286] For

---

275 *Id.*

276 *See* Rainie, *supra* note 58 (discussing Americans' attitudes about personal information privacy).

277 Smith, *supra* note 23.

278 *Id.*

279 *Id.*

280 *See* Riley v. California, 134 S. Ct. 2473, 2480 (2014) (stating that some of the data accessed by police included contact lists, text messages, videos, photographs, and messages).

281 *See id.* at 2480 (stating that some of the data accessed by police included contact lists, text messages, videos, photographs, and messages).

282 *Id.*

283 *Id.* at 2489 (discussing the importance of location data to new electronic devices despite the case not explicitly involve location data, therefore setting the tone for future cases purely involving location data).

284 *See In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1013–15 (N.D. Cal. 2015).

285 *See supra* Section II.A.

286 *See* Michael Grothaus, *iPhone 7 vs Samsung Galaxy S7: The BIG Flagship Fight Rages On*, KNOW YOUR MOBILE (Oct. 7, 2016), http://www.knowyourmobile.com/mobile phones/apple-iphone-7/23410/iphone-7-vs-samsung-galaxy-s7-edge-specs-features-price-detailed-ios-10-android-n (showing that since the release of the first iPhone by Apple in 2007, the mobile device has become implanted into the average American's daily life because they provide GPS services, banking services, news services, and store unimaginable amounts of data); Rainie, *supra* note 58 (acknowledging 65% of Americans want to control

example, had the British known where and when General Washington's troops were crossing the Delaware River, the American Revolution may have ended very differently. Similarly, if the government knows citizens' whereabouts at all times, there is an inherent breakdown of personal freedoms and protections.[287]

3. Post-September 11 America, the PATRIOT Act, and New American Expectations

It has been over fifteen years since September 11, 2001, and Americans have moved beyond the terror-infused mentality that spurred the government to collect troves of data for "security" reasons.[288] In recent twenty-first century America, a majority of Americans are not willing to sacrifice their personal liberties and privacy rights to the same degree to allow collecting and retaining data.[289] There is a definite difference between the years immediately following the terrorist attacks in New York, Pennsylvania, and Washington, D.C. where Americans were willing to allow passage of such laws as the PATRIOT Act,[290] and today where Americans have slid more towards the middle of protecting the nation but also not invading personal liberties.[291]

The PATRIOT Act was one of the most all-encompassing and comprehensive national security laws to be passed in modern America,[292] and with that came a greatly diminished sense of personal privacy and security in one's electronic communications.[293] At that time, Americans were willing to forego those

---

what information is collected about them).

287 *See infra* Section IV.A.3.

288 Rosenbaum, *supra* note 59 (highlighting the opinion of one man, "[t]his is a scary world and if it helps find terrorists or helps combat the war against terrorism, then it's OK.").

289 *See* Rainie, *supra* note 58 (noting that 65% of Americans say there are not enough limits on what telephone and internet data the government can collect on citizens); Susan Milligan, *A Question of Risk*, U.S. NEWS (June 12, 2015, 6:00 AM), https://www.usnews.com/news/the-report/articles/2015/06/12/privacy-or-terrorism-a-question-of-risk (finding that Americans are now less willing to give up privacy to protect them from terrorism).

290 David W. Moore, *Public Little Concerned About Patriot Act*, GALLUP (Sept. 9, 2003), http://news.gallup.com/poll/9205/public-little-concerned-about-patriot-act.aspx.

291 *Id*.; Rosenbaum, *supra* note 59; Milligan, *supra* note 289 (finding that Americans are now less willing to give up privacy to protect them from terrorism).

292 *See* Dara Lind, *Everyone's heard of the Patriot Act. Here's what it actually does*, VOX (June 2, 2015), https://www.vox.com/2015/6/2/8701499/patriot-act-explain; Jeremy Diamond, *Everything you need to know about the Patriot Act debate*, CNN (May 23, 2015, 1:44 AM), https://www.cnn.com/2015/05/22/politics/patriot-act-debate-explainer-nsa/index.html.

293 *See* USA PATRIOT Act of 2001, H.R. 3162, 107th Cong. §§ 201-03, 209, 213-14 (allowing the government to intercept communications related to terrorism and computer

protections and securities in order to secure the nation against future terrorist attacks and foreign actions.[294] However, Americans have generally moved away from that mentality, due to the passage of time from the attack and newfound technology, to a mentality that leans more towards protecting personal information unless it is for extreme national security purposes.[295]

It is high time that the Supreme Court, and thus all American courts, recognize a new and expanded reasonableness test to deal with the advent of modern technology, mobile-device use, and American expectations of privacy in electronic information. That new and expanded test would be served well by the creation of a legally recognized exception to the Fourth Amendment's warrant requirement.[296] Such a new exception to the warrant requirement could be effectuated through a modernized reasonableness test focusing on balancing the rights and interests of the individual against the interests of the government in preventing crime.[297]

