THE FALSE HOPE OF MISSOURI'S AMENDMENT NINE AND THE REAL PROBLEMS WITH CONSTITUTIONAL PROTECTION OF ELECTRONIC DATA AND COMMUNICATIONS FROM GOVERNMENT INTRUSION

INTRODUCTION

On August 5, 2014, Missouri voters passed Amendment Nine to the Missouri Constitution.[1] The amendment (hereafter "Amendment Nine") changed the text of Article I, Section 15, Missouri's analog to the United States Constitution's Fourth Amendment, to include protections for "electronic data" and "electronic communications" in the enumerated list that previously tracked the language of the Fourth Amendment: "persons, papers, homes, and effects."[2] The bill introducing Amendment Nine was sponsored by Republican State Senators Rob Schaaf and Bob Dixon.[3] Amendment Nine passed by a 74.25% to 25.75% vote in the statewide election.[4]

In late June, shortly before the Missouri election, the United States Supreme Court decided *Riley v. California*.[5] *Riley* held that the warrantless search of the contents of a cell phone incident to an arrest was a violation of the Fourth Amendment, other than in extremely rare situations where the phone itself presents a danger.[6] Many questioned whether Amendment Nine would have any effect in the wake of *Riley*.[7]

In a recent Missouri case, a party argued that Amendment Nine "demonstrates a clear public policy choice" to protect "citizens' electronic data" from "harvesting" by the government.[8] The argument that Amendment

1. *Missouri Electronic Data Protection, Amendment 9 (August 2014)*, BALLOTPEDIA, http://ballotpedia.org/Missouri_Electronic_Data_Protection,_Amendment_9_(August_2014) [http://perma.cc/PH2N-LT6B] [hereinafter BALLOTPEDIA] (last visited July 16, 2015).

2. MO. CONST. art. I, § 15; BALLOTPEDIA, *supra* note 1.

3. Kevin McDermott, *Proposed Missouri Amendment Would Extend Privacy Protection to Cell Phones, Email*, ST. LOUIS POST-DISPATCH, July 22, 2014, at A1, http://www.stltoday.com/news/local/govt-and-politics/proposed-missouri-amendment-would-extend-privacy-protection-to-cell-phones/article_53aa9cb5-b73b-5008-9805-c45ebe73e29e.html [http://perma.cc/S7XF-V87A]; BALLOTPEDIA, *supra* note 1.

4. BALLOTPEDIA, *supra* note 1.

5. Riley v. California, 134 S. Ct. 2473 (2014).

6. *Id.* at 2495.

7. *See infra* Part I.B.

8. Brief of Appellees at 33, State *ex rel* Koster v. Charter Commc'ns, Inc., 461 S.W.3d 851 (Mo. Ct. App. May 26, 2015).

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

Nine be given effect continued, saying "[Amendment Nine] also demonstrates a policy choice to bolster privacy protections . . . ."[9] Although the trial court did not reach this argument, the Western District of the Court of Appeals did: "Because the Fourth Amendment is already being interpreted to protect electronic communications and data, we conclude that article I, section 15, even as amended, is not currently measurably more restrictive on the government than is the Fourth Amendment."[10]

This analysis will argue that the Western District was correct: Amendment Nine should have no more than expressive effect because current Fourth Amendment jurisprudence at the federal and state levels already extends to electronic data and communication. The real controversy in this area exists in the application of third party doctrine of Fourth Amendment jurisprudence. The courts have established a relatively well developed third party doctrine, but there remains a controversy over how to determine when data has been voluntarily given to a third party carrier. Part of this controversy might lead to the adoption of a different rule for collecting real-time or prospective data and communications as opposed to historic or stored data and communications. Amendment Nine offers no help to Missouri in resolving this controversy.

Part I explores the motives for Amendment Nine and the debate surrounding it. Because the third party doctrine is why electronic data and communication is often not protected, Part II introduces and describes that doctrine. Part III describes the state of Missouri law prior to Amendment Nine. Part IV examines some of the principal electronic data and electronic technologies before reviewing the vanishing "circuit split" surrounding the application of third party doctrine to cases involving third party collection of cell site location information (CSLI). Part V refines the controversy to determine what Missouri's options in handling such a case might be. Part VI shows that Amendment Nine will not help Missouri decide this controversy.

I. PASSAGE OF AMENDMENT NINE

A. Amendment Nine was motivated by concerns regarding widespread use of newer technologies

Use of electronic data and electronic communications has become ubiquitous in twenty-first century America. According to the United States Census Bureau, as of 2013, nearly 85% of households in the United States "reported computer ownership," and nearly 75% of households had home

9. *Id.*

10. *Charter Commc'ns, Inc.*, 461 S.W.3d at 857–58.

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

internet access.[11] The Pew Research Center reports that in January 2014, 90% of American adults owned a cell phone, 58% of adults owned a smart phone, and 42% of adults owned a tablet computer.[12] In 2013, there were an estimated 833 million Twitter accounts, with new accounts registering at a rate of over one million per month.[13] In 2010, there were over 133 million Facebook subscribers in the United States.[14] And we Americans use our data generating and transmitting technology constantly. Of the cited Twitter accounts, 233 million were "monthly active users."[15] In 2014, 71% of online adults used Facebook, while growing numbers of them used competing social media.[16] Daily, or even hourly, we create, store, and transmit electronic data about nearly every aspect of our lives.[17]

Along with our unprecedented use of technology that creates, stores, and transmits data comes concern for protection of that data from government intrusion. As Justice Sotomayor observed in her concurring opinion in *United States v. Jones*, previously restraints on law enforcement information gathering came from "limited police resources and community hostility" rather than constitutional limits.[18] New technologies make possible, for example, inexpensive, unobtrusive, and continuous, long-term tracking of a vehicle's movements in public places.[19] Without the physical restraints, and without some change in Fourth Amendment jurisprudence, the vast amounts of information people emanate nearly non-stop (and often without specific user awareness) might be accessible to law enforcement.[20] Concern for protection

11. Thom File & Camille Ryan, *Computer and Internet Use in the United States: American Community Survey Reports*, U.S. CENSUS BUREAU (Nov. 2014), http://www.census.gov/content/dam/Census/library/publications/2014/acs/acs-28.pdf [http://perma.cc/J3KA-VYZH].

12. *Mobile Technology Fact Sheet*, PEW RES. CTR., http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ [http://perma.cc/D8MJ-TTAE] (last visited Mar. 28, 2015).

13. Jim Edwards, *Twitter's 'Dark Pool': IPO Didn't Mention 651 Million Users Who Abandoned Twitter*, BUS. INSIDER (Nov. 3, 2013), http://www.businessinsider.com/twitter-total-registered-users-v-monthly-active-users-2013-11 [http://perma.cc/58WG-8YA2].

14. *United States of America Internet and User Stats*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats26.htm [http://perma.cc/T5ZJ-CT65] (last visited Mar. 28, 2015).

15. Edwards, *supra* note 13.

16. Maeve Duggan et al., *Social Media Update 2014*, PEW RES. CTR. (Jan. 9, 2015), http://www.pewinternet.org/2015/01/09/social-media-update-2014/ [http://perma.cc/ZG49-V2EX].

17. *E.g.*, Kathryn Nobuko Horwath, *A Check-In on Privacy After United States v. Jones: Current Fourth Amendment Jurisprudence in the Context of Location-Based Applications and Services*, 40 HASTINGS CONST. L.Q. 925, 925–26 (2013) (describing just a portion of the information a typical person distributes via Twitter, Facebook, etc. throughout a typical day).

18. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

19. *Id.* at 955–56.

20. *E.g.*, Horwath, *supra* note 17, at 925–26 (describing just a portion of the information a typical person distributes via Twitter, Facebook, and Foursquare throughout a typical day).

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

of this data from government searches grew dramatically following Edward Snowden's revelation in June of 2013 that the National Security Administration was collecting in bulk cell phone metadata.[21]

B. The debate focused on whether Amendment Nine would have any effect, and not on whether it was a good or bad idea in itself

In Missouri, this concern brought together a wide range of organizations in support of Amendment Nine: from liberal to libertarian and beyond.[22] Proponent organizations included the Missouri American Civil Liberties Union, the Missouri Libertarian Party, the Missouri NAACP, and the Tenth Amendment Center (TAC).[23] TAC claims Amendment Nine is part of a broader agenda aimed at nullification of federal law (that is, promoting states' rights).[24] TAC is a member of OffNow, a coalition promoting model legislation aimed at state non-cooperation with federal authorities.[25] OffNow also sees Amendment Nine (what it calls the "Electronic Data Privacy Act") as a stepping stone to nullification laws aimed at restraining federal surveillance practices.[26] More mainstream thinkers perceive the need for a state role in

21. Barton Gellman, *NSA Surveillance: The Architecture; Four-Pronged U.S. Approach Relies Heavily on Data Behind Internet, Phone Communications*, WASH. POST, June 16, 2013, at A1; Tobias T. Gibson, *Why Amendment Nine Matters*, COLUMBIA DAILY TRIB., Aug. 17, 2014, http://www.columbiatribune.com/opinion/oped/why-amendment-matters/article_3d3d0e9e-17f5-5008-8a89-8b4f3276e543.html [http://perma.cc/LQ34-R5MA].

22. *Vote Yes on Amendment 9*, AM. CIV. LIBERTIES UNION OF MO., http://www.aclu-mo.org/legislation/2014-privacy-bills/vote-yes-on-amendment-9/ [http://perma.cc/2MEG-Z8TK] [herein after ACLU-MO] (last visited Mar. 28, 2015).

23. *Id.*

24. *Vote to Nullify: Five States, Seven Ballot Measures*, TENTH AMEND. CTR., http://tenthamendmentcenter.com/2014/11/03/vote-to-nullify-five-states-seven-ballot-measures/ [http://perma.cc/6X66-GZ9F] (last visited Mar. 28, 2015).

25. *Standing Together Against the Surveillance State*, OFFNOW, http://www.offnow.org/coalition [http://perma.cc/67EZ-XLUK] (last visited Mar. 28, 2015). Another blogger writes,

> The only lasting hope for freedom from government consolidation of all power is the refusal by states to enforce or participate in any federal program not specifically authorized by the contract that created that power in the first place— the Constitution. Lawmakers in Missouri are to be applauded for their effort to enforce the terms of the contract that created federal authority in the first place.

He supports Amendment Nine in part because he feels that relying on the courts to protect us from government intrusion is a bad idea. Joe Wolverton, II, *Amendment to Missouri Constitution Would Protect Digital Communication*, THE NEW AM. (June 25, 2014), http://www.thenewamerican.com/usnews/constitution/item/18558-amendment-to-mo-constitution-would-protect-digital-communication [http://perma.cc/96L7-KMFC].

26. *See Model Legislation*, OFFNOW, http://www.offnow.org/legislation [http://perma.cc/3JDT-XHMA] (last visited Mar. 28, 2015).

protecting or extending Fourth Amendment protections in the light of new technology.[27]

What little opposition there was to Amendment Nine suggested that it was unnecessary or would not have an effect.[28] Most of these opponents point to *Riley*. The *St. Louis Post-Dispatch* (hereafter the "*Post*") said Amendment Nine was "the least bad" of the amendments on the August ballot.[29] The *Post* opposed the change because it believed the Supreme Court (presumably in *Riley*) already offered the same protections and that it would "rather see this issue dealt with at the federal level."[30] Other opponents included: *West Plains Daily Quill*, citing *Riley* explicitly;[31] the *News Tribune*, claiming "a statewide amendment is insufficient to address ever-expanding technologies, communications and privacy issues;"[32] the *Joplin Globe*, pointing to "costly, burdensome legal challenges that tie up the court system" in response to unnecessary constitutional amendments;[33] The *Columbia Daily Tribune*, pointing to *Riley* to claim the amendment is "redundant" and would just be "clutter;"[34] and *The Kansas City Star*, saying the amendment has a good intent but there has been "too little discussion about the potential consequences" and they would rather see the subject "more thoroughly explored by the courts and in legislative debate before it is enshrined in the Missouri constitution."[35]

27. ACLU-MO, *supra* note 22; Gibson, *supra* note 21; Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 373–74, 393–94 (2006).

28. "Opponents do not castigate the amendment as potentially harmful, only that it is an unnecessary, 'feel-good' state policy likely to be superseded by federal law." Editorial, *Our Opinion: Amendment Won't Be Final Word on Digital Privacy Issue*, NEWS TRIB., July 31, 2014, http://www.newstribune.com/news/news/story/2014/jul/31/our-opinion-amendment-wont-be-final-word-digital-p/438004/ [http://perma.cc/6VQX-3DK6].

29. Editorial, *Just Vote No, No, No, No and No*, ST. LOUIS POST-DISPATCH, Aug. 3, 2014, at A18.

30. *Id.*

31. Frank L. Martin, Editorial, *Amendment 9 Is Unnecessary*, WEST PLAINS DAILY QUILL (Aug. 1, 2014), http://www.westplainsdailyquill.net/opinion/editorials/article_5c5277c8-1999-11e4-8dc4-0017a43b2370.html [http://perma.cc/36E9-G6JJ].

