AT THE INTERSECTION OF FOURTH AND SIXTH: GPS EVIDENCE AND THE CONSTITUTIONAL RIGHTS OF CRIMINAL DEFENDANTS

TIM KOLESK*

TABLE OF CONTENTS

INTRODUCTION

Robin Brooks exited the credit union, looking for his getaway car.[1] Attempting to conceal a package under his jacket, Brooks ran up the street and leapt into the back seat of a waiting Buick. Holding an envelope containing nearly six thousand dollars, he was unaware of the Global

* Executive Senior Editor, *Southern California Law Review*, Volume 90. J.D., University of Southern California Gould School of Law, 2017. The author would like to thank Professor Thomas D. Lyon for his guidance and the editors of the *Southern California Law Review* for their support.

1. This hypothetical is loosely based on the facts of *United States v. Brooks*, 715 F.3d 1069, 1073 (8th Cir. 2013). The pertinent facts have been simplified and dramatized for the effectiveness of the hypothetical.

Positioning System ("GPS") device buried in the stack of twenties. The police had already begun to track him. At trial, the evidence generated by the GPS device would be admitted as a business record of the credit union's security company. An executive for the security company would testify about the routine collection of GPS data to establish this information as a business record, and in so doing, he would secure Brooks's conviction.

Law enforcement suspected Michael Aaron Jayne of kidnapping a young woman.[2] They had a witness in custody who knew Jayne's cell-phone number and provider. Law enforcement contacted the cell-phone provider, and the provider began to generate a record of that user's "pings" off of cell-phone towers. For trial, the cell-phone provider produced that record, certifying its authenticity. Police testified about the circumstances of the request, but no one testified about the records.

These two scenarios highlight the role that law enforcement and the business-record producer play in the generation of GPS data for trial. While once the stuff of police thrillers and spy movies, GPS tracking technology and cell-phone tracking capabilities have become commonplace. Casual users of the technology may use it as part of their daily commute, finding the least time-consuming way to get to their destination.[3] Similarly, police and investigators use it in their work in a manner that may seem routine. As the omnipresence of these devices grows, along with their ability to track our movements down to a few meters, implications arise about how they may be properly used in our court system—notably, who, if anyone, is required to testify about the technology, and how it can be utilized against a criminal defendant.

This Note seeks to address how the sprawl of GPS technology in our lives has permeated into the courts and affected the rights of criminal defendants. The first Part provides general background about the technology and its broader role in the court system, while the second Part examines GPS and the law. The second Part will look at the rules of evidence and the hurdles—however minimal—that GPS evidence may need to overcome when admitted at trial. Because GPS technology, while common, is still subject to errors and tampering, the evidence should be required to be properly authenticated. A GPS record can be—and has been—viewed as a kind of a statement, reporting where a particular person

2. This hypothetical is loosely based on the facts of *Jayne v. Sprint P.C.S.*, No. 2:07-cv-2522, 2010 U.S. Dist. LEXIS 71508 (E.D. Cal. July 14, 2010). The pertinent facts have been simplified and dramatized for the effectiveness of the hypothetical.

3. *See, e.g.*, David Yanofsky, *At Least 10% of Los Angeles Is Using Waze*, QUARTZ (Apr. 24, 2015), http://qz.com/390119/at-least-10-of-los-angeles-uses-waze-to-beat-traffic-jams.

was at a particular time. For this reason, courts have considered the evidence through hearsay analysis and admitted it through the business records exception. Additionally, the second Part discusses the constitutional issues that arise with the introduction of GPS evidence. Specifically, the Confrontation Clause of the Sixth Amendment guarantees a criminal defendant the right to cross-examine the person who makes a report submitted at trial.[4] GPS data can be considered a statement against a criminal defendant, about where the defendant was at a particular time—e.g., when a crime was being committed. The issue becomes whether a criminal defendant is entitled to "confront" the makers of these statements. Finally, the third Part of this Note concludes with concerns of how to properly deal with GPS tracking technology, considering how far it can reach, in light of the general public's seeming non-concern with the level of government use of it. The fact that most of us carry GPS-enabled smartphones in our pockets every day gives rise to questions about the government's ability to track us and what procedural safeguards should be maintained when evidence from these devices is admitted against an individual at trial.