B. Create a New Exception to the Warrant Requirement by a Modern Take on a Traditional Test

The Supreme Court has a duty to settle the issue of law enforcement obtaining mobile-device location data through warrantless compulsion of service providers. This question, how far police and the government can go to use location data against a person when the data was obtained without a warrant, has been skirted or only addressed in generalities by the Court to date.[298] With the

---

fraud, share criminal investigative information, seize voice-mail messages with warrants, delay notification of a warrant being issued, and modify the law relating to pen registers); *see* Lind, *supra* note 292.

294 *See* Rosenbaum, *supra* note 59; Lind, *supra* note 292.

295 *See generally* Owsley, *supra* note 9, at 224 (referencing Congressman Bliley's concern over the government knowing too much about cell phone subscribers' locations); Rosenbaum, *supra* note 59 (reporting privacy concerns as cell phone and GPS technology becomes more advanced).

296 *See generally* Roberto Iraola, *New Detection Technologies and the Fourth Amendment*, 47 S.D. L. REV. 8, 15 (2002) (explaining the Fourth Amendment's warrant clause and how the reasonableness clause has historically found refuge in unique circumstances).

297 *Id.* at 15–16.

298 *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014) (finding a lack of "precise guidance" in how to determine what type of search to exempt from the Fourth Amendment's warrant requirement); City of Ontario v. Quon, 560 U.S. 746, 759 (2010) (stating that the judiciary must proceed with caution in not making a ruling before knowing where electronic communications fit into society); Arizona v. Hicks, 480 U.S. 321, 325 (1987) (holding that a police officer's viewing of an item in plain view does not constitute a search but physically moving furniture to see something does constitute a search); Ryan Birss, *Alito's Way: Application of Justice Alito's Concurring Opinion in* United States v. Jones *to Cell Phone Location Data*, 65 HASTINGS L.J. 899, 928 (2014) (concluding that the majority opinion in

ever-evolving and expanding world of mobile device communications and GPS,[299] there needs to be a clear rule for courts to follow when facing such challenges.[300] One solution is for the Supreme Court to create a newly recognized exception to the Fourth Amendment's warrant requirement.[301] This exception would recognize the modern expectation of privacy in mobile devices, thereby making such tactics a search and allow police to bypass the warrant requirement only upon a sufficient showing of government need outweighing privacy interests.[302]

1. Recognize the Modern Expectation of Privacy in One's Mobile Device Location Data

It is imperative for the Supreme Court to recognize that the average American has a strong, personal, and reasonable expectation of privacy when it comes to *all data* on his or her mobile devices, data that undeniably includes location-based information.[303] The Court should establish a binding presumption on the right to privacy of mobile-device location data, a presumption that makes it a search to obtain such data.[304] However, that presumption should come with a

---

United States v. Jones, 565 U.S. 400, 404 (2012) limits privacy interest in cell phone technology and noting that Justice Alito's concurrence gives courts a way to allow Americans to have a reasonable expectation of privacy of their location through cell phone data).

299 *See* Elizabeth Gula Hodgson, *The Propriety of Probable Cause: Why the U.S. Supreme Court Should Protect Historical Cell Site Data with a Higher Standard*, 120 PA. ST. L. REV. 251, 277 n.195 (2015) (noting Congress recognizes an increase of triangulation and GPA usage with the advent of smartphones thus effecting a greater need for law enforcement to show probable cause to obtain a warrant).

300 *See id.*

301 Riley, 134 S. Ct. at 2493 (employing a balancing test that weighs the degree of intrusion upon an individual's privacy compared to the degree needed for the promotion of government interests).

302 *See infra* Section IV.B.1–2; *see also Exigent Circumstances*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/exigent_circumstances (last visited May 24, 2018) (defining the exigency exception) (applying the exigency exception when an officer does not have sufficient time to secure a warrant, reasonably believes safety is at risk, or reasonably believes that evidence will be destroyed).

303 *See* Babst, *supra* note 242, at 378–79 (showing that cell phone users take steps to privatize data tracking in their smartphones); *cf.* Riley, 134 S. Ct. at 2489 (distinguishing that the third-party doctrine does not apply to CSLI and location data obtained directly through a mobile device or forced "pings"). *See generally* Smith, *supra* note 23 (stating that a "number of Americans" only access to the Internet is through a smartphone).