32. Editorial, NEWS TRIB., *supra* note 28.

33. Editorial, *Our View: No Need for No. 9*, JOPLIN GLOBE (July 29, 2014), http://www.joplinglobe.com/opinion/editorials/our-view-no-need-for-no/article_f3c48511-a3f9-5f1a-86f1-012cc003a5d4.html [http://perma.cc/Y42V-4SKT].

34. Henry J. Waters, III, Editorial, *Amendments: Cluttering the Constitution*, COLUMBIA DAILY TRIB. (July 27, 2014), http://www.columbiatribune.com/opinion/the_tribunes_view/amendments/article_236e5a28-110f-564a-b46e-c230342ddb14.html [http://perma.cc/WA53-9PLF].

35. Tammy L. Jungblad, Editorial, *Vote "No" on Gun and Data Questions in Missouri*, THE KANSAS CITY STAR, (June 23, 2014), http://www.kansascity.com/opinion/editorials/article591383.html [http://perma.cc/QK5B-G5B2].

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

Some less than enthusiastic supporters echoed some of the less than enthusiastic opponents because they believe Amendment Nine was harmless, even if it was likely unnecessary and ineffective.[36]

C. Riley *is irrelevant*

Proponents responded to the claim that *Riley* mooted Amendment Nine by pointing out that *Riley*'s holding was limited to the warrantless search of a cell phone seized directly from a person incident to arrest.[37] *Riley* made no other new pronouncements on questions concerning Fourth Amendment protection for electronic data and electronic communications. While the opinion contained the observation that a cell phone was analogous to other electronic devices, such as cameras, desktop and laptop computers, tablets, flash drives, and so on,[38] that the Fourth Amendment protected data stored on such devices was not a new holding.[39] Perhaps more significantly, *Riley* made no holding on third party search doctrine.[40] Its only addition to protection of electronic data was limited to the question of whether a cell phone can be searched incident to an arrest under one or another exception.[41]

36. The *Sullivan Journal*, for example, recommended a "yes" vote but considered the matter resolved by *Riley*. Editorial, *Say "No" to Amendment 7 and Amendment 1 Right to Farm*, SULLIVAN J. (Aug. 3, 2014), http://www.sullivanjournal.com/editorial/article_56fa7ad8-1b0f-11e4-a3a4-0017a43b2370.html [http://perma.cc/A9MA-NN5N].

37. *E.g.*, *Frequently Asked Questions About Amendment 9*, ACLU-MO, http://www.aclu-mo.org/legislation/2014-privacy-bills/vote-yes-on-amendment-9/frequently-asked-questions-about-amendment-9/ [http://perma.cc/RRH3-QG5V] (last visited Mar. 28, 2015).

38. Riley v. California, 134 S. Ct. 2473, 2489 (2014) ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

39. The fact that such electronic data falls under Fourth Amendment protection is generally assumed. For example, in *City of Ontario, Cal. v. Quon*, the Supreme Court resolved a Fourth Amendment challenge to the search of a police officer's text message on government-owned pagers. The analysis did not depend on the idea that the mere fact that it was electronic data somehow put it beyond the scope of the Fourth Amendment, but rather depended on the fact that the texts were work-related and were stored on pagers owned by the city. City of Ontario, Cal. v. Quon, 560 U.S. 746, 750–51, 764–65 (2010).

40. *Riley* broached this issue by observing that it may be difficult to discern what data is stored on the cell phone and what is stored remotely, on a "cloud" server, for example, and merely accessed via the cell phone. However, the case only addressed the question of searching the data *from the phone* seized incident to arrest, and did not address the question of getting that same data somehow from the third party that stored a copy of it. In fact, the government conceded that there was no *Chimel* exception that allowed for the warrantless search of that remotely stored data. That is, the government only wanted to search data stored exclusively locally on the cell phone. *Riley*, 134 S. Ct. at 2491.

41. *Id.* at 2485–89, 2494–95.

Furthermore, *Riley* did not touch at all on the topic of electronic communications, treating the cell phone simply as the repository of stored data.[42] However, since at least 1967, the Supreme Court has recognized Fourth Amendment protection for electronic communications.[43] In *Katz*, police installed a device on the outside of a public phone booth that allowed them to listen to the suspect's phone conversation.[44] The Court rejected the older rule that defined Fourth Amendment violations as only those involving a trespass into a constitutionally protected place, famously holding, "the Fourth Amendment protects people, not places."[45] The two-part *Katz* test, recognizing Fourth Amendment protection when there is both an actual or subjective expectation of privacy, and society recognizes that expectation as reasonable,[46] extended Fourth Amendment protection to the suspect's telephone conversation, which is a form of electronic communication.

Thus, although proponents were correct in pointing out that *Riley* was not relevant to the Amendment Nine debate, they were wrong in assuming that electronic data and electronic communications were not already subject to Fourth Amendment protection.[47]

II. THIRD PARTY DOCTRINE

A. The Rule

As we will see, Fourth Amendment protection from "first party" searches of electronic data and communications has long been recognized in Missouri under the Fourth Amendment and coextensively under Missouri's Constitution. The third party doctrine, which says that a person has no expectation of privacy, and therefore no Fourth Amendment interest, in information voluntarily given to a third party[48] is the reason collection of electronic data and communications often falls outside Fourth Amendment protections. Put simply, a person has no reasonable expectation of privacy regarding what he or

42. *But see supra* note 40.

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

44. *Id.* at 348.

45. *Id.* at 351.

46. *Id.* at 361 (Harlan, J., concurring); Smith v. Maryland, 442 U.S. 735, 740 (1979).

47. That proponents made this assumption is clear from Amendment Nine's ballot language: "Shall the Missouri Constitution be amended so that the people shall be secure in their electronic communications and data from unreasonable searches and seizures *as they are now likewise secure in their persons, homes, papers and effects*?" BALLOTPEDIA, *supra* note 1 (emphasis added).

48. *Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

she exposes to the public or voluntarily gives to another.[49] Stephen Henderson considers this a blanket rule of federal Fourth Amendment jurisprudence:

> [A]s interpreted by the United States Supreme Court, the [Fourth] Amendment places no restriction on police combing through your financial records; your telephone, e-mail, and website transactional records; and your garbage left for collection. Instead "third party information," meaning all information provided to third parties, receives no Fourth Amendment protection. Hence your very movements, be they tracked via a police transponder placed on your vehicle or via your mobile phone, are seemingly available to police without any Fourth Amendment limitation.[50]

Jennifer Arner points out that with regard to e-mail, therefore, the difference between using Post Office Protocol 3 (POP3, which stores messages locally and deletes them from the mail server) and Internet Message Access Protocol (IMAP, which leaves messages on the server) is the difference between having and not having Fourth Amendment protection available.[51]

However, when the third party is an "intermediary" or "carrier," not all of the data is considered voluntarily given to that third party carrier.[52] Orin Kerr suggests it is helpful to analogize to third party doctrine dealing with physical things so that our rules are technology-neutral.[53] He argues that non-content information is like the outside of letters and packages given to the third party carrier.[54] The Ninth Circuit has noted:

> [i]n a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on

49. In a way, this question is similar to the question of "standing" in Fourth Amendment jurisprudence. Fourth Amendment rights are personal rights and cannot be asserted vicariously. *E.g.*, Rakas v. Illinois, 439 U.S. 128, 133 (1978). For example, an employee had no expectation of privacy of the contents of a computer owned by his employer. State v. Faruqi, 344 S.W.3d 193, 204–05 (Mo. 2011). That these two doctrines overlap is apparent from the following hypothetical: police illegally enter my friend's house and seize a letter I wrote and mailed to my friend. I have no standing to suppress that letter as evidence against me because I have no reasonable expectation of privacy in the letter I voluntarily gave to a third party and because I have no standing to challenge the illegal entry of my friend's house.

50. Henderson, *supra* note 27, at 373.

51. Jennifer Arner, *Looking Forward by Looking Backward:* United States v. Jones *Predicts Fourth Amendment Property Rights Protections in E-Mail*, 24 GEO. MASON U. C.R. L.J. 349, 349–50 (2014).

52. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("NuVox was an *intermediary*, not the intended recipient of the emails.").

53. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1022–23 (2010).

54. *Id.*

> the outside of mail, because that information is voluntarily transmitted to third parties.[55]

In *Smith v. Maryland*, back in the days when most homes had landline telephones, the Supreme Court examined the question of whether installation of a pen register is a Fourth Amendment search.[56] A pen register is a device installed at the telephone company that captures phone numbers dialed by a given telephone but does not intercept the conversation or content of the call.[57] The Court distinguished the case from *Katz* on that very content/non-content distinction, holding that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[58]

When the third party is an "intermediary" or "carrier" of information to another recipient, only the "outside" or "non-content" data is considered voluntarily given to the carrier third party. The *content* is still protected by the Fourth Amendment with respect to the third party carriers. The content is, however, voluntarily given to the third party *recipient* who is free to turn it over to law enforcement. Another way courts have explained essentially the same distinction is to consider which data the third party carrier needs to receive from the subscriber to provide its service—the sort of data it needs and normally stores as part of conducting its business.[59]

B. The assumption underlying Amendment Nine ignores the third party rule

A great deal of the electronic data and communications motivating proponents of Amendment Nine involve the third party rule: information uploaded to internet servers, information transmitted to cell phone service providers, location data broadcast by a vehicle's OnStar system, and so on. When dealing with physically recorded information (which easily fit into the constitutionally-protected categories "papers" or "effects"), there is normally little doubt as to when we have voluntarily given the information to another or made it available to the public. As we will see, the question of when we

55. United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008).

56. Smith v. Maryland, 442 U.S. 735, 736 (1979).

57. *Id.* at 736 n.1.

58. *Id.* at 741.

59. *Id.* at 743 ("Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."). Also note: the business record approach illustrates why the fact that the user has no Fourth Amendment interest leads to the idea that the government can compel disclosure by the third party carrier under the lesser standard of the SCA. The data as a business record is owned by the phone company, but it has no privacy interest in it—unlike trade secrets or personnel records. In other words, the user cannot vicariously assert property interests in the data, and the entity with property interests has no privacy interest in it.

voluntarily give electronic data to a third party is a more controversial question.[60] However, the distinction between information that is and is not protected by the Fourth Amendment does not depend on whether the information is in electronic or physical form, but rather on whether or not the person has exposed it to another or the public in general.[61] Amendment Nine wrongly assumes that electronic data and communications were not previously protected. More specifically, it assumes that differences in protection can be remedied by the inclusion of the terms "electronic data" and "electronic communications" in the list of constitutionally protected areas. This assumption ignores the fact that the difference in protection stems largely from the workings of the third party rule and not from whether the information is in electronic form.

III. MISSOURI LAW PRIOR TO AMENDMENT NINE

A. Missouri Constitution Article I, Section 15 offers protections that are "coextensive" with Fourth Amendment protections

The Fourth Amendment provides a floor.[62] States can offer greater protections, but cannot cut into or decrease the Fourth Amendment right.[63] States vary in how they treat their own constitutional protections as compared to the Fourth Amendment protection.[64] The variation is perhaps best treated as a continuum: at one extreme are states that treat their constitutional protection as remaining coequal and in lockstep with federal Fourth Amendment

60. *See infra* Part V.A; *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010) [hereinafter *Third Circuit CSLI Case*].

61. *E.g.*, Alderman v. United States, 394 U.S. 165, 172–73 (1969) (holding that seizure of narcotics from a third party did not violate the defendant's Fourth Amendment rights); United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that under the third party doctrine, the Fourth Amendment did not prohibit seizure of defendant's cancelled checks, deposit slips, and microfilm duplicates from the banks, but detailing some statutory protection).

62. *See* Supremacy Clause, U.S. CONST. art. VI; *see* Mapp v. Ohio, 367 U.S. 643, 655 (1961) (holding that the Fourth Amendment is enforceable against the states under the Due Process Clause of the Fourteenth Amendment by implementation of the exclusionary rule); Irma S. Raker, *Fourth Amendment and Independent State Grounds*, 77 MISS. L.J. 401, 401 (2007).

63. The Constitution of Michigan, for example, has in addition to a nearly identically worded analog of the Fourth Amendment this sentence: "The provisions of this section shall not be construed to bar from evidence in any criminal proceeding any narcotic drug, firearm, bomb, explosive or any other dangerous weapon, seized by a peace officer outside the curtilage of any dwelling house in this state." MICH. CONST. art. I, § 11. The Sixth Circuit held this provision to be in conflict with the Fourth Amendment and therefore invalid. Lucas v. Michigan, 420 F.2d 259, 263 (6th Cir. 1970).