Ultimately, this Note will conclude that when GPS evidence presents a hearsay issue—which involves any human intervention that can alter the data—then the limits of the public records exception to hearsay and the Confrontation Clause are serious and cannot be avoided, because the hearsay at issue is being produced by law enforcement (or agents of law enforcement) and is arguably testimonial. When it comes to GPS tracking data, the criminal defendant should have the right guaranteed by the Confrontation Clause: the ability to cross-examine the person who prepared the report. Despite the erosion of privacy rights, procedural safeguards may at a minimum keep a debate alive about how GPS technology is used in our court system.

I. FROM SCI-FI TO SO WHAT: A BACKGROUND OF GPS TECHNOLOGY

GPS is a navigation system with its roots in the U.S. Department of Defense.[5] The technology dates back to the Cold War, when the United States Navy developed the first satellite navigation system; it took hours for submarines to receive signals from the satellites.[6] It was not until 1985 that

4. U.S. CONST. amend. VI.

5. *What Is GPS?*, GARMIN, http://www8.garmin.com/aboutGPS (last visited Sept. 8, 2017).

6. Marc Sullivan, *A Brief History of GPS*, PC WORLD (Aug. 9, 2012, 7:00 AM), http://www.pcworld.com/article/2000276/a-brief-history-of-gps.html.

the government began to contract with private entities to develop portable GPS receivers: devices that could be placed on ships, airplanes, or persons.[7] As early as 1998, criminal defendants were protesting the use of these devices to track their movements.[8] By 2000, the technology had advanced to the point where people could reasonably afford to have the devices in their cars and, by 2004, on their phones.[9]

Today, GPS receivers can pinpoint a user's location within three to fifteen meters, depending on the technology.[10] There are a number of factors that can reduce this accuracy, including the user being surrounded by tall buildings or large rock surfaces, less-than-ideal satellite location, and suboptimal atmospheric conditions.[11] With most devices, users can upload the information logged in their devices directly onto Google Earth to easily view the GPS data plotted onto Google Maps.[12] Professional companies, like security firms, also keep logs of customers' devices, usually searchable with a device identification number and login information.[13]

Beyond simple GPS data is the location information gathered from beepers and cell-phone towers. With cell-phone towers, the location of an individual can be approximated by coordinating the individual's cell-phone pings off nearby towers.[14] This information is of great importance to law enforcement. In 2013, over 37,000 requests for location data were issued to just one cell-phone company, AT&T.[15] Location information is vital to determining the guilt or innocence of a charged individual, with perhaps

7. *Id.*

8. *See, e.g.*, United States v. Eberle, 993 F. Supp. 794, 798 (D. Mont. 1998) (ruling that law enforcement agents who placed a tracker on a defendant's truck without a warrant did not violate defendant's Fourth Amendment rights, because "the truck was not within the curtilage of the home"), *aff'd sub nom.* United States v. McIver, 186 F.3d 1119 (9th Cir. 1999).

9. Sullivan, *supra* note 6.

10. GARMIN, *supra* note 5. Up until 2000, the U.S. Department of Defense intentionally degraded the accuracy of consumer GPS technology, as a way to "prevent military adversaries from using the highly accurate GPS signals." *Id.*

11. *Id.*

12. *See Import Data from GPS Devices*, GOOGLE EARTH, https://support.google.com/earth/answer/148095?hl=en#ImportingExisting (last visited Sept. 8, 2017).

13. *See, e.g.*, *GPS Tracking Security*, POSITION LOGIC, https://www.positionlogic.com/industries-gps-tracking-solutions/gps-tracking-solution-security (last visited Sept. 8, 2017).

14. Douglas Starr, *What Your Cell Phone Can't Tell the Police*, NEW YORKER (June 26, 2014), http://www.newyorker.com/news/news-desk/what-your-cell-phone-cant-tell-the-police.