304 *See In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1019 (N.D. Cal. 2015) (reasoning that mobile devices are considered modern "effects" protected under the Fourth Amendment); KINKEAD, *supra* note 273, at 283 (recognizing that protecting one's belongings and possessions is the most valuable civil rights besides health and security).

caveat that it is not absolute and may be rebutted by a strong showing of public need.[305]

Courts must undertake a balancing of competing interests to determine the level of intrusion, expectation of privacy, and ultimate potential harm to the public.[306] In a perfect world, police would also perform the balancing test in order to ensure accountability and privacy protections; however, this is not a perfect world and the most practical means of accomplishing the balancing test would likely have to remain within the purview of the courts.[307] While it is true that Americans have a strong expectation of privacy in their personal location data,[308] the reasonableness of that belief must be tempered by either a high or low expectation of privacy.[309] It can be extremely high, as with one's personal mobile device that is not used for work purposes.[310] However, it can also be very low, as when the device is used primarily for work purposes.[311] Americans cannot expect to retain their privacy rights to the full extent of constitutional protection when they receive a mobile device from an employer or contract to have information reviewed by another party.[312] The proposed exception would have to make the delineation between purely personal devices and those that have a dual-purpose.[313] As a correlation, the higher the expectation of privacy in

---

305 Arizona v. Hicks, 480 U.S. 321, 326–27 (1987) (presuming that a warrant is required, yet it can be avoided by a showing of probable cause that governmental interests outweigh the individual's privacy interest); *see also* United States v. Chavez, No. 3:14-cr-00185, 2016 WL 740246, at *3 (D. Conn. Feb. 24, 2016) (stating that there is no reasonable expectation of privacy when a person hands information to a third party).

306 *See, e.g.*, Liming, *supra* note 223, at 729 (discussing how balancing tests best weigh the interests of law enforcement and citizens to determine which has the stronger argument and considering the total reasonableness of the search, courts would be able to determine whether the obtained information was legitimate).

307 *Cf.* Baradaran, *supra* note 10, at 8–9 (2013) (describing "blind balancing" as a judge's unbiased balance between privacy rights and societal safety).

308 *See* Rainie, *supra* note 58.

309 *See id.* (reporting 52% of Americans being concerned about government surveillance of their data).

310 *See* United States v. Lambis, 197 F. Supp. 3d 606, 608–09 (S.D.N.Y. 2016) (discussing how DEA agents used pen registers and CSLI relating to a personal mobile device to track the whereabouts of a suspect).

311 *See* City of Ontario v. Quon, 560 U.S. 746, 752 (2010) (displaying example of an individual using a mobile device provided by an employer for uses outside scope of employment and showing Quon's presumed low expectation of privacy in work provided pager through his signed statement of "no expectation of privacy").

312 *See id.* at 764 (holding that search of employer provided pager due to employee's repeated excessive non-work related text messages was reasonable because pager was provided for work-related purposes and search was not excessive in scope).

313 *Compare* Quon, 560 U.S. at 752 (describing employee using employer provided pager for personal reasons); *with* United States v. Lambis, 197 F. Supp. 3d 606, 614 (S.D.N.Y. 2016) (finding that people with personal cell phones are not voluntarily giving their location data to a third party each time they turn on their smartphone).

the eyes of the public, the more likely courts would be able to find that obtaining location data without a warrant constitutes an impermissible search.[314]

Having the Supreme Court engage in a balancing test between the potential harm to the public versus the rights of the individual is not a wildly revolutionary concept.[315] It is generally accepted that courts conduct balancing tests to weigh the safety and welfare of society against the individual's personal privacy interests.[316] This portion of the test should look very similar to other Fourth Amendment balancing tests, in that the overall determination concerns when the public's welfare and safety becomes threatened at a rate disproportionate to the individual's need for privacy.[317] When this occurs, obtaining location data without a warrant may become necessary and expected.[318] However, this burden must be placed on the government and not the individual. The government has vast resources at its disposal to aid in the apprehension of suspects, and therefore must show that no other alternative was available.

---

314 *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2491 (2014) (stating modern mobile devices contain more information about a person than what a search of a traditional house would reveal); Rainie, *supra* note 58 (reporting 74% of Americans want to be in control of who has access to their information and 65% want to be able to control what information is collected by the government). With Americans feeling so strongly about protecting their privacy, the Court needs to acknowledge that privacy interests have extended beyond the traditional home search. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742 (1979) (finding that people cannot have an expectation of privacy in the phone numbers they dial on a phone); *see also* Rainie, *supra* note 58 (reporting that over 60% of Americans believe the government is not doing enough to keep data private); Rosenbaum, *supra* note 59 (reporting privacy concerns as cell phone and GPS technology becomes more advanced).