64. *See generally* Henderson, *supra* note 27; Michael J. Gorman, *Survey: State Search and Seizure Analogs*, 77 MISS. L.J. 417 (2007).

jurisprudence.[65] Interpretation of the state constitutional protection changes in exact synchrony or "lockstep" with changes in Fourth Amendment jurisprudence.[66] At the other extreme are states that explicitly afford greater protections above and beyond the Fourth Amendment floor.[67] In between are states in "limited lockstep" who recognize the right to treat their constitutions as affording greater protections, but who have employed that right in only extremely limited circumstances if at all.[68] There is not always a correlation between having virtually identical wording in the state's Fourth Amendment analog and viewing the protection as the same.[69]

Missouri is solidly at the first end of the spectrum. Missouri courts have long held that Article I, Section 15 rights are "coextensive" with Fourth Amendment rights, and that "the same analysis applies."[70] Missouri has never found a greater protection in the state constitution than in the Fourth Amendment. Missouri is certainly free to break its long history and amend its constitution in a way that provides greater privacy protections than offered in the Fourth Amendment,[71] but will Amendment Nine have that effect? Indeed, Missouri courts have continued to recite the "coextensive" and "the same analysis applies" mantra even in decisions issued after the passage of Amendment Nine, however most of these cases did not involve electronic data and communications.[72] The Western District has explicitly addressed the issue

65. *E.g.*, People v. Caballes, 851 N.E.2d 26, 41 (Ill. 2006) (describing and reviewing the literature on the "lockstep" doctrine).

66. *Id.*

67. *E.g.*, Washington's constitution offers greater protections. WASH. CONST. art. I, § 7; Gorman, *supra* note 64, at 461–62.

68. *E.g.*, North Dakota's Fourth Amendment analog has been interpreted to *allow* the state to offer greater protections, but the state has not done so. Gorman, *supra* note 64, at 448.

69. *E.g.*, Indiana's analog is virtually identical to the Fourth Amendment, yet the courts have held that the analysis is not the same, and that the state offers greater protections. Jon Laramore & Daniel E. Pulliam, *Indiana Constitutional Developments: Small Steps*, 47 IND. L. REV. 1015, 1029 (2014); McIlquham v. State, 10 N.E.3d 506, 511 (Ind. 2014) ("Our State constitutional provision, 'although almost identical in text to its federal counterpart, nevertheless requires a different analysis. . . .'").

70. *E.g.*, State v. Rushing, 935 S.W.2d 30, 34 (Mo. 1996); State v. Lovelady, 432 S.W.3d 187, 190 (Mo. 2014).

71. *Rushing*, 935 S.W.2d at 34.

72. Most of these cases explicitly recited that the federal and state constitutional protections are "coextensive" and that the "same analysis applies." *E.g.*, State v. Walker, 460 S.W.3d 81, 85 (Mo. Ct. App. 2015). Some of them made no mention of the Missouri constitutional provision at all, but conducted the review based solely on the Fourth Amendment. *E.g.*, State v. Spires, ED 101279, 2014 WL 5839734, at *2 (Mo. Ct. App. Nov. 12, 2014). Fewer recited that both constitutional provisions are involved, and while not explicitly saying how the two are related implying the analysis is the same by conducting only one analysis. *E.g.*, State v. Nunez, 455 S.W.3d 529, 531 (Mo. Ct. App. 2015).

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

and held that even with Amendment Nine's added language, the Missouri Constitution offers no greater protections than the Fourth Amendment.[73]

B. Missouri case law prior to Amendment Nine already recognized protection for electronic data and communications and already recognized and limited the third party rule

Missouri already recognized protection in "first party" searches of electronic data.[74] That is, if the person does not voluntarily give the data to a third party, there is no doubt that the contents of cell phones, computers, digital cameras, storage media, etc. were already protected to the same degree as "persons, homes, papers, and effects."

In *State v. Oliver*, for example, police officers seized the defendant's computer, computer data storage disks, digital camera, and camera data card based on the defendant's wife's consent following the defendant's refusal to give consent to the search of his home office.[75] Two weeks later, police searched the electronically stored contents of these items under a search warrant.[76] The court held that even if the wife's consent was invalid, the evidence found from searching the contents of these items was admissible either due to the inevitable discovery doctrine or because the bad seizure did not invalidate the search warrant.[77] All of this reasoning is based on the presumption that the electronic data stored on these devices is protected to the same degree by pre-Amendment Nine Article I, Section 15 and the Fourth Amendment. That is, the police either needed valid consent or an exception to the warrant requirement to search the electronically stored data on these items.

In *State v. Sachs*, the court held that the police officer's act of merely clicking an icon to bring to view a currently running but minimized application on a desktop computer lawfully seized by police was a search under the Fourth Amendment and the Missouri Constitution.[78] In *Sachs*, the police officer lawfully seized the defendant's then-running desktop computer in the

73. State *ex rel* Koster v. Charter Commc'ns, Inc., 461 S.W.3d 851, 857–58 (Mo. Ct. App. 2015) ("Because the Fourth Amendment is already being interpreted to protect electronic communications and data, we conclude that article I, section 15, even as amended, is not currently measurably more restrictive on the government than is the Fourth Amendment.").

74. *See* State v. Oliver, 293 S.W.3d 437, 443 (Mo. 2009).

75. *Id.* at 440.

76. *Id.*

77. *Id.* at 442, 443–44 ("The officers did not obtain a warrant to search the office and seize the items; rather, the detective conducted the search and seizure based on Oliver's wife's consent. The validity of this consent does not affect the admissibility of the items because had the detective not relied on the consent, he would have discovered this evidence pursuant to a search warrant. . . . The initial seizure did not affect the validity of the warrant obtained to search these items.").

78. State v. Sachs, 372 S.W.3d 56, 61 (Mo. Ct. App. 2012).

defendant's home.[79] The screen showed a running word processor program, but the officer could see the minimized icon indicating that other applications were running, including what he recognized as a bit-torrent client application.[80] The defendant refused to consent to a search of the contents of the computer, and the officer clicked on the icon without waiting for a search warrant.[81] The court, relying on a Ninth Circuit case that held that merely moving the mouse to "wake up" a computer screen was a search, ruled that the officer's actions constituted a search under Missouri and federal constitutional law.[82] Again, the reasoning in *Sachs* depends on the idea that the electronic data on the computer is subject to the same Fourth Amendment protections as "persons, homes, papers, and effects" even before Missouri added "electronic data" to the list.

Furthermore, the "coextensive" treatment applies to "electronic communications" as well. Missouri is bound by *Katz*, which is a case that clearly recognized Fourth Amendment protections for electronic telephone communications.[83]

In *State v. Clampitt*, Missouri recognized the third party doctrine and limited its application to "outside" or non-content information.[84] This case involved the collection of data from the defendant's cell phone carrier to use as evidence that would place the defendant at the location of a motor vehicle accident.[85] The court held that text messages stored on the defendant's cell phone were protected, even though the messages were also accessible by the phone service provider.[86] This holding echoes what *Riley* said about data stored on the cloud but accessible on the phone, but deals with a fact set involving law enforcement's attempt to obtain that information from the third-party phone service provider. The *Clampitt* court recognized the third party rule from *Smith v. Maryland*, but based its reasoning in limiting that rule largely on a Sixth Circuit case, *United States v. Warshak*.[87] *Warshak* recognized protection for the *content* of e-mails accessible or in the possession of an Internet Service Provider (ISP).[88] *Warshak* makes clearer the distinction between what we hand over to a third party *recipient* and a third party carrier,

79. *Id.* at 59.

80. *Id.*

81. *Id.* at 60.

82. *Id.* at 61, 63.

83. *E.g.*, State v. Bates, 344 S.W.3d 783, 787 (Mo. Ct. App. 2011) (applying the two-part *Katz* reasonable expectation of privacy test); s*ee supra* text accompanying note 43 (observing *Katz* protects electronic communications).

84. State v. Clampitt, 364 S.W.3d 605, 610 (Mo. Ct. App. 2012).

85. *Id.* at 607–08. To clarify, this information was text message content providing location, not cell tower information or CSLI.

86. *Id.* at 611.

87. *Id.* at 610–11.

88. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

or what it refers to as an "intermediary."[89] The Sixth Circuit analogizes e-mail to traditional mail that passes through the hands of a number of letter carriers after we entrust it to the Post Office.[90] The Missouri court adopted this reasoning to hold that the content of text messages were analogous to the content of e-mail, which *Warshak* found analogous to the contents or insides of a letter, and thus the third party rule was not applicable.[91]

IV. ELECTRONIC DATA AND COMMUNICATIONS TECHNOLOGIES AND THE VANISHING "CIRCUIT SPLIT" IN APPLYING THIRD PARTY DOCTRINE TO CSLI CASES

A. The technology in CSLI collection

As we will see, the facts in these CSLI cases vary somewhat, but what they all have in common is that law enforcement obtained data from the cell phone service provider that includes information allowing them to determine—to a greater or lesser degree of precision[92]—the location of the cell phone and therefore the person carrying the cell phone.[93] These cases rely on the fact that in order for the company to provide cell phone services, the phone must carry on two-way communication with nearby "base stations" also known as "cell towers."[94] Most cell towers have several antennae (or "cell sectors" or "cell sites") oriented in different directions.[95] Towers provide connectivity within a

89. *Id.* at 285.

90. *Id.* Professor Kerr would approve of this sort of analogy because analogizing between electronic data and communications and physical things helps make rules that are "technology neutral." Kerr, *supra* note 53, at 1007.

91. *Clampitt*, 364 S.W.3d at 611.

92. On the one hand are those who argue that it only provides crude location primarily due to the often wrong assumption that the tower with which the phone establishes a connection is the nearest. If the nearest tower has a high volume of traffic, the phone will connect to the next nearest, and so on. It is possible to connect to a tower as far as twenty miles away. Douglas Starr, *What Your Cell Phone Can't Tell Police*, THE NEW YORKER, June 26, 2014, http://www.newyorker.com/news/news-desk/what-your-cell-phone-cant-tell-the-police [http://perma.cc/38R7-83ZT]. On the other hand, an expert gave testimony at Congressional hearings that although location precision varies, it can provide "locational precision similar to that of GPS." ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 81–85, 93–94 (2010), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg57082/pdf/CHRG-111hhrg57082.pdf [http://perma.cc/7ZWA-Y7SW].

93. For a nice summary of how the technology works, see *In re* Application for Tel. Info. Needed for a Criminal Investigation, 15XR90304HRL1LHK, 2015 WL 4594558, at *1–3 (N.D. Cal. July 29, 2015) [hereinafter *N.D. Cal. CSLI Case*].

94. *Id.* at *1.

95. *Id.*

"cell," the hexagonal area covered by that tower.[96] The CSLI can be generated and recorded when the user places a call or sends or receives a text message or other communications.[97] In others, it is the result of a "ping" either initiated by the phone service provider (that is, sent out from the tower[98]) or initiated by the phone itself.[99] For example, whenever a user first turns on a cell phone, the phone pings nearby towers in order to establish a connection with the nearest available tower and look for missed calls and text messages, update the date and time settings, and conduct any other automatic communications.[100] An example of such an automatic communication is an app running continuously in the background that alerts the user of sports scores, weather information, and so on.[101] When the cell phone is moving, as when the user is driving down the highway, it will periodically ping towers in order to maintain the best possible connection.[102] In high traffic areas, such as urban centers, effective cells are generally very small and CSLI is more precise.[103] Finally, whenever the user places or receives a call or message in real time, the phone communicates with the tower, and the service provider obtains and records the "outside" or "non-content" information it needs to provide the service.[104] It

96. *See* Robert D. Keith, *How Cell Phones Work*, INTERACTIVE MEDIA LAB, U. OF FLA., http://iml.jou.ufl.edu/projects/fall04/keith/Works.htm [http://perma.cc/F5GT-KHWG] (last visited Mar. 28, 2015); *See, e.g.*, United States v. Caraballo, 963 F. Supp. 2d 341, 347–48 (D. Vt. 2013); Marshall Brain et al., *How Cell Phones Work*, HOW STUFF WORKS, http://electronics.howstuffworks.com/cell-phone1.htm [http://perma.cc/U9QF-QJQZ] (last visited Mar. 28, 2015).

97. *N.D. Cal. CSLI Case*, 2015 WL 4594558, at *1.

98. *Id.* at *2 ("Pinging is automatic and occurs whenever the phone is on, without the user's input or control.") (citing U.S. Dep't of Homeland Sec., Lesson Plan: How Cell Phones Work 9 (2010), http://www.eff.org/files/filenode/3259_how_cell_phones_work_lp.pdf [http://perma.cc/D6HJ-M9SL]); *e.g.*, State v. Hosier, 454 S.W.3d 883, 890 n.4 (Mo. 2015), *reh'g denied* (Mar. 31, 2015), *cert. denied*, 136 S. Ct. 37 (2015).

99. *N.D. Cal. CSLI Case*, 2015 WL 4594558, at *2.

100. *See id.*; Keith, *supra* note 96; Marshall Brain et al., *How Cell Phones Work*, HOW STUFF WORKS, http://electronics.howstuffworks.com/cell-phone3.htm [http://perma.cc/6HKD-T7RL] (last visited Mar. 28, 2015).

101. *iPhone 3g Commercial "There's an App for That 2009,"* YOUTUBE (Feb. 4, 2009), http://www.youtube.com/watch?v=szrsfeyLzyg [http://perma.cc/3X68-26NW].