15. *The Two Towers: Junk Science Is Putting Innocent People in Jail*, ECONOMIST (Sept. 6, 2014), http://www.economist.com/news/united-states/21615622-junk-science-putting-innocent-people-jail-two-towers.

only DNA providing a clearer determination.[16] The evidence is critical, and as it makes it way into trial, the rights of the defendant should be preserved accordingly.

II. GPS AND THE LAW

Being able to track an individual's movements has obvious advantages for law enforcement personnel. Instead of time-consuming surveillance measures, GPS devices can provide a suspect's whereabouts with greatly reduced efforts.[17] In addition, since most smart phones are now equipped with this technology, its use in our criminal justice system has become more complicated.[18] This data can be collected from a device placed on an individual or the individual's car or, alternatively, gathered from the data stream emanating from a device the individual already owns.[19] GPS devices are used to track parolees, cheating spouses,[20] and employees suspected of fraud,[21] and the trackers can later use this information at trial.

Understanding the collection of GPS data is an important step in determining its evidentiary status. Generally, there are three different types of GPS tracking devices: data loggers, data pushers, and data pullers.[22] They differ in where and how the data is stored. A data logger records the GPS information on a device's internal memory card.[23] A data pusher regularly sends data to a central database, providing updates on where the users are, where they are going, and how fast they are getting there.[24] Because the data is not contained within the actual device, data pushers have security benefits and can be used commercially for tracking truck and

16. David A. Schumann, *GPS Evidence: Ability to Detect True Innocence, and Avoid the Temptation of Law Enforcement Evidence Fabrication*, GPS EVIDENCE ISSUES (Mar. 18, 2012, 2:12 PM), http://gpsevidence.blogspot.com/2012/03/gps-evidence-ability-to-detect-true.html.

17. *See* United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) ("[B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices . . . .").

18. Adam Cohen, *What Your Cell Phone Could Be Telling the Government*, TIME (Sept. 15, 2010), http://content.time.com/time/nation/article/0,8599,2019239,00.html.

19. Nathan J. Buchok, Note, *Plotting a Course for GPS Evidence*, 28 QUINNIPIAC L. REV. 1019, 1023 (2010).

20. *See, e.g.*, Villanova v. Innovative Investigations, Inc., 21 A.3d 650, 651 (N.J. Super. Ct. App. Div. 2011).

21. *See, e.g.*, *10 NJ Transit Workers Disciplined After GPS Technology Catches Vehicle Misuse*, NBC N.Y., (May 6, 2014, 7:02 AM), http://www.nbcnewyork.com/news/local/NJ-Transit-Discipline-GPS-Technology-Vehicle-Use-Fraud-258087101.html.

22. *How GPS Tracking Works*, TECH-FAQ, http://www.tech-faq.com/how-gps-tracking-works.html (last visited Sept. 9, 2017).

23. *Id.*

24. *Id.*

delivery-vehicle fleets.[25] The third type of device is the data puller, which enables the owner of the device to extract data as needed. This type of device may be used to trace stolen goods.[26]

After being collected, GPS data is either downloaded from or transmitted to the user's computer. Using specialized software, the recorded data may then be transposed onto a map in real time or stored for later analysis.[27] Companies can purchase systems of these devices and track devices via consumer-based software.[28] For the personal user, an individual can download information from the data logger and import it directly into Google Earth.[29] This is the point in the process that raises potential hearsay concerns: a human agent performing an administerial task may alter or refine the data to produce specific information that is to be presented against an individual.

Once obtained and presented for trial purposes, GPS evidence is subject to the court system's rules of evidence. Because GPS evidence has become so widespread and readily accepted, little thought is given to its accuracy or reliability when admitting it into evidence.[30] In a recent opinion, the First Circuit noted the casual acceptance of GPS by a trial judge, who commented, "You don't have to be a rocket scientist to read a GPS," and "My nine year old can do that."[31] But the role of human agency—even that of a nine-year-old—in the collection of GPS data is still important for the criminal defendant. This data can be as incriminating as DNA evidence, but GPS evidence has become so common that courts' attitudes towards it have relaxed, to the point where no one is required to testify about the technology's effectiveness.