315 *Cf.* Riley v. California, 134 S. Ct. 2473, 2478 (2014) (finding information on a cell phone found on person incident to arrest does not further government interest and does implicate a "substantially greater" privacy interest than a simple pat down of clothing); City of Ontario v. Quon, 560 U.S. 746, 757 (2010) (stating that a reasonableness standard should be used when balancing employee privacy rights and work related conduct); United States v. Graham, 824 F.3d 421, 427–28 (4th Cir. 2016) (*en banc*) (finding that making and receiving calls and texts on mobile device is like the pen register in Smith v. Maryland, 442 U.S. 735 (1979) where defendant voluntarily gave information to cell phone carrier towers and "assumed the risk" of that third party giving the information to the government).

316 David H. Kaye, *A Fourth Amendment Theory for Arrestee DNA and Other Biometric* Databases, 15 U. PA. J. CONST. L. 1095, 1109 (2013) (stating that the circuit courts apply the Supreme Court of the United States' Fourth Amendment balancing test between government interest and individual privacy rights in their decisions); *see also* United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016); Quon, 560 U.S. at 759–760; Riley, 134 S. Ct. at 2488.

317 *See* Riley, 134 S. Ct. at 2494 (holding the interests of society can be weighed against the privacy rights of the individual in an exigent situation); New York v. Quarles, 467 U.S. 649, 657 (1984) (finding that the safety of society outweighed the privacy interest of suspect when he hid a gun in a supermarket and police asked him where it was before reading his Miranda rights).

318 *See* Riley, 134 S. Ct. at 2494 (holding that, generally, a warrant is required to search a cell phone incident to arrest but there may be an exigency situation to justify a warrantless search of a specific phone).

2. Overcoming the Presumption of Privacy Inherent in Mobile Device Location Data

If the government shows there is a low expectation of privacy, intrusion would be minimal, and potential harm to the public could be great, the presumption would be rebutted.[319] The reason for a rebuttable presumption is that there will be instances where the government and law enforcement need to protect public safety in a small window of time.[320] As with other exceptions to the warrant requirement, this exception must be narrowly tailored to specific reasons for which the government would be able to bypass obtaining a warrant.[321] The government's strongest argument would come by relying on the third-party doctrine to differentiate between instances where the police search a mobile device's content or force the device to perform, and where location data is merely obtained from a service provider.[322] If it can show that the location data was obtained similar to a situation like a pen register, there is more legal weight to the argument.[323]

While it may seem that creating exceptions to the warrant requirement allow the government to bypass a constitutional protection, that is not the case.[324] There is a reason that exceptions to the warrant requirement are so few and far between, and the solution posited does not advocate for the weakening of personal protections. Rather, this exception and test would allow for a judicially recognized presumption of the individual's right to privacy in their mobile device's location data while also giving the government the opportunity to

---

319 *See* Owsley, *supra* note 9, at 227 (stating that under the third-party doctrine, cell phone users arguably do not have a reasonable expectation of privacy in their location data transmitted from their device).

320 *See, e.g.*, United States v. Ledbetter, No. 2:15-CR-080, 2015 WL 7758930, at *3–5, 12 (S.D. Ohio Dec. 2, 2015) (denying defendant's motion to suppress cell phone records because traffic stop and vehicle search uncovering two cell phones were lawful along with subsequent subpoena for cell phone records, and finding defendant coming under the third-party doctrine when using a cell phone and cell carrier to conduct murders).

321 *See, e.g.*, Riley, 134 S. Ct. at 2482, 2494 (holding that a warrant is needed to search a cell phone incident to arrest, and acknowledging the exceptions that exist to prevent the destruction of evidence and when a police officer is pursuing a fleeing suspect, assisting injured persons, or assisting persons threated with imminent injury).

322 THOMPSON, *supra* note 11, at 11 (stating that the government can obtain data information from cell carriers under the *Smith* third-party and assumption of risk doctrines). Getting the location data from a provider, which would be considered a third-party, would make the search more like the installation of a pen register than directly tapping a phone. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (finding that when a phone number is dialed, the dialer is conveying that information to a third party).

323 *See* Smith, 442 U.S. at 742 (finding that telephone users must convey the number they are dialing to a telephone company's switch board).