102. *N.D. Cal. CSLI Case*, 2015 WL 4594558, at *2 ("[C]ell phones periodically identify themselves to the closest cell tower—i.e., the one with the strongest radio signal—as they move throughout their network's coverage area.").

103. United States v. Davis, 785 F.3d 498, 542 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015) ("As a person walks around town, particularly a dense, urban environment, her cell phone continuously and without notice to her connects with towers, antennas, microcells, and femtocells that reveal her location information with differing levels of precision—to the nearest mile, or the nearest block, or the nearest foot.").

104. Orin Kerr, *Eleventh Circuit Rules for the Feds on Cell-Site Records—But Then Overreaches*, WASH. POST: VOLOKH CONSPIRACY (May 5, 2015), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/05/eleventh-circuit-rules-for-the-feds-on-cell-site-records-but-then-overreaches/ [http://perma.cc/5D72-48K5] ("Cell tower location records do not

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

acts as an intermediary or carrier to "inside" or "content" information transmitted to others.

In some of these cases, law enforcement sought historic data: the stored records of past calls, usually to "place" a suspect near the scene of the crime; in others, law enforcement obtained the information prospectively, essentially tracking the movement of the cell phone in real time.[105] Also, some of the cases are reviews of orders granted under the Stored Communications Act, and some are challenges to the refusal of a magistrate to grant the order, or challenges to the authority of the magistrate to grant such an order before it has been issued.[106]

Generally, CSLI locates the cell phone because the location of the tower is known, and any phone that communicates with a particular tower must be within that tower's cell—that is, it must be near enough to connect. Therefore, location is within the cell size. CSLI can include data as to which direction from the cell tower the phone was, based on which directionally-oriented antenna on the tower was used.[107]

Some cell phone service providers also use and record another type of location information: Per Call Measurement Data (PCMD).[108] PCMD relies on a measure of the time it takes a signal to travel between the phone and the tower to calculate the distance between the two.[109] PCMD is created and recorded for calls, text messages, and other data transmissions.[110] PCMD was originally generated and recorded to help service providers track dropped calls and reposition tower antennae to minimize signal loss.[111] Not all carriers generate and record this information, and those that do only preserve it for a week or two.[112] PCMD can provide better evidence of a cell phone's location,

contain private communications of the subscriber. This type of non-content evidence, lawfully created by a third-party telephone company for legitimate business purposes, does not belong to Davis, even if it concerns him.").

105. *See infra* Part IV.D.

106. These procedural distinctions are not relevant to this analysis, so will be treated cursorily.

107. *N.D. Cal. CSLI Case*, 2015 WL 4594558, at *1 (describing a typical tower with three antennae oriented such that each antennae covers an area within the cell swept out by a 120-degree arc).

108. AARON EDENS, CELL PHONE INVESTIGATIONS™: NARCOTICS OPERATIONS 17 (2012), http://policetechnical.com/wp-content/uploads/2012/04/Cell-Phone-Conference-Narcotics.pdf [http://perma.cc/Q8XC-9PUD].

109. *Id.*

110. *Id.*

111. *Id.*

112. *Id.* at 18–19; Senior Member, *Per Call Measurement Data*, FORENSIC FOCUS: FOR DIGITAL AND EDISCOVERY PROFS. (Jan. 25, 2011), http://www.forensicfocus.com/Forums/viewtopic/t=7122/ [http://perma.cc/LP27-FSTN].

but still not as accurate as GPS.[113] PCMD may be treated as distinct from CSLI.[114]

B. Why CSLI?

In examining the effectiveness of Amendment Nine, it is necessary to see what kind of current controversies the state faces before determining whether Amendment Nine will help Missouri in any way. The terms "electronic data" and "electronic communications" encompass all sorts of technologies that might involve government collection of information, especially from third parties. Furthermore, the intention was surely broader than the technical meaning of these terms.[115] So why choose CSLI as a test for the effectiveness of Amendment Nine?

Since any good third party rule should be technology-neutral,[116] cases involving any of these technologies should yield the same result. Even though the choice is therefore ultimately arbitrary, a quick look at the other likely candidates shows that CSLI is best for in-depth testing of the effect of Amendment Nine because it is the hottest topic (in terms of having the most federal appellate level opinions) that the Missouri Constitution could likely reach.

113. EDENS, *supra* note 108, at 17–18.

114. State v. Ford, 454 S.W.3d 407, 410–11 (Mo. Ct. App. 2015) ("PCMD was different from the cell tower data, because it measured the radio frequency distance between the telephone and nearby towers, and gave an estimate of the location of the telephone itself during the call.").

115. Strictly speaking, data on CDs and DVDs is stored optically, not electronically. *See, e.g.*, Jeff Tyson, *How Removable Storage Works: Optical Storage*, HOW STUFF WORKS, http://computer.howstuffworks.com/removable-storage7.html [http://perma.cc/Q5JQ-TJJU] (last visited Dec. 18, 2015); Inst. for Local Self-Reliance, *Fiberoptic Networks*, COMMUNITY BROADBAND NETWORKS, http://muninetworks.org/content/fiber-optic-network [http://perma.cc/CKR8-ZKD5] (last visited Dec. 18, 2015). Most familiar "electronic" storage media are magnetic media, though physically magnetism and electricity are interrelated. Jeff Tyson, *How Removable Storage Works: Magnetic Storage*, HOW STUFF WORKS, http://computer.howstuffworks.com/removable-storage2.htm [http://perma.cc/Y9BQ-8PFY] (last visited Dec. 18, 2015); *Electricity and Magnetism*, RON KURTUS' SCH. FOR CHAMPIONS, http://www.school-for-champions.com/electricity.htm [http://perma.cc/GXY2-PDDZ] (last visited Dec. 18, 2015). Development of biological storage media is underway. Sebastian Anthony, *Harvard Cracks DNA Storage, Crams 700 Terabytes of Data Into a Single Gram*, EXTREMETECH (Aug. 17, 2012), http://www.extremetech.com/extreme/134672-harvard-cracks-dna-storage-crams-700-terabytes-of-data-into-a-single-gram [http://perma.cc/MT5N-Q277]; *see also* W. DANIEL HILLIS, THE PATTERN ON THE STONE: THE SIMPLE IDEAS THAT MAKE COMPUTERS WORK, at VIII (1998) (explaining that data storage and manipulation—computers—"transcend[] technology" and could even be made with "valves and water pipes, or from sticks and strings").

116. Kerr, *supra* note 53, at 1007.

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

1. Global Positioning System (GPS) and Other Electronic Tracking

A GPS device receives signals from government-owned satellites.[117] These satellites broadcast their ephemerides (information about the satellite's location in the sky at any moment) along with a precise time stamp.[118] The receiving device uses this information to calculate by trilateration its position on the Earth's surface converted by the device to traditional latitude and longitude coordinates.[119] To be used as a tracker, a GPS device must either store or, as in the *Jones* case, transmit that location data to law enforcement.[120]

In *Knotts*, police used a simple radio beeper as a tracking device.[121] This gadget simply broadcasts a radio signal that helps police follow the suspect's vehicle from a greater distance and with less risk of losing the suspect than a conventional police "tail."[122] The familiar holding from *Knotts* is that a person has no reasonable expectation of privacy in his movements on public roadways.[123]

In *Jones*, police used a GPS tracking device to monitor the vehicle's movements over nearly a one-month period.[124] Jones argued a version of the Mosaic Theory, but the majority decision of the Court disposed of the issue based on the trespass rule: when police trespass on one of areas enumerated in the Fourth Amendment for the purpose of collecting information, they violate the Fourth Amendment.[125] Some of the concurring opinions accepted a "long term Katz" test or Mosaic rule.[126]

117. *The Global Positioning System: What Is GPS?*, GPS.GOV, http://www.gps.gov/systems/gps/ [http://perma.cc/QTH9-2KG2] (last visited Mar. 23, 2015).

118. *GPS Signals*, WIKIPEDIA, http://en.wikipedia.org/wiki/GPS_signals [http://perma.cc/6ZBS-W6HL] (last visited Mar. 23, 2015).

119. *Trilateration Exercise*, GPS.GOV, http://www.gps.gov/multimedia/tutorials/trilateration/ [http://perma.cc/8D73-YSFV] (last visited Mar. 23, 2015); *Global Positioning System*, WIKIPEDIA, http://en.wikipedia.org/wiki/Global_Positioning_System#Fundamentals [http://perma.cc/AS65-JRC9] (last visited Mar. 23, 2015).

120. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 948 (2012) ("By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer."); Chris Hoffman, *HTG Explains How GPS Actually Works*, HOW-TO GEEK (Feb. 21, 2013), http://www.howtogeek.com/137862/htg-explains-how-gps-actually-works/ [http://perma.cc/4TES-K9UB] ("GPS tracking devices don't just use GPS receivers—they store the GPS data for later retrieval or transmit the GPS data.").

121. United States v. Knotts, 460 U.S. 276, 277 (1983).

122. *Id.* at 278–79.

123. *Id.* at 281 ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

124. *Jones*, 132 S. Ct. at 946.

125. Orin Kerr, *Does Fourth Amendment Standing Work Differently for* Jones *Trespass Searches, Traditional* Katz *Searches, and Long-Term* Katz *Searches?*, VOLOKH CONSPIRACY (Feb. 14, 2012), http://volokh.com/2012/02/14/does-fourth-amendment-standing-work-different

Most smartphones are also GPS devices.[127] Other data, such as street maps and navigation apps are provided by other service providers.[128] This GPS location information is not required by the phone company to provide its services.[129] The phone company, in providing cell phone service, does not normally receive and store GPS data. The phone company *acting as an intermediary* might transmit that data to other service providers (for use in a street navigation app, for example). The phone can function as a GPS device even without communicating to any cell phone towers.[130] I would distinguish GPS data from CSLI by characterizing the GPS data as "content" or "inside" data that is not voluntarily given to the cell phone service provider. In this way it is the same as the content of a phone conversation, and should be protected by the Fourth Amendment.

Most dedicated GPS devices, like Garmins or TomToms, are strictly receivers and not transmitters.[131] Other tracking devices, such as LoJack, involve voluntarily conveying the information to law enforcement; in other words, the service provided *is* turning the information over to police.[132]

Even this cursory look at GPS and other trackers indicates that Amendment Nine will be no help.

2. Remote Data Storage

This category includes explicit third party storage services such as Microsoft Cloud, Google Drive, DropBox, and IMAP e-mail (Internet Mail Access Protocol, that is web based e-mail).[133] What these have in common is

ly-for-jones-trespass-searches-traditional-katz-searches-and-katz-long-term-expectation-of-privacy-searches/ [http://perma.cc/8JYX-D6QB].

126. *Id.*; *e.g.*, *Jones*, 132 S. Ct. at 964 (Sotomayor, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

127. *See* Eric A. Taub, *What Stand-Alone GPS Devices Do That Smartphones Can't*, N.Y. TIMES, July 15, 2015, at B7, http://www.nytimes.com/2015/07/16/technology/personaltech/what-stand-alone-gps-devices-do-that-smartphones-cant.html [http://nyti.ms/1Hvwt6C].

128. *See, e.g.*, *Latest Navigation*, ANDROID FREEWARE, http://www.androidfreeware.net/tag-navigation.html [http://perma.cc/3CX5-KYDT] (last visited Aug. 23, 2015) (listing several free service providers and app download links for android devices).

129. That is, you can disable the GPS feature on a cell phone and the device will still function as a cell phone, including data services other than GPS. *E.g.*, *How to Turn Off GPS on the iPhone*, WIKIHOW, http://www.wikihow.com/Turn-off-GPS-on-the-iPhone [http://perma.cc/68E3-EBY5] (last visited Dec. 14, 2015).

130. Christopher Null, *We Tested 4 GPS Apps That Work Even When You're Offline*, WIRED (Apr. 6, 2015), http://www.wired.com/2015/04/offline-gps-apps/ [http://perma.cc/5U2B-9QE7].

131. Hoffman, *supra* note 120 ("GPS on its own isn't a privacy concern—for example, if you have an old GPS unit for your car, it likely isn't capable of transmitting your location.").

132. *How LoJack Works*, http://www.lojack.com/Cars,-Trucks-And-Classics/How-LoJack-Works [http://perma.cc/4K8X-ZX3H] (last visited Dec. 15, 2015).

133. *See* Joe Kissell, *Backup Basics: The Quick Something-Is-Better-Than-Nothing Backup System*, MACWORLD (Nov. 6, 2012), http://www.macworld.com/article/2013004/backup-basics-

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

that data is stored either exclusively in third party storage accessible by a user interface on a local device, or simultaneously in both locations. The third party doctrine would apply to "content" or "inside" data, but not to outside or non-content.[134] This is the equivalent of putting effects in a self-storage locker. The fact that you used a storage locker (the terms of your contract with the self-storage company which might include the rental period, the size of the locker, etc.) is non-content or outside information, analogous to the exterior of an envelope or parcel sent via the mail, and therefore should be accessible to police without implicating the Fourth Amendment. The distinction between content and non-content might not be so clear-cut because some typically non-content information might convey content.[135] In my self-storage analogy, that would be like sizes of boxes and individual labels on those boxes inside a storage locker. I would argue that police can only get the overall outside data—nothing they would have to open the locker to obtain. In cloud storage, that means only that the user has an account and what the overall storage size available to you is. If they start looking at file names, types, and sizes, they have opened the locker door and started looking at characteristics of the contents, even if they have yet to open any sealed boxes.