The lack of an in-court witness for GPS evidence raises hearsay issues. Although one writer predicted that "it is ultimately unlikely that court[s] will treat GPS evidence as [hearsay],"[32] recent court decisions have done so. Indeed, several state courts have followed this unlikely path. When hearsay evidence is admitted against a criminal defendant, that

25. *Id.*

26. *Id.*

27. *See Fleetistics LITE*, FLEETISTICS, https://www.fleetistics.com/features (last visited Sept. 9, 2017).

28. *See id.*

29. *See* GOOGLE EARTH, *supra* note 12.

30. *But see* Buchok, *supra* note 19, at 1020 (noting the "reliability flaws inherent in the technology itself and the vulnerability of GPS systems to intentional tampering by third parties," but ultimately concluding that GPS technology "is reliable enough for use at trial").

31. United States v. Espinal-Almeida, 699 F.3d 588, 611 (1st Cir. 2012).

32. Buchok, *supra* note 19, at 1056–57.

defendant's Confrontation Clause right is triggered—a right strengthened by the Supreme Court in *Crawford v. Washington*, in which the Court made clear that reliability of evidence alone does not satisfy the goals of the Sixth Amendment.[33] The following section examines the rules of evidence, recent cases interpreting these rules when dealing with GPS evidence, and the constitutional constraints upon its admission.

A. THE "RULES" OF THE ROAD

Trials serve larger purposes beyond simply determining what happened in a given case.[34] The process hopefully instills in the participants a sense that the judicial system is fair. This broader goal is spelled out in the Federal Rules of Evidence ("FRE," or "Rules"), applicable in "federal criminal proceedings and in civil proceedings in federal court."[35] The Rules state that their purpose is to "administer every proceeding fairly, eliminate unjustifiable expense and delay, and promote the development of evidence law, to the end of ascertaining the truth and securing a just determination."[36] Fairness, it is worth noting, is the first larger aspirational ideal laid out in Rule 102,[37] with truth following later, suggesting that fairness and truth may not always be entirely compatible. Fairness and the admissibility of GPS evidence intersect when evidence is excluded on the grounds that it has been obtained without a warrant, in potential violation of the Fourth Amendment, noted in Part III.C; or when obtained through or created by a governmental agent but admitted through the business records exception to the rule against hearsay, examined in Part III.B. Fairness is upheld when the rules—and Rules—are respected. Under the FRE, fairness requires someone to testify about the accuracy of GPS data evidence. The first opportunity for testimony on GPS data is through the authentication of the evidence.

B. AUTHENTICATION

GPS evidence, like all evidence to be admitted at trial, is subject to authentication. To authenticate an item of evidence under the FRE, "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[38] Rule 901(b) sets out a

33. *See* Crawford v. Washington, 541 U.S. 36, 62 (2004).

34. JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S EVIDENCE MANUAL § 1.01 (Matthew Bender 2015).

35. CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, 1 FEDERAL EVIDENCE § 8:2 (4th ed.), Westlaw (database updated June 2017).

36. FED. R. EVID. 102.

37. *See* MUELLER & KIRKPATRICK, *supra* note 35, § 1:2.

38. FED. R. EVID. 901(a).

nonexhaustive list of examples of evidence that can properly authenticate the item in question.[39] Of relevance for GPS evidence is Rule 901(b)(1), which requires testimony of a witness with knowledge "that an item is what it is claimed to be;" 901(b)(4), which allows authentication through evidence that describes the distinctive characteristics of the item in question; and 901(b)(9), which requires "[e]vidence describing a process or system and showing that it produces an accurate result."[40] Computer-generated output can be authenticated through evidence that demonstrates that the technology that generated the evidence was in good condition, that qualified users of the technology were involved with the output, that appropriate protocol was followed, and that there were no problems with the software.[41] The witness who provides the authentication testimony must be a person familiar with the process that produced the output, but that person does not have to be the person individually responsible for the specific process at issue.[42] Nor does the witness necessarily need to possess any particular technical prowess.[43]