324 *See* City of Ontario v. Quon, 560 U.S. 746, 764 (2010) (finding that search did not become unreasonable when the government obtained information from a third party).

protect public safety in instances where obtaining a warrant would unfairly compromise public welfare.[325]

3. Shaping the New Exception to the Warrant Requirement and a Proffered Example

The novelty of this solution is that it creates an exception to the warrant requirement, recognizing the modern-day importance of location data to Americans while also allowing law enforcement to perform its duty of protecting citizens.[326] Courts need to adhere to the test established by Justice Harlan in recognizing societal interests in protecting personal data information.[327] Yet an overarching and absolute protection of location data would prejudice law enforcement's ability to keep people safe and prevent crime.[328] That is why creating an exception to the Fourth Amendment's warrant requirement would be a viable solution to this issue. It would allow for the presumption of societal interest in protecting location data while also giving police the opportunity to overcome the presumption in special cases.[329]

Using a balancing test, courts would be able to determine whether the government met its burden to overcome the newly recognized protection of mobile-device location data.[330] Take for example the Boston Marathon Bombing in 2013; had the police been able to dispense of the traditional procedure of obtaining a warrant, the Tsarnaev brothers, modern-day terrorists, may have

---

325 *See supra* Section IV.B.1; *see also* Arizona v. Hicks, 480 U.S. 321, 327–28 (1987) (holding that dispensing of the need for warrants in some circumstances is not the same as accepting a lesser standard than what a warrant would mandate).

326 United States v. Graham, 824 F.3d 421, 437–38 (4th Cir. 2016) (affirming the district court's holding that the government did not violate the Fourth Amendment when it acquired CSLI records from the defendant's cell phone carrier).

327 *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (establishing a two-part test for search in that the first part is a subjective belief of privacy and the second part is society's objective belief in recognizing that privacy).

328 *See, e.g.*, Rob Cerullo, *GPS Tracking Devices and the Constitution*, POLICE CHIEF, Aug. 2016, at 2 (showing cases where warrantless GPS use by police upheld by courts and warning against restricting use too much and rendering law enforcement unable to perform its duties).

329 *See supra* Section V.B.1–2.

330 *See, e.g.*, Baradaran, *supra* note 10, at 57 (stating that while no balancing test is fair, it is needed so a judge does not rely merely on her gut intuition). Unlike the "blind balancing" concept Professor Baradaran advocates against, a proper balancing test in this warrant requirement exception would eliminate judges considering costs and benefits to parties and society which lacks relevance and completeness. When applying "blind balancing," judicial members are prone to ignoring important evidence which provides context to the individual case before the bench. *Id.*

been apprehended sooner and lives saved.[331] Police could have easily demonstrated to a court that the government's interest in protecting the public from suspected terrorists in this instance far outweighed the Tsarnaevs' privacy interest in protecting their location data.[332] This type of event would satisfy the exception.

The purpose of recognizing a new exception to the warrant requirement, and using a balancing test for that exception, is to provide individualized, case-by-case analysis of Fourth Amendment legal issues in a twenty-first century world.[333] Law enforcement would still be able to obtain a warrant for CSLI and location data through traditional means. The new exception would simply provide a vehicle for recognizing public interest in location data privacy, provide situations where the government could dispense with obtaining a warrant, and settle the debate over constitutionality of warrantless searches of mobile-device location data.[334]

C. Addressing Counterarguments from the Majority of Scholarship

As with any scholarly issue there will be counterarguments to the solution advocated. With a modern issue like mobile device location data tracking, there are bound to be strong opinions on both sides of the debate.[335] Addressing

---

331 *See generally* O'Neill, *supra* note 69 (showing suspect's data usage regarding bombing two months prior to crime).

332 Police could also have provided sufficient need for GPS location data from the phones due to the ongoing emergency. *How GPS Works*, GPS.GOV, http://www.gps.gov/multimedia/poster/ (last modified Sep. 26, 2016).

333 *See The Problem with Mobile Phones*, SURVEILLANCE SELF-DEFENSE, https://ssd.eff.org/en/module/problem-mobile-phones (last updated Feb. 10, 2015) (discussing the surveillance problems associated with the ubiquity of mobile devices being used a primary means of communication); *see also* Baradaran, *supra* note 10, at 57–58 (quoting Professor Baradaran) ("[J]udicial balancing ignores broader evidence the provides context to the individual case at hand."). A case-by-case approach would dispose of cases and issues before courts in a fair and constitutional manner. *Id.*

334 *See* Rainie, *supra* note 58 (presenting data regarding Americans general concerns about location data privacy). *Compare* United States v. Ledbetter, No. 2:15-CR-080, 2015 WL 7758930, at *1 (S.D. Ohio Dec. 2, 2015) (denying defendant's motion to suppress evidence obtained from the government's use of cell site location information), *with In re* Application for Tel. Information Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1013 (N.D. Cal. 2015) (denying the government's application "to obtain historical cell site location information associated with [Redacted] target cell phones"), *and* United States v. Lambis, 197 F. Supp. 3d 606, 608 (S.D.N.Y. 2016) (granting the defendant's motion to suppress evidence recovered by DEA agents use of cell site location), *and* United States v. Chavez, No. 3:14-cr-00185(JAM), 2016 WL 740246, at *1 (D. Conn. 2016) (denying the defendant's motion to suppress evidence acquired by the government's use of cell site location information).