In *Riley*, the Supreme Court treated in dicta a different question, the problem of data accessible via a local device that is stored remotely.[136] The Court said that viewing remote data on the device would be "like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock

the-quick-something-is-better-than-nothing-backup-system.html [http://perma.cc/9QWC-ACBT]; Sanebox, Inc., *The Differences Between POP and IMAP*, POP2IMAP, http://www.pop2imap.com/ [http://perma.cc/ZJD8-GVVA] (last visited Dec. 18, 2015).

134. Kerr, *supra* note 53; Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004) ("Several courts have applied this rationale and held that an Internet user does not retain a reasonable expectation of privacy in noncontent information disclosed to an ISP."). *But see* United States v. Warshak, 631 F.3d 266, 283 (6th Cir. 2010) (noting that the SCA allows the government to obtain e-mail content that has been left on the e-mail server more than 180 days without a warrant). This *Warshak* holding might have to do with a theory that something abandoned has been exposed, possibly the basis of the rule regarding searching an opaque trash container left on the curb for trash collection. *See* California v. Greenwood, 486 U.S. 35, 55 (1988) (finding a distinction between trash in an opaque container for trash pickup and a package or envelope left for mail pickup in holding that there is a reasonable expectation of privacy in the contents of the latter but not the former).

135. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2123–44, 2150, 2167 (2009) (noting that file names, e-mail and file size, e-mail headers, etc. might reveal content); United States v. Borowy, 595 F.3d 1045, 1049 (9th Cir. 2010) (finding in the context of a plain view argument under *Hicks* that visible file names made evident that the files were probably illegal child pornography image files) (applying Arizona v. Hicks, 480 U.S. 321, 324–26 (1987) (holding that the doctrine requires the illicit nature of the thing seized to be apparent by sight without further manipulation)).

136. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

and search a house."[137] This implies that the reverse is also a search under the Fourth Amendment: that is, if police are not permitted to search the device without a warrant, the fact that the same content is also stored remotely (in the possession of a third party) does not obviate the need for a warrant. This rule makes sense because this data is "content" (i.e. not information voluntarily conveyed to the third party) and would not be available without a warrant even from the third party. Therefore, nothing about the third party doctrine would change the principal holding in *Riley* that police may not obtain the contents of a cell phone in a search incident to arrest without a warrant except in vanishingly rare exigent circumstances.[138]

Again, Amendment Nine will not help resolve any controversies in this category.

3. Wi-Fi Location Information

Mobile devices that have Wi-Fi capability can also calculate their position based on information about Wi-Fi access points.[139] It is used as an alternative to GPS, for example, in some Kindle Fire models.[140] A federal district court examined this location method along with the other "geolocation" methods (notably GPS and CSLI) for calculating the location of a mobile device.[141] Like GPS, this data is calculated by an app on the local device and can be shared with third party app service providers.[142] Unlike CSLI, it is not

137. *Id.*

138. *Id.* at 2485, 2494 (holding that such vanishingly rare circumstances as "a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone" were absent in the case at bar and that otherwise digital content did not comprise exigent circumstances).

139. Fred Zahradnik, *Wi-Fi Positioning System*, ABOUT TECH (Dec. 4, 2014), http://gps.about.com/od/glossary/g/wifi_position.htm [http://perma.cc/YZ39-VL2B]. A recent case in federal district court dealt with patent infringement claims on the various technologies involved in calculating location this way. Skyhook Wireless, Inc. v. Google, Inc., CIV.A. 10-11571-RWZ, 2014 WL 898595, at *1 (D. Mass. Mar. 6, 2014). Mozilla Location services blends CSLI and Wi-Fi location technologies. *Overview*, MOZILLA LOCATION SERVS., http://location.services.mozilla.com/ [http://perma.cc/C9BG-MLR5] (last visited Dec. 18, 2015).

140. *Device and Feature Specifications*, AMAZON, http://developer.amazon.com/appsandservices/solutions/devices/kindle-fire/specifications/01-device-and-feature-specifications [http://perma.cc/88HC-TW6Z] (last visited Dec. 18, 2015).

141. *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 137 (E.D.N.Y. 2013).

142. *Location Services FAQ*, AMAZON, http://www.amazon.com/gp/help/customer/display.html/ref=hp_terms_us?nodeId=201604200 [http://perma.cc/XR5P-JUUG] (last visited Dec. 18, 2015). Since Amazon can also collect and use this data for providing services to Kindle users, while other times it merely relays the data to other service providers, Amazon is sometimes a third party carrier/intermediary and sometimes a third party recipient. *See id.* Also note that Kindles equipped with 4G (cell phone) connectivity can also use CSLI to calculate their position. *Id.*

information normally calculated and stored by the phone company to provide its services. Furthermore, like GPS but not CSLI, Wi-Fi location services can be disabled by the user, and stored data can be deleted by the user.[143] Owners of Wi-Fi access points can also disable location information being collected by Google for Wi-Fi location purposes.[144] I would argue that Wi-Fi location information falls under the same category as GPS data when transmitted via the phone company to another recipient. That is, it should count as content, especially since it can be disabled without destroying the functionality of the device, and thus not something voluntarily given to the third party carrier/intermediary (the phone company). The dearth of Fourth Amendment cases involving this technology is probably due to the fact that use of these devices is not as ubiquitous as is the use of cell phones.

4. Data Conveyed to an Internet Service Provider (ISP)

When a user enters a web address into a web browser, is that information analogous to the numbers dialed on a telephone in *Smith v. Maryland*? If so, then most of the litigation in this area will happen under the statutory protections rather than the Fourth Amendment.[145] But there is still controversy over that point.[146] I suspect there is less litigation on this point because law enforcement normally seeks a warrant (or its equivalent, supported by probable cause) for information sought from ISPs since at least much of the information of interest will be content. At any rate, clearly Amendment Nine will offer no help in making the critical distinction in making the third party doctrine analysis in these cases.

5. National Security Agency (NSA) Collection of Phone Call Metadata

Since Edward Snowden leaked the existence of a widespread NSA program collecting cell phone call metadata, this category has been a hot topic.[147] At any rate, this is not a good test for Missouri's Amendment Nine

143. *E.g.*, *id.* (instructing Kindle Fire users how to disable Wi-Fi location services and how to delete location history). The fact that Kindle Fire users with Wi-Fi location services can disable location services, argues that it is not information Amazon must collect and store in order to provide services (in this case, the service is allowing the user to purchase and display e-books, audiobooks, movies, games, and so on).

144. Zahradnik, *supra* note 139 ("Simply add '_nomap' to the name of the Wi-Fi network, and Google will not map it.").

145. *E.g.*, *In re* Zynga Privacy Litig., 750 F.3d 1098, 1108–09 (9th Cir. 2014) (holding that since such information "does not constitute the contents of a communication," distinctions needed to resolve the case fell entirely under the E.C.P.A.).

146. Tokson, *supra* note 135, at 2167; United States v. Forrester, 512 F.3d 500, 510 n.6 (9th Cir. 2008) (observing in dicta that URLs might be content for Fourth Amendment purposes).

147. *E.g.*, Charlie Savage, *Judge Deals a Blow to N.S.A. Data Collection Program*, N.Y. TIMES, Nov. 9, 2015, at A17, http://www.nytimes.com/2015/11/10/us/politics/judge-deals-a-blow-to-nsa-phone-surveillance-program.html [http://perma.cc/33SB-8F5T]; Klayman v. Obama, CV

since the Missouri Constitution will likely not find any application to NSA practices.[148]

6. Cell Site Emulators ("Triggerfish" and "Stingray")

This category refers to devices made by the Harris Corporation used by law enforcement to spoof a cell tower in order to obtain the location and identity of cell phones.[149] The existence and use of these devices by law enforcement had been classified.[150] In fact, the secrecy meant law enforcement was unable to bring evidence gathered this way to trial, bargaining down charges[151] and even dismissing charges altogether[152] rather than subjecting the technology to court scrutiny. Therefore, there are few cases to look at in this category.

I would argue that the third party doctrine applies, and the key distinctions have to be between content and non-content data. It seems strange to put this under third party doctrine since the device allows police to intercept radio waves directly from the cell phones and not rely on cell phone company records. However, the frequencies used for cell phones are exclusive use

13-851 (RJL), 2015 WL 6873127, at *1 (D.D.C. Nov. 9, 2015); Obama v. Klayman, 800 F.3d 559, 561 (D.C. Cir. 2015).

148. Despite allegations that the NSA is sharing this data with state and local law enforcement for use in criminal prosecutions, Michael Maharrey, *Surprise: NSA Apologist Opposes Missouri Amendment 9 Ballot Measure*, OFFNOW (July 1, 2014), http://offnow.org/surprise-nsa-apologist-opposes-missouri-amendment-9-ballot-measure/ [http://perma.cc/8TXJ-NVZX] ("We know that the NSA expressly shares warrantless data with state and local law enforcement through a super-secret DEA unit known as the Special Operations Division (SOD). We know that state prosecutors use the information in criminal cases."), I have found no Missouri or other state cases where prosecution attempted to use such data as evidence. On the contrary, in a recent Missouri case, the defendant hoped to use CSLI to prove his alibi defense, but the phone company had already destroyed the data. The defendant tried, apparently without success, to get the NSA metadata under a Freedom of Information Act (FOIA) request. State v. Moore, 469 S.W.3d 512, 514–15 (Mo. Ct. App. 2015).

149. Jennifer Valentino-Devries, *"Stingray" Phone Tracker Fuels Constitutional Clash*, WALL ST. J., Sept. 22, 2011, http://www.wsj.com/articles/SB10001424053111904194604576583112723197574 [http://perma.cc/L2NQ-CPPF]; EDENS, *supra* note 108, at 20.

150. EDENS, *supra* note 108, at 20. These devices were the subject of a Freedom of Information Act Lawsuit. Am. Civil Liberties Union of N. Cal. v. Dep't of Justice, 70 F. Supp. 3d 1018, 1022–23 (N.D. Cal. 2014).

151. Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASH. POST (Feb. 22, 2015), http://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html [http://perma.cc/F9SY-PMYN].

152. Robert Patrick, *Controversial Secret Phone Tracker Figured in Dropped St. Louis Case*, ST. LOUIS POST-DISPATCH, Apr. 19, 2015, at A1, http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_fbb82630-aa7f-5200-b221-a7f90252b2d0.html [http://perma.cc/SRL3-6W3H].

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

licenses.[153] By contrast, Citizen's Band (CB) radio frequencies are "licensed by rule" meaning that anyone who owns a transceiver can use the frequencies.[154] Although the frequencies used by cell phones are still public airwaves, the phone companies paid the government for the right to exclusive use of certain frequencies in certain geographic areas.[155] Therefore, radio waves sent from a cell phone to a tower are in the possession of the cell phone company the instant they leave the phone. While there may be further statutory limitations on how police can use these devices, the Fourth Amendment analysis should only depend on whether they are gathering content or non-content information.

At the time of this writing, because the technology was kept secret, there are few cases involving cell tower emulators. At any rate, it is plain that Amendment Nine will provide no help in resolving this key area of controversy.

7. Miscellaneous

Other types of data storage and communications that implicate Fourth Amendment concerns are nearly endless: Radio Frequency Identity (RFID) chips, removable media drives, etc. In a case out of New Mexico, the Tenth Circuit faced the question of whether police officers reading data off magnetic strips on credit cards without a warrant violated the Fourth Amendment.[156]

153. *What Is Licensed Spectrum*?, SELECT SPECTRUM, http://selectspectrum.com/Spectrum.html [http://perma.cc/Q4QY-8Q86] (last visited Dec. 18, 2015) ("Commercial operators including . . . mobile phone companies . . . acquire protection from interference in the form of FCC spectrum licenses which provide for exclusive use and protection from interference in specific areas."); Kimberly M. Randolph, *Spectrum Licenses: Valuation Intricacies*, STOUT, RISIUS, ROSS GLOBAL FIN. ADVISORY SERVS., http://www.srr.com/article/spectrum-licenses-valuation-intricacies [http://perma.cc/3RM6-QPYQ] (last visited Dec. 18, 2015) ("Examples of exclusive use licenses include cellular mobile . . . ").

154. *Citizens Band (CB) Service*, FCC.GOV, http://www.fcc.gov/general/citizens-band-cb-service [http://perma.cc/G4A4-R3PQ] (last visited Dec. 18, 2015) ("The CB Service is licensed by rule."); 47 C.F.R. § 95.404 (2009) (specifying no individual license is required to use CB).