335 *See* Dolan, Lennon & Munoz, *supra* note 9, at 38–41 (recognizing privacy advocates' increasing concerns with the potential for covert police surveillance of mobile device GPS

counterarguments against one's solution while acknowledging potential weaknesses is a vital step towards furthering theory and debate.

1. Fundamental "American" Rights of Privacy and Security in Oneself and Possessions

There is a pervasive notion that individual rights and security are an inherently "American" concept that cannot be encroached upon.[336] A large portion of scholarship supports the view that mobile device location data is the modern equivalent of one's essential property and should therefore be protected against governmental search.[337] However, mobile devices are only tools for making life, arguably, easier; they do not hold the same legal significance as the home or birth certificate. Unlike one's wallet or social security card, which can be zealously guarded and physically protected, mobile device data is sent via cell towers, uploaded onto social media, downloaded and stored by service providers, and easily accessible by third parties.[338] History has shown that these rights are curbed against the overall interests of society and the protection of the Union.[339] Therefore, it stands to reason that case law indicating one's mobile

---

data and acknowledging that courts have yet to definitively take a stance against the Fourth Amendment violations such surveillance poses).

336 *See, e.g.*, THE FEDERALIST No. 51 (James Madison) ("A double security arises to the rights of the people . . . It is of great importance in a republic . . . to guard one part of the society against the injustice of the other part . . . If a majority be united by a common interest, the rights of the minority will be insecure.").

337 Ross Hoogstraten, *Implications on the Constitutionality of Student Cell Phone Searches Following* Riley v. California, 24 WM. & MARY BILL OF RTS. J. 879, 911 (2016) (arguing that warrantless searches of cell phones are unreasonable "almost in every context because of the reasonable expectation of privacy" one has in the data on the device, which outweighs government concerns); Jordan Miller, *New Age Tracking Technologies in the Post-*United States v. Jones *Environment: The Need for Model Legislation*, 48 CREIGHTON L. REV. 553, 603 (2015) (arguing that the best way to protect individuals from wide-ranging government searches is "to adopt comprehensive legislation . . . able to predict the future developments of technology . . . as technology advances in the field of tracking searches.").

338 *See, e.g.*, HARRIS, *supra* note 61, at 2–4 (explaining how mobile devices and the information stored within them can be accessed by anyone with the devices' unlocking combination or password to personal websites, whereas a wallet and social security card must physically be taken in order to be used by another person); THOMPSON, *supra* note 11, at 7 (discussing the relationship between the Fourth Amendment and "government access to records and other information held by third parties").

339 Marc McAllister, *GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis*, 82 U. CIN. L. REV. 207, 235 (2013) (demonstrating that the Supreme Court has reasoned that a "search" considers whether "society is prepared to recognize [a defendant's asserted expectation of privacy] as reasonable which shows that consideration of individual interests against government searches turns on whether society believes that the individual should be free from such searches." Protecting the interests of society comes before the interests of the individual when the individual's interest would harm society).

device is not necessarily his or her "castle" may be in line with historical Fourth Amendment analysis.[340]

Another line of argument for requiring location data to be obtained only through a warrant is that *Riley v. California* should be read broadly, extending well beyond the search-incident-to-arrest exception.[341] The basis for this claim is the belief that the Court in *Riley* created a *per se* rule that requires a warrant every time content is accessed on mobile devices.[342] In his argument, one author states, "Many of the cases taking a narrow view of *Riley* ignore the vast storage capacity that cell phones have, frustrating the qualitative differences that the Court saw between these devices and other articles."[343] However, this argument fails to consider the fact that *Riley* was a unanimous decision from the Court.[344] This is a feat that would arguably have been impossible to attain if the ruling were to be read broadly as applying to almost any situation involving mobile devices.

The "Conservative Wing," for example, would be very unlikely to vote for a consistently broad interpretation that does not consider every applicable factor.[345] Broadly interpreting the decision, as pointed out, would suffer the same flaws as narrowly interpreting the decision.[346] Yet, it would also create an expansive interpretation beyond the Court's holding. [347] Weight must be given to the Court refusing to specifically address the privacy protections inherent in location data and CSLI in *Riley*, a fact tending to caution against broad application of the holding.[348] Besides the above mentioned counter arguments, a substantial amount of scholarship claims that the only reason warrantless location data tracking is considered constitutional is because of surveillance

---

340 *See* United States v. Skinner, 690 F.3d 772, 781 (6th Cir. 2012) (reasoning that since GPS data is inherently included in the communicative feature of mobile devices, and users know that such communications are not private, the defendant had no reasonable expectation of privacy in his location data).