155. *Cellular Service*, FCC.GOV, http://www.fcc.gov/general/cellular-service [http://perma.cc/V3JL-4BHH] (last visited June 14, 2015); *Accessing Spectrum*, FCC.GOV, http://www.fcc.gov/general/accessing-spectrum [http://perma.cc/TG3C-2ZCX] (last visited June 14, 2015) (describing exclusive licensing in geographic areas for commercial use); David McCabe, *Five Biggest FCC Stories of 2015*, THE HILL (Dec. 20, 2015), http://thehill.com/policy/technology/263788-five-biggest-fcc-stories-of-2015 [http://perma.cc/EN3K-KUPL] (describing plans by the FCC to buy back spectrum from broadcasters and auction it to cell phone providers); Alan Holmes, *Wireless Companies Fight for Their Futures*, CTR. FOR PUB. INTEGRITY (Mar. 21, 2014), http://www.publicintegrity.org/2014/03/21/14433/wireless-companies-fight-their-futures [http://perma.cc/5TTR-HZ4S] (describing fierce competition among cell phone companies for frequencies auctioned by the government).

156. United States v. Alabi, 597 Fed. App'x 991, 993 (10th Cir. 2015). The court ultimately did not decide the issue, reasoning that even if there was a Fourth Amendment violation, the

These cases often do not implicate third party doctrine at all, and there are few cases of any one type of technology. CSLI cases, by contrast, are numerous.[157]

C. Statutory Protections

In most of these cases, law enforcement acted under the belief that collection of the data in question falls outside the Fourth Amendment and therefore is not a search. In 1986, in response to cases like *Smith*, Congress attempted to provide statutory protections beyond Fourth Amendment protections, with the Electronic Communications Privacy Act (ECPA).[158] A brief description of these statutory protections will be helpful in understanding some of the cases that comprise the cell phone location data controversy.

The ECPA includes three portions: The Pen Register Act, the Wire Tap Act, and the Stored Communications Act (SCA).[159] The Pen Register Act and the SCA offer limited protections for this type of electronic information voluntarily given to third parties (usually the telephone or internet service provider). The SCA allows law enforcement to obtain a court order compelling the third party to turn over that data with a showing of reasonable suspicion.[160] More specifically, the SCA says that police can compel the third party carrier to turn over non-content information[161] without the customer's consent[162] and without giving the customer notice[163] either by obtaining a warrant in the normal way which requires a showing of probable cause,[164] by obtaining a court order under the lesser standard of "specific and articulable facts,"[165] with no requirement of showing anything when the data is limited to specific metadata,[166] and finally by formal request when the data is relevant to an

evidence was admissible under the inevitable discovery exception to the exclusionary rule. *Id.* at 998.

157. *See infra* Part IV.0.

158. Kerr, *A User's Guide*, *supra* note 134, at 1209–13. While Arner says the ECPA was a response to *Katz*, she notes that it was not enacted until eighteen years after *Katz*. Arner, *supra* note 51, at 358.

159. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2520 (2012); Arner, *supra* note 51, at 359.

160. 18 U.S.C. § 2703(d) (2012).

161. *Id.* § 2703(c).

162. *Id.* § 2703(c)(1)(C).

163. *Id.* § 2703(c)(3).

164. *Id.* § 2703 (c)(1)(A).

165. 18 U.S.C. § 2703(c)(1)(B) (2012) (referring to the standard in §2703(d)).

166. *Id.* § 2703(c)(1)(E) (referring to the list of specific data given in § 2703(c)(2)). That list includes only the name and address of the account holder (as given by the account holder, something not necessarily verified by the company, especially when the cell phone is a pre-paid type obviating the need for a credit check), call metadata (connection time, duration of call), subscriber's phone number (or account number or other such subscriber ID), and, upon obtaining a grand jury or trial subpoena or any of the other means described in this section (that is, warrant, consent, court order on "specific and articulable facts," or with notice to the subscriber), the

investigation in a telemarketing fraud case defined elsewhere in the Chapter.[167] Furthermore, violations of the SCA are not necessarily enforceable by excluding the evidence gained.[168] The Pen Register Act requires only a showing that the information is relevant to an investigation for installing pen registers which collect just one type of third party data: telephone numbers to and from which calls are made.[169]

Since the ECPA offers lower protections, the third party doctrine is hugely important in determining whether electronic data transmitted by cell phones gets Fourth Amendment protection. Analysis should begin by determining whether or not law enforcement's conduct falls inside or outside of the Fourth Amendment. In these cases, this determination invariably depends on whether or not the third party doctrine applies. If the third party doctrine applies, and it is not a Fourth Amendment search, then the court should then proceed to see whether law enforcement complied with statutory requirements.

D. The Cases

1. Historic

As recently as late 2015, more than a year after Amendment Nine's passage,[170] there was an arguably legitimate circuit split on the question of the collection of historic CSLI without a warrant. While there is still some controversy over details, the rule is that collection of CSLI records is not a

method of payment information, including credit card or bank account numbers. *Id.* Other than the payment information, this is the "metadata" collected by the NSA.

167. *Id.* § 2703(c)(1)(D) (referring to § 2325).

168. Kerr points to "the absence of a statutory suppression remedy" as one of several "[d]ichotomies and ambiguities" in the SCA. Kerr, *A User's Guide*, *supra* note 134, at 1224.

169. 18 U.S.C. § 3121 generally prohibits pen register and trap and trace without a court order as provided in § 3123. Section 3123 allows for a court order when the information is relevant to an ongoing criminal investigation.

170. That is, before the Eleventh Circuit vacated its panel opinion in *Davis* and then reached the opposite decision on this issue en banc, and before the Fourth Circuit vacated its decision in *Graham* for an en banc decision, which is currently pending. United States v. Davis, 754 F.3d 1205 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 Fed. App'x 925 (11th Cir. 2014) and *on reh'g en banc in part*, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015); United States v. Graham, 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015); *see also* Orin Kerr, *Fourth Circuit Grants Rehearing, Eliminates Split, on Cell-Site Surveillance*, WASH. POST: VOLOKH CONSPIRACY (Oct. 29, 2015), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/10/29/fourth-circuit-grants-rehearing-eliminates-split-on-cell-site-surveillance/ [http://perma.cc/DRR5-BGTV]; United States v. Daniels, 803 F.3d 335, 351 (7th Cir. 2015) (referring to "this circuit split" characterized by the Fourth Circuit's opinion in *Graham* on the one side, and the Fifth and Eleventh Circuit opinions on the other).

search under the Fourth Amendment.[171] The only remaining circuit split is over one of these peripheral questions. The following is a chronological description of some of the key circuit court cases.

In 2010, the Third Circuit issued a confused opinion in a case involving collection of historic CSLI.[172] The court held that collection of historic CSLI is not protected by the Fourth Amendment and therefore the analysis proceeds under the SCA.[173] But in construing the statute, the court held that the statute provides the option of either obtaining a warrant by a showing of probable cause or obtaining an order by showing "specific and articulable facts," and that this choice means the magistrate was not *required* to grant the order upon the lesser showing.[174] However, the concurrence would limit the magistrate judge's discretion to require probable cause to just two situations: (1) where the government has failed to provide the lesser standard given in the applicable part of the SCA, or (2) where the magistrate judge finds that the order would violate the Fourth Amendment by providing location data within the interior or curtilage of the suspect's home.[175] So the analysis seems to be back under the Fourth Amendment. The court found the third party doctrine not applicable because the site information is not "voluntarily" given to the third party since most users are not aware location information is collected and stored.[176] At any rate, the Third Circuit held that it was within the judge's discretion to require probable cause, but it also indicated that law enforcement only had to provide reasonable suspicion under the SCA.[177]

In 2013, the Fifth Circuit explicitly applied the third party rule by holding that "cell site information is clearly a business record."[178] This is data "[t]he cell service provider collects and stores . . . for its own business purposes" and not sent from the user to convey to a recipient that is "anyone other than his service provider."[179] Therefore, the cell phone user has no Fourth Amendment protection for this data, and the provisions in the SCA are adequate.[180] The

171. *In re* United States for Historical Cell Site Data, 724 F.3d 600, 614–15 (5th Cir. 2013) [hereinafter *Fifth Circuit CSLI Case*].

172. *Third Circuit CSLI Case*, 620 F.3d 304 (3d Cir. 2010).

173. *Id.* at 313 ("[W]e hold that CSLI from cell phone calls is obtainable under a § 2703(d) [of the SCA] order and that such an order does not require the traditional probable cause determination. . . .").

174. *Id.* at 319.

175. *Id.* at 320 (Tashima, J., concurring).

176. *Id.* at 317 ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."). The court goes on to assert, "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information." *Id.*

177. *Third Circuit CSLI Case*, 620 F.3d at 313.

178. *Fifth Circuit CSLI Case*, 724 F.3d 600, 611 (5th Cir. 2013).

179. *Id.* at 611–12.

180. *Id.* at 615.

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

court rejected that the user does not voluntarily give the information to the provider.[181] The Fifth Circuit explicitly disagreed with the Third Circuit in holding that the SCA leaves no room for the magistrate judge to require probable cause once the SCA requirements are met.[182] In response to the idea that we should change the third party doctrine to reflect the ease and ubiquity of data collection due to changes in technology, the court noted that this was outside the Fourth Amendment, and thus the realm of the legislature, which has already acted in creating the SCA.[183]

In 2014, the Eleventh Circuit held "that cell site location information is within the subscriber's reasonable expectation of privacy. The obtaining of that data without a warrant is a Fourth Amendment violation."[184] It rejected the applicability of third party doctrine holding that the Fourth Amendment protects "not only content, but also the transmission itself when it reveals information about the personal source of the transmission, specifically his location."[185] The court asserted as a conclusion without support that users do not voluntarily give their location information to cell phone carriers.[186] However, the Eleventh Circuit vacated this decision, and decided the case en banc in 2015. [187] In its en banc opinion, the Eleventh Circuit found collection of CSLI was not a search under the Fourth Amendment due to the third party

181. *Id.* at 612. The court supported this conclusion in several ways. First, the information is given voluntarily for the simple fact that one is free not to use or possess a cell phone. *Id.* at 613. Second, it responded to the argument that only the phone numbers actually dialed, as in *Smith*, are outside the content protected by the Fourth Amendment, calling this a "crabbed understanding of voluntary conveyance" that would "lead to absurd results." *Id.* For example, if phones are preprogrammed to dial the number automatically (as with speed dial, or simply "call" under a phone book entry), then even the numbers the phone company needs to complete the call would somehow be treated as not voluntarily conveyed. *Id.* Also, users are generally aware of when they are out of range of towers. *Id.* Furthermore, coverage areas and how many bars customers get are frequent subject matter of marketing campaigns. Not only are customers generally aware, it is often the reason they choose a given carrier. *E.g.*, *AT&T Commercial—Across the Nation*, YOUTUBE (Mar. 29, 2009), http://www.youtube.com/watch?v=8c_nrA_BUz4 [http://perma.cc/6FWP-TCQJ] (advertising "more bars in more places"—a huge marketing campaign suggesting cell phone customers are generally aware of the importance of signal strength and availability for providing cell phone service). Finally, the court notes that subscribers agree to a contract, which includes terms regarding the disclosure of this information and the carrier's privacy policy. *Fifth Circuit CSLI Case*, 724 F.3d at 613.

182. *Fifth Circuit CSLI Case*, 724 F.3d at 607.

183. *Id.* at 614–15.

184. United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*, 573 Fed. App'x 925 (11th Cir. 2014).

185. *Id.* at 1213, 1216.

186. *Id.* at 1216–17.

187. United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc).

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

doctrine, and even if it was a search, it is a reasonable one when law enforcement satisfies the requirements of the SCA.[188]

In August of 2015, the Fourth Circuit held that the warrantless collection of a vast amount of CSLI was a violation of the Fourth Amendment.[189] The court reasoned that the third party doctrine did not apply because cell phone users do not voluntarily give their location information to the phone company.[190] The court explained that the user does not convey the information because the phone company itself generates CSLI.[191] In October of 2015, the Fourth Circuit vacated this opinion for hearing en banc.[192] The case is schedule for oral argument in March of 2016.[193]

Other circuit courts have disposed of cases without having to decide this issue.[194] We can only glean hints of which way those circuits would have gone had they reached the issue.[195]

2. Real-Time/Prospective

In 2012, in *United States v. Skinner*, the Sixth Circuit held that there was no Fourth Amendment protection for prospective CSLI because there was no reasonable expectation of privacy for location data given off by the cell phone.[196] This holding is despite the fact that the case involved several facts

188. *Id.* at 517–18.

189. United States v. Graham, 796 F.3d 332, 344–45 (4th Cir. 2015), *reh'g en banc granted*, 624 Fed. App'x 75 (2015) ("We hold that the government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical CSLI for an extended period of time.").

190. *Id.* at 353–55.

191. *Id.* at 356.

192. *Graham*, 624 Fed. App'x at 75.

193. *Id.*

194. *E.g.*, United States v. Thousand, 558 Fed. App'x 666, 672 (7th Cir. 2014) (noting that police provided probable cause in their SCA application anyway); United States v. Daniels, 803 F.3d 335, 352, 352 n.3 (7th Cir. 2015) (disposing of the issue because the defendant failed to preserve it by a motion to suppress and noting that even if the rule from the now-vacated *Graham* decision applied, officers relied on the SCA in good faith); Jayne v. Blunk, 502 Fed. App'x 641, 642 (9th Cir. 2012) (declining to reach the issue in a § 1983 case because police withdrew their order to turn over historic and real-time CSLI before the phone company responded); United States v. McCullough, 523 Fed. App'x 82, 83–84 (2d Cir. 2013) (disposing of the issue based on defendant's failure to timely move to suppress the CSLI evidence and, in a separate ineffective assistance of counsel argument, that officers' good faith reliance on the SCA meant the defendant was not prejudiced).

195. *E.g.*, *Thousand*, 558 Fed. App'x at 670 ("We have not found any federal appellate decision accepting [the defendant's] premise that obtaining cell-site data from telecommunications companies—under any factual scenario—raises a concern under the Fourth Amendment.").

196. United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012). Police obtained an order from a federal magistrate for prospective data on first one phone, then another, thus allowing police to track the defendant's movements in real time. *Id.* at 774–76.

that might tend toward a favorable outcome for the defendant: the order was prospective, rather than historic; the order included the collection of GPS data; and tracking included having the phone service provider initiate "continuous pings" to the phones.[197] The court did not invoke the third party rule; instead, it accepted that the phones functioned as tracking devices, and distinguished the case from *Jones* while analogizing to *Karo*.[198] The court also noted that even though otherwise lawful tracking becomes illegal when it is long-term or comprehensive (citing the *Jones* concurrences), law enforcement only tracked Skinner for three days so such a rule would not apply here anyway.[199]

In 2013, the Tenth Circuit disposed of a prospective CSLI case without reaching the issue of concern.[200] The court invoked the officers' good faith reliance on the court order that mistakenly authorized collection of prospective cell site location information.[201] The court unfortunately referred to pings initiated by the cell phone service provide at law enforcement's direction for purposes of locating the phone as "GPS pings" and CSLI as "GPS data."[202]

Finally, one state case involving real-time or prospective CSLI is worth mentioning. The Florida Supreme Court held that collecting such data requires a warrant based on probable cause.[203] Under the Pen Register Act, law enforcement obtained a pen register to capture numbers dialed on the suspect's cell phone.[204] Although officers did not request it, the phone company also provided them with historical and real-time CSLI.[205] Officers used this

197. *Id.* at 776.

198. *Id.* at 780–81. The court indirectly brought in third party doctrine when it likened movements in public to the phone numbers dialed in *Smith* in that there is no recognized reasonable expectation of privacy. *Id.*

199. *Id.* at 780.

200. United States v. Barajas, 710 F.3d 1102, 1109 (10th Cir. 2013), *cert. denied*, 134 S. Ct. 230 (2013).

201. *Id.* at 1109.

202. Based on the description of the process, the court simply meant CSLI generated by cell tower pings expressed in terms of latitude and longitude coordinates. *Id.* at 1105 n.1. Latitude and longitude coordinates are not properly "GPS coordinates" since they were in use centuries before GPS technology. J.J. O'Connor & E.F. Robertson, *History Topic: Longitude and the Académie Royale*, MACTUTOR HIST. OF MATHEMATICS ARCHIVE, U. OF ST. ANDREWS, SCOTLAND (Feb. 1997), http://www-groups.dcs.st-and.ac.uk/~history/PrintHT/Longitude1.html [http://perma.cc/8GSW-KM64] ("Eratosthenes calculated the Earth's circumference and he was the first to attempt to produce a map of the World based on a system of lines of latitude and longitude."). GPS location information is not generated the same way CSLI is generated. *E.g.*, *How GPS Works*, GPS.GOV, http://www.gps.gov/multimedia/poster/ [http://perma.cc/HP5F-H9DX] (last visited Mar. 28, 2015).

203. Tracey v. State, 152 So. 3d 504, 507–08, 526 (Fla. 2014).

204. *Id.* at 507.

205. *Id.* at 507–08. In fact, the court order did specify historical CSLI, not requested by officers. *Id.* at 508 n.2.

information to track the suspect's movements and location.[206] Florida held that this was a search under the Fourth Amendment, and that the third party doctrine did not apply because cell phone users do not voluntarily give their location information for any purpose.[207]

Despite the current absence of a circuit split on the issue of CSLI, the minority position persists.[208]

V. REFINING THE CONTROVERSY: WHAT ARE MISSOURI'S LIKELY OPTIONS?

This section is meant to be a cursory look at Missouri's options and not an exhaustive treatment of the questions of "voluntary gives," prospective versus historic data collection, or the Mosaic Theory. In other words, the issues are refined only enough to determine whether Amendment Nine will be effective or helpful.

A. The vanishing "circuit split" is not a controversy whether the third party rule is applicable to electronic data at all but merely a question as to which data a person "voluntarily gives" to a third party carrier.

1. The Majority Position

Whether the third party doctrine applies in CSLI cases boils down to whether the data in question was voluntarily given to the phone service provider. Kerr points out the need to analyze this question by analogy to physical searches rather than developing a series of technology dependent rules which cannot anticipate unforeseeable technological developments.[209] The best

206. *Id.* at 508.

207. *Id.* at 522 ("While a person may voluntarily convey personal information to a business or other entity for personal purposes, such disclosure cannot reasonably be considered to be disclosure for all purposes to third parties not involved in that transaction.").

208. *E.g.*, *Commonwealth v. Wyatt*, CRIM. A. 2011-00693, 2012 WL 4815307, at *7 (Mass. Super. Aug. 7, 2012); *In re* Application for Tel. Info. Needed for a Criminal Investigation, 15-XR-90304-HRL-1(LHK), 2015 WL 4594558, at *12 (N.D. Cal. July 29, 2015); Brian L. Owsley, *Teaching Criminal Procedure—Especially on Fourth Amendment and Electronic Surveillance—to Everyone but Law Students*, 60 ST. LOUIS U. L.J. 507, 511 (2016).

209. Kerr, *supra* note 53, at 1021–22, 1030. An example of such a rule is the language in New York's Fourth Amendment analog, which enumerates "telephone and telegraph communication." N.Y. CONST. art. I, § 12. New York courts have found this language to have no effect (that is, they still hold their analog's protections to be in lockstep or limited lockstep with the Fourth Amendment, and have not relied on this "telephone and telegraph" language to be the basis for greater protections. If the language were effective, the provision would be long overdue for overhaul since the telegraph is wholly obsolete and "telephone" communication is very nearly a completely different technology than it was when the language was adopted. Gorman, *supra* note 64, at 447. Gorman notes that New York in fact has departed from Fourth Amendment jurisprudence (in some significant ways), *id.*, none of the "departures" have even a remote basis in the "telephone and telegraph communication" language.

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

analogy for data given to third party carriers is to physical letters or packages given to the Post Office or other carriers, such as FedEx. In the physical world, the distinction between content and non-content is the same as the distinction between inside and outside.[210] Part of the problem with the SCA is that it specifies different standards for content or non-content data without defining the terms.[211] It does list with great specificity the information that it considers to be metadata which is presumed wholly outside the Fourth Amendment.[212] But how can the courts tell whether or not Congress' presumptions were valid? What is a good test to distinguish content from non-content in the realm of CSLI?

According to the Fifth Circuit, the information is "voluntarily given" because using or carrying a cell phone at all is a voluntary matter, and cell phone users cannot reasonably claim not to be aware that the phone is effectively sending location information (inferable from knowing with which tower the phone communicates).[213] The court supported its conclusion that the data is given voluntarily.[214] For example, cell phone users should be aware of the fact that their phones must communicate with cell towers because "coverage" is part of cell phone service marketing.[215]

The Fifth Circuit also looks at the idea of the information being part of a business record. Although the court kept this analysis separate from the question of "voluntarily gives," it is really another way of looking at the same issue. Because this is information the business must collect, generate, and store to provide services, a person voluntarily contracting for those services voluntarily gives that data to the business.

2. The Minority Position

The Third Circuit seems to acknowledge that the third party doctrine is applicable to electronic data generally, but deems the action to be a Fourth Amendment search because data revealed the person's location in his home or curtilage.

The Third Circuit's reasoning is flawed. It muddies the waters by putting the question of whether or not the action is a search under the Fourth Amendment back inside construction of the SCA, when the statute should only

210. Kerr, *supra* note 53, at 1009–12, 1020–22 ("In the physical world, the inside/outside distinction strikes a sensible balance. It generally lets the government observe where people go, when they go, and to whom they are communicating while protecting the actual substance of their speech from government observation without a warrant unless the speech is made in a setting open to the public. The content/non-content distinction preserves that function.").

211. 18 U.S.C. § 2711 (2009) ("Definitions for chapter" fail to define "contents").

212. *Id.* § 2703(c)(2).

213. *Fifth Circuit CSLI Case*, 724 F.3d 600, 613 (5th Cir. 2013).

214. *Id.* at 614.

215. *See, e.g.*, *AT&T Commercial—Across the Nation*, *supra* note 181.

apply when there is no Fourth Amendment search. That is, the statute can only add *additional* protections, and cannot displace the Fourth Amendment. The proper analysis should begin with the determination of whether or not the third party doctrine applies, and therefore whether or not there is a Fourth Amendment search. Only if there is *not* a search is the SCA controlling (other than a likely good faith exception to the exclusionary rule because law enforcement relied on the statute). Put another way, if the third party doctrine applies and the action is therefore not a search under the Fourth Amendment, the fact that the information lies inside the home or curtilage cannot drag it back into the Fourth Amendment. Again, *Katz* said a person has no reasonable expectation of privacy in matters made known to others, even in the home or office.[216]

Furthermore, the Third Circuit and Eleventh Circuit panels made the relatively bald assertion that CSLI data is not voluntarily given. They seemed to rely on confusing "awareness" with the question of "voluntarily gives." While the Fifth Circuit makes a strong case that such knowledge is reasonable to infer, strictly speaking actual knowledge or awareness—especially at any given moment—is not required. Focusing on actual or subjective awareness this way would absurdly hamstring law enforcement even in long settled areas of physical searches. For example, that a criminal is genuinely unaware that his actions in his home or curtilage are readily observable from the public street is irrelevant in determining whether that observation constitutes a search.[217]

The Florida Supreme Court made a similarly confused argument. Construing the Fifth Circuit's analysis of "voluntarily gives" as a question of the purpose for giving the data to the third party, Florida then confused this notion of purpose with the question of consent to a search.[218] That is, whether one "voluntarily gives" location data to the carrier depends on whether one consents to law enforcement collecting that data.[219] Like the Third Circuit, Florida was asking questions that only apply when there is a search in order to determine whether or not there is a search; it was simultaneously reasoning inside and outside the Fourth Amendment.

216. Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

217. *See* Florida v. Riley, 488 U.S. 445, 450–52 (1989).

218. *Tracey v. State*, 152 So. 3d 504, 522 (Fla. 2014).

219. *Id.* ("While a person may voluntarily convey personal information to a business or other entity for personal purposes, such disclosure cannot reasonably be considered to be disclosure for all purposes to third parties not involved in that transaction."). This confusion of "voluntarily gives" and "consent" is illustrated where *Tracey* quotes with approval *Third Circuit CSLI Case*, "The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone must be rejected." *Id.*

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

B. Whether data collection is prospective or historic might matter

Another option facing Missouri is whether or not it matters if police collect historic/stored data as opposed to prospective/real-time data. When law enforcement collects historic location information, they are dealing with stored business records. When they collect data prospectively, the argument goes, they are effectively using the cell phone as a tracking device.

C. The Mosaic Theory is another layer to the analysis whose moment has not yet come

The Mosaic Theory posits that when law enforcement collect massive quantities of data or monitors someone continuously for a long period of time, and such actions would not otherwise constitute a Fourth Amendment search, they can infringe on a reasonable expectation of privacy by drawing a gestalt picture from the aggregation of data.[220] In the metaphor, while the collection of any individual tile is not a search, putting enough tiles together reveals an image. The whole is greater than the sum of its parts. While there is no societally-recognized expectation of privacy in any of the tiles, there may be one in the mosaic. The doctrine reached prominence in Justice Sotomayor's concurrence in the *Jones* case.[221] After that, two district courts adopted the theory,[222] at least in name.[223] The Fourth Circuit then adopted a version of the Mosaic Theory in its now-vacated decision in *Graham*.[224]

220. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd in part sub nom*; United States v. Jones, 132 S. Ct. 945 (2012).

221. *Jones*, 132 S. Ct. at 955–56.

222. Orin Kerr, *Two District Courts Adopt the Mosaic Theory of the Fourth Amendment*, WASH. POST: VOLOKH CONSPIRACY (Dec. 18, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/12/18/two-district-courts-adopt-the-mosaic-theory-of-the-fourth-amendment/ [http://perma.cc/EN79-URHX].