341 Bryan Sandford, *A Castle in the Sky: GPS Tracking of a Defendant's Cell Phone Post–Riley v. California*, 2015 WIS. L. REV. 907, 938 (2015) (arguing that reading Riley's holding narrowly "ignores the plain language of the decision and frustrates the underlying policy articulated by the Court.").

342 *See id.* at 909–10 (arguing that the Court's recent decisions support a *per se* rule which would require courts to apply every warrant requirement exception to see if any fit, before allowing the police to obtain data without a warrant).

343 *Id.* at 922.

344 *See* Riley v. California, 134 S. Ct. 2480, 2495 (2014).

345 *See* Arizona v. Hicks, 480 U.S. 321, 327 (1987) (stating that overly-broad holdings would jeopardize doctrinal theories protecting the authority of police to make warrantless searches and seizures in public places).

346 Sandford, *supra* note 341, at 938.

347 *See* LaChance, *supra* note 8 (arguing that a warrant is still necessary regardless of cell phones' technological advances and efficiencies).

348 *See* Riley v. California, 134 S. Ct. 2480, 2490, 2492, 2494 (2014) (addressing the important role cell phone location data can play in proving an individual's guilt).

statues enacted by Congress.[349]

2. Congressionally Enacted Surveillance Statutes Provide the Only Justification to Warrantless Location Data Tracking Being Considered Constitutional

Some academics have claimed that the constitutionality of location data tracking without a warrant is doubtful at best, and the legal basis can only be found in surveillance statutes.[350] Such statutes are binding law, and when consumers willingly leave their location tracking apps open on their mobile devices, they are put on notice as to the ramifications. [351] If citizens do not want their locations tracked via GPS, they only have to disable GPS capabilities of their mobile devices. A counter to that reasoning is that misinterpretation of landmark Supreme Court Fourth Amendment decisions risks eroding civil liberties.[352] Claiming that since the public does not favor a "surveillance state" the Court must follow public opinion misinterprets the American system's foundation upon checks and balances between coequal branches of government.[353]

Americans expect the freedom to move about in relative anonymity, without the government keeping an individualized itinerary of their comings and

---

349 *See infra* Section IV.C.2.

350 *See* Ian James Samuel, *Warrantless Location Tracking*, 83 N.Y.U. L. REV. 1324, 1351 (2008) ("[T]he 'right to be let alone' does not mean much if, thanks to the vicarious presence of the state in one's phone, solitude is an illusion."); *see also* Nathaniel Wackman, *Historical Cellular Location Information and the Fourth Amendment*, 2015 U. ILL. REV. 263, 315, 318 (2015) (recognizing that Congress has legislated the Stored Communications Act to regulate such searches, and advocates for amendments to include suppression remedies for location data seized).

351 The age-old legal doctrine that ignorance of the law is no excuse proves telling in this instance because consumers are given ample opportunity to decline third-party tracking and data sharing when they are given the choice of downloading and using a program, app or website. *See* Oliver Wendell Holmes Jr., *The Common Law*, U. OF TORONTO L. SCH. 1, 45, 52 (2011) ("Ignorance of a fact and inability to foresee a consequence have the same effect on blameworthiness.").

352 *See* Tim Sheehan, *Taking the Third-Party Doctrine Too Far*, 13 GEO. J.L. & PUB. POL'Y 181, 182 (2015) (claiming that public opinion at this time is "firmly in favor of curtailing, not enlarging, the surveillance state.").

353 *See, e.g.*, Baradaran, *supra* note 10, at 49–50 (stating that the judicial branch of government is *supposed* to be above the public's influence; it cannot issue effective legal decisions if it is beholden to public whims); Sheehan, *supra* note 352, at 182 (explaining that the Supreme Court has never sought to issue a clear ruling on this topic, even though those arguing for a straight ban on compelling location data without a warrant would lead readers to believe that there is binding precedent supporting requiring a warrant in such circumstances).

goings.[354] Latching onto this concept, an argument has been made that the constitutionality of warrantless tracking should depend upon the nature of the crime being investigated.[355] Not only is this discrimination against certain classes of crimes, it would most likely constitute extreme selectivity of crimes that would be rebuked by courts and legislatures alike.[356] Applying selective standards would be a step in the wrong direction and would only lead to more confusion for law enforcement and courts reviewing the actions of those law enforcement officers.

One of the most common counterarguments is that the ubiquitous nature of mobile devices and technology in American society has created a new expectation of privacy in such property.[357] Yes, technological advances can create modernized expectations of privacy. However, in a technological age it is also important to adapt the legal protections afforded to law enforcement.[358] Modern mobile devices allow those seeking to break the law to look up the locations they plan to visit, communicate GPS coordinates and roadmaps, hack

---

354 *See* Renee M. Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 455 (2007) ("[C]itizens of this country largely expect the freedom to move about in relative anonymity without the government keeping an individualized, turn-by-turn itinerary of our comings and goings."). This point aligns with the solution posited in this Note that there is a need for a test differentiating when the freedom to move about should be protected and when it is heavily outweighed by the public interest because public opinion is only one factor considered for whether privacy expectations are reasonable and must be weighed against the potential harm to society. *See supra* Section IV.B.

355 McAllister, *supra* note 339, at 250–53 (delineating three categories of individuals and standards to be applied: "Those Suspected of Severe Crimes," "Those Suspected of Minor Crimes," and "Those Not Suspected of Any Crime"); Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 638 (2016) (arguing that "magistrates should not authorize police to. . . download and comb through millions of pages of data that is unrelated to the crime being investigated.").

356 On top of that legal issue, there is the assumption that such a selective and discriminatory test would enrage the populace and receive little to no support from Congress. *See* McAllister, *supra* note 339, at 246–50 (analyzing public survey results and recent congressional and judicial decisions to prove a general societal preference to limit the government's ability to obtain cell phone information from individuals without a warrant).

357 Owsley, *supra* note 9, at 230; *see, e.g.*, Freiwald, *supra* note 10, at 748–49 (stating that a probable cause standard which requires notifying the target and providing meaningful remedies would make a significant difference in protecting individuals privacy rights from "government compulsion of disclosure of location data"); *see also* Suuberg, *supra* note 12, at 330 (pointing to the Electronic Frontier Foundation's summary of a Sixth Circuit's reasoning in a privacy protection case as being a harmful denial of "an expectation of privacy in cell phones.").

358 *See* Freiwald, *supra* note 10, at 725 (stating that "Location data has furnished law enforcement with investigatory and prosecutorial value in the past several years."); Cerullo, *supra* note 328, at 2 ("Advanced technology greatly enhances a police officer's ability to fight crime.").

into users' bank accounts and social media sites, and countless other illegal acts.[359] Not allowing law enforcement, under specific conditions, to access the information on those devices would lead to a gross imbalance of power between lawbreakers and the men and women whose duty it is to prevent violations of the law.[360] It would harm society to hamstring the police by forcing them into using outdated technology and methods to find and track suspects.[361]

Modern technology must be allowed to progress, and law enforcement must be able to similarly adapt.[362] Arguments will inevitably be raised against this proposed solution; however, the fundamental issue of how to balance law enforcement's needs and societal interests remains.[363] Merely stating that there is a problem, and that it needs fixed, will not bring about change.[364] Change can only come from educated discourse, on both sides of the issue, leading to a refined and balanced solution.

V. CONCLUSION

The United States Supreme Court must act sooner, rather than later, in taking up a litmus test case that will set new precedent for upcoming mobile device location tracking jurisprudence. By forming a new exception to the Fourth Amendment's warrant requirement, the Court will craft a more comprehensive and applicable standard for the inevitable rise in electronic-mobile cases.[365] It is not enough to broadly hold that law enforcement's obtaining of location tracking data from service providers is not a breach of the Fourth Amendment because that would be a travesty to the rights and freedoms protected under the Amendment.[366] A test establishing factors relevant to a constitutional analysis will enable courts to protect against unwarranted searches at the same time as protecting individual privacy interests.[367] Additionally, the test will give courts flexibility to weigh the interests of the public against the individual's right to privacy, and in certain cases to uphold law enforcement's use of location data

---

359 Van Ells, *supra* note 24.

360 *See supra* Section IV.B.

361 *See* Cerullo, *supra* note 328, at 2 (noting that America cannot have it both ways: To be protected from modern crime, and to push law enforcement and government out of citizens' location data completely); *see also* Dolan, Lennon & Munoz, *supra* note 9, at 39–41 (highlighting cases wherein modern GPS tracking data has assisted investigators in solving cases by accurately tracing the locations of criminals).

362 *See supra* Section I.B.3.

363 *See supra* Section IV.B.1–3.

364 *See supra* Section IV.A-C.

365 *See supra* Section IV.B.3.

366 *See supra* Section IV.B.1.

367 *See supra* Section IV.B.3.

obtained without a warrant.[368]

As America continually progresses into a more technologically advanced nation, the problem of law enforcement, and the government, using electronic location data to track suspects will only continue to fester.[369] With the advent of even more advanced technology, Americans will immerse themselves to a greater degree into the electronic mobile world. The legal field needs to be ready to adapt to that new reality and recognize the inherent expectation of privacy in mobile-device location data.[370] Without comprehensive and modernized mobile device jurisprudence, the risk of constitutional rights being trampled will only multiply.[371]

368 *See supra* Section IV.B.3.
369 *See supra* Section I.A.
370 *See supra* Part III.
371 *See supra* Sections IV.A-C.