223. Both of these cases depended more on the length of time of surveillance rather than on the aggregation of data. United States v. White, 62 F. Supp. 3d 614, 623–24, 628 (E.D. Mich. 2014); Order Granting Defendant's Motion to Suppress, United States v. Vargas, 2:13-cr-06025-EFS (E.D. Wash. Dec. 15, 2014), ECF No. 106, http://www.eff.org/files/2014/12/15/vargas_order.pdf [http://perma.cc/B9BB-72BZ]. Although Sotomayor in *Jones* speaks of aggregating the data, she does not use the term "mosaic." *Jones*, 132 S. Ct. at 954–57. Elsewhere Kerr refers to the "Long Term Katz Search" rather than Mosaic Theory. Orin Kerr, *Does Fourth Amendment Standing Work Differently for* Jones *Trespass Searches, Traditional* Katz *Searches, and Long-Term* Katz *Searches*, VOLOKH CONSPIRACY (Feb. 14, 2012), http://volokh.com/2012/02/14/does-fourth-amendment-standing-work-differently-for-jones-trespass-searches-traditional-katz-searches-and-katz-long-term-expectation-of-privacy-searches/ [http://perma.cc/4FBF-X76G]. When, as in *Vargas*, police are trying to catch a single fish rather than emergent properties of the school of fish, I prefer to think of long-term surveillance as a "dragnet" rather than a "mosaic."

224. United States v. Graham, 796 F.3d 332, 349 (4th Cir. 2015), *reh'g en banc granted*, 12-4659 L, 2015 WL 6531272 (4th Cir. Oct. 28, 2015) (recognizing a Fourth Amendment privacy interest in "long-term CSLI").

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

VI. AMENDMENT NINE WILL HAVE NO EFFECT: MISSOURI LIKELY WILL WAIT UNTIL A BINDING FEDERAL COURT EXPLICITLY ACCEPTS OR REJECTS THE MOSAIC THEORY OR A RULE DISTINGUISHING HISTORIC FROM PROSPECTIVE DATA

At this point, it is obvious that Amendment Nine will not help Missouri answer any of these questions. None of the questions hinge on whether something is electronic data or electronic communication as opposed to the conventional areas protected by the Fourth Amendment. Amendment Nine proponents were wrong in assuming electronic data and communications did not already fall under Fourth Amendment and Missouri's coextensive protection. That Amendment Nine will be no help is supported by a look at some recent Missouri CSLI cases.

A. Missouri has already adopted the Fifth Circuit's position with regard to historic data

Missouri has so routinely treated historic cell phone data as business records obtainable by subpoena that most of these cases did not even raise search and seizure questions (under the Fourth Amendment or the Missouri Constitution).[225] In each of these cases, law enforcement obtained historic CSLI without a warrant.[226] In each case, police used the data to "place" the defendant at a certain location.[227] The cases reached the appellate court over questions surrounding expert opinion that the records could prove the location of the cell phone.[228] In none of these cases did the defendant even move to suppress the records themselves as illegal searches or seizures. At least with respect to *historic* CSLI data, Missouri has already accepted the Fifth Circuit's approach. Relying on the business records approach, Missouri seems to assume that the cell phone user has no privacy interest in the data; rather, the data as information kept in business records belongs wholly to the cell phone company. Amendment Nine cannot change that. Again, saying the records belong to the company is tantamount to saying the user has voluntarily given the data to the company.

225. *See* State v. Manzella, 128 S.W.3d 602, 605–06 (Mo. Ct. App. 2004); Midgyett v. State, 392 S.W.3d 8, 10–12 (Mo. Ct. App. 2012); State v. Patton, 419 S.W.3d 125, 128–29 (Mo. Ct. App. 2013), *reh'g and/or transfer denied* (Nov. 19, 2013), *transfer denied* (Feb. 25, 2014); State v. Ford, 454 S.W.3d 407, 410 (Mo. Ct. App. 2015).

226. *See, e.g.*, Brief of Respondent at 15, State v. Patton, 419 S.W.3d 125 (Mo. Ct. App. 2013) (No. ED98051), 2013 WL 3363827 ("Prior to trial, the State filed records from AT&T for Defendant's cell phone along with a business records affidavit from AT&T's custodian of records pursuant to § 490.692, RSMo. 2000.").

227. *Manzella*, 128 S.W.3d at 606; *Midgyett*, 392 S.W.3d at 13–14 n.3; *Patton*, 419 S.W.3d at 132; *Ford*, 454 S.W.3d at 413–14.

228. *Manzella*, 128 S.W.3d at 609; *Midgyett*, 392 S.W.3d at 11; *Patton*, 419 S.W.3d at 128–29, 131–32; *Ford*, 454 S.W.3d at 414.

B. Missouri has not decided the question regarding prospective CSLI

State v. Hosier recently presented the Missouri Supreme Court with a *prospective* collection of CSLI case.[229] The court disposed of the case that offered a challenge to the application of third party doctrine to police collection of cell phone location information pursuant to a warrantless order without reaching the underlying question.[230] In *Hosier*, the defendant was a suspect in a double murder that took place in Missouri.[231] Police in Missouri obtained an order under the SCA for the cell phone company to "ping" the suspect's cell phone and thereby provide police with real-time location information based on which cell towers received the ping response—that is, to track his location.[232] Based on that order, Oklahoma police located and stopped the suspect driving on public roads in Oklahoma and discovered evidence in his car.[233] The defense sought to quash this evidence as the fruit of the poisonous tree of the warrantless search.[234] The state argued that under third party doctrine the ping information is only protected by the SCA requirements and not by the Fourth Amendment, and, in the alternative, even if it were protected, officers presented probable cause in their SCA order application anyway.[235]

The case facts gave the court several options to duck the question of interest here, and it exploited one of them.[236] When Oklahoma police activated their siren and beacons to stop Hosier, Hosier sped off.[237] Police chased him until he eventually did pull over.[238] Even if collection of the cell phone location information under the lesser standard of the SCA was a Fourth

229. State v. Hosier, 454 S.W.3d 883, 890 (Mo. 2015), *reh'g denied* (Mar. 31, 2015), *cert. denied*, 136 S. Ct. 37 (2015).

230. *Id.* at 892.

231. *Id.* at 888.

232. *Id.* at 891–92.

233. *Id.* at 891.

234. *Hosier*, 454 S.W.3d at 892.

235. Brief of Respondent at 46, 52–53, 62–64, State v. Hosier, 454 S.W.3d 883 (Mo. 2014) (No. SC93855), 2014 WL 4793514; Oral Argument, State v. Hosier, 454 S.W.3d 883 (Mo. 2014) (No. SC93855), http://www.courts.mo.gov/SUP/index.nsf/fe8feff4659e0b7b8625699f0079eddf/058ddfb765acf27c86257d3800556085/$FILE/SC93855.mp3 [http://perma.cc/X4VW-HAWF].

236. The court could also have ducked the issue by finding that police did provide evidence of probable cause in obtaining the ping order since they had probable cause for a warrant to search Hosier's apartment, or conversely that police failed even to provide the lesser SCA standard on the other. It could also have employed the good faith exception to the exclusionary rule. *See Hosier*, 454 S.W.3d at 888, 891–92.

237. *Id.* at 890.

238. *Id.*

Amendment violation, the taint of that violation was purged by the circumstances, and the evidence should be admitted.[239]

So *Hosier* only makes clear the fact that "[n]o Missouri state court has ruled on this issue."[240] Given the above cases on *historic* CSLI, the "issue" the court refers to is strictly prospective data. In its very brief discussion of this unanswered question, the court did not cite *Fifth Circuit CSLI Case*, but only *Barajas*, the Tenth Circuit case, which dealt with prospective CSLI collection.[241]

Under strict third party doctrine, it should not matter whether the data collected is historic or prospective. Indeed, in the seminal case developing the doctrine, *Smith*, the data was prospective (as are by definition all pen register or trap and trace orders). What keeps this issue an open question in Missouri is a failure to see the connection between treating the data as business records and the third party doctrine. A holding that prospective/real-time collection of CSLI is a search under the Fourth Amendment would be a new rule, and would be inconsistent with *Smith* or the Pen Register Act, absent some way of distinguishing cell phone records from pen register data (such as application of a version of the Mosaic doctrine to long-term prospective CSLI). Since the Pen Register Act requires only reasonable suspicion ("specific and articulable facts") and not probable cause,[242] the new rule would require finding that statute to be unconstitutional. However, since Amendment Nine makes no distinction between historic/stored or prospective/real-time electronic data or communications, it will have no effect on whether or not Missouri accepts this possible new rule. I predict Missouri will maintain its "coextensive" and "the-same-analysis-applies" approach and refrain from giving any effect to Amendment Nine's language. Missouri will likely wait for a broader consensus—either by more federal circuit courts or by the United States Supreme Court—on whether collection of CSLI is a search under the Fourth Amendment.[243]

239. Whether evidence collected in violation of the Fourth Amendment can be "purged of the taint" of that violation depended on a three-factor test. The court found two of the factors persuasive: the intervening event of the car chase when Hosier fled the Oklahoma police car, and the fact that the violation, if it existed, was done pursuant to the SCA in the context of a circuit split on this question, so it was not a flagrant abuse by police. *Id.* at 892–93. Note that the last factor is really a version of the "good faith" exception nearly always available when police relied in good faith on the SCA order and case law suggesting this practice is legal.

240. *Id.* at 892.

241. *Hosier*, 454 S.W.3d at 892.

242. 18 U.S.C. § 2703(c)(1)(B) (2012) (referring to the standard in §2703(d)).

243. Because review of most of these cases by the Missouri Supreme Court is discretionary, the court need not accept them when the facts do not allow them an "out" to avoid deciding this issue. These cases nearly always offer the good faith exception so even when purging the taint is not available, there is nearly always an "out." *E.g.*, *Hosier*, 454 S.W.3d at 892.

C. Amendment Nine will have no effect on whether Missouri adopts the Mosaic Theory

Missouri courts have not looked at the Mosaic Theory at all as of this writing. Since the Mosaic Theory relies on the fact that electronic technology makes possible the unobtrusive collection of great quantities of data at extremely low cost to law enforcement, Amendment Nine would seem to be helpful. Since we have to presume a change in the language of a constitution or statute has an effect, at first glance, it seems obvious that Amendment Nine cuts in favor of adopting the Mosaic Theory. There are two reasons why Amendment Nine should have no effect at all on this question.

First, the Mosaic Theory's focus is on the electronic (and therefore cheap and unobtrusive) nature of the *collection* rather than on the nature of the *data*. While NSA's wholesale collection of phone call metadata targets electronic data, other cases invoking the Mosaic Theory do not. In *Jones*, the data generated was the movement of a vehicle on public roads.[244] Although that information can be reduced to electronic data, it did not start out as electronic data belonging to the suspect. In *Vargas*, the technology involved installation of a camera, but the data collected was digital imagery of the suspect's movements in parts of his front yard readily visible from a public road.[245] Amendment Nine would make that suspect's electronic data and communications as secure as his home, but here the government collected no such electronic data.

Second, for Amendment Nine to have any effect, the Mosaic Theory would have to create a greater degree of protection for electronic data; it could not elevate protection to a position equal to that of the "person, home, papers, and effects" because it already has that same protection. The theory that Amendment Nine would help relies on the fact that electronic data is more readily shared with third parties, even unwittingly. The Mosaic Theory would suspend the third party doctrine in data collection that would not otherwise constitute a search under the Fourth Amendment. Non-electronic information shared with third parties does not enjoy that carve out, at least not if we rely on Amendment Nine to adopt the Mosaic Theory. Therefore, if Missouri is to abide by the ballot language of Amendment Nine and give electronic data and communications the *same* protections previously extended to "persons, homes, papers, and effects," Missouri must either adopt the Mosaic Theory across the board or not at all. Therefore, adding "electronic data" and "electronic communications" to the list would only prevent Missouri from adopting the Mosaic Theory for everything other than electronic data, something it could

244. United States v. Jones, 132 S. Ct. 945, 948 (2012).

245. Order Granting Defendant's Motion to Suppress, United States v. Vargas, 2:13-cr-06025-EFS (W.D. Wash. Dec. 15, 2014), ECF No. 106, http://www.eff.org/files/2014/12/15/vargas_order.pdf [http://perma.cc/22V6-M4GU].

not do under its current "coextensive" and "the analysis is the same" approach to state constitutional protections.

CONCLUSION

Amendment Nine will likely have no more than expressive effect. It was based on the false assumption that neither the Missouri Constitution nor Fourth Amendment jurisprudence considered electronic data and electronic communications to be protected. Since Missouri and federal protections already extended to electronic data and communications, Amendment Nine does nothing. Furthermore, it will not help guide Missouri in answering any of the unanswered questions involving federal Fourth Amendment jurisprudence.

JOSEPH C. WELLING*

* J.D. Candidate, 2016, St. Louis University School of Law. I am deeply indebted to Professor Chad Flanders, not only for his guidance, insight, and advice on this paper, but also for his infectious enthusiasm for thinking and writing about the law. Special thanks to Sara Robertson, Emily Roman, and all the editors and staffers who worked long and hard to produce a fine Volume 60. Finally, I am extremely grateful to Rados Stoddard for her essential and wholehearted support of my decision to begin a career in law in the second half of my life.

SAINT LOUIS UNIVERSITY SCHOOL OF LAW