The lack of expertise of the testifying witness and the growing comfort with GPS technology results in a low threshold for admissibility.[44] In *United States v. Espinal-Almeida*, the First Circuit held that GPS evidence downloaded from a device was properly authenticated through the testimony of a "Customs forensic scientist" who described the processes of the GPS and software, did not have any reservations about the data, and provided corroboration that the coordinates produced roughly matched those taken by a Coast Guard photographer present at the scene.[45] Despite the title of "Customs forensic scientist," the court also noted that expert testimony was not necessary for the GPS evidence.[46] State courts have also examined the authentication process of GPS evidence and have not required the authenticating witness to be an expert in the field. In one of the

39. *Id.* 901(b).

40. *Id.* 901(b)(1), (9).

41. MUELLER & KIRKPATRICK, *supra* note 35, § 9:20.

42. *Id.*

43. *Id.*

44. The standard for authentication generally is "evidence sufficient to support a finding that the item is what the proponent claims to be," one of the lower thresholds of admissibility in the FRE. FED. R. EVID. 901(a). While not often creating a serious hurdle for the admission of GPS evidence, authentication is nevertheless a hurdle that must be cleared.

45. United States v. Espinal-Almeida, 699 F.3d 588, 613 (1st Cir. 2012).

46. *Id.* at 612–13 ("The issues surrounding the processes employed by the GPS and software, and their accuracy, were not so scientifically or technologically grounded that expert testimony was required to authenticate the evidence, and thus the testimony of [the Customs forensic scientist], someone knowledgeable, trained, and experienced in analyzing GPS devices, was sufficient to authenticate the GPS data and software generated evidence.").

more factually interesting cases involving GPS evidence, *State v. Kandutsch*, the Wisconsin Supreme Court considered whether GPS evidence could be admitted to show that the defendant had driven while intoxicated, after he had been spotted drinking at a part, and his electronic monitor placed him at home fifteen minutes later.[47] The court concluded that the testimony of "two Department of Corrections agents was sufficient . . . to provide a foundation for the report's accuracy and reliability."[48] Note the role of the law enforcement officer or agency as in-court witness for authentication purposes, as this takes on added significance in the hearsay analysis *infra*.

Additionally, between the lines of Rule 901 lies another safeguard. Normally, for tangible objects a proper foundation must be laid to establish the "chain of custody": witnesses who had custody of the item in question––as in a gun or knife—from the time of the event until trial must testify, by offering distinctive characteristics, that the item is the same one recovered and has not materially changed.[49] With GPS evidence, the chain of custody of a GPS device may need to be established.[50] And with GPS tracking data, the foundation is laid by an individual able to describe the distinctive characteristics of the data in question. For example, the forensic scientist in *Espinal-Almeida* was able to establish the precise protocol of how his agency handled the device in question while confirming that the location data matched the photographer's pictures.[51] While the potential for tampering with GPS evidence carries serious implications,[52] there has been little published case law regarding fraudulently manufactured GPS information. But devices can malfunction and lose track of the suspect, creating gaps in the data. A human agent is needed to fill in this information.

As with authentication issues generally, little is required to lay a foundation for the admission of GPS evidence. But when dealing with

47. State v. Kandutsch, 799 N.W.2d 865, 868 (Wisc. 2011).

48. *Id.*

49. MUELLER & KIRKPATRICK, *supra* note 35, § 9:10 ("Authenticating objects by showing chain of custody is not specifically regulated in the Rules, but the approach is common and well accepted in the profession, and Rule 901(b)(1) and (b)(4) together embrace this technique.").

50. *See Espinal-Almeida*, 699 F.3d at 609–10 (establishing the chain of custody for a seized GPS device when a government witness testified that he took possession of unit from officers at scene and recorded its serial number on an agency evidence form).

51. *Id.* at 608 ("The GPS device that was seized from the mothership was admitted into evidence after being identified by Cabán, the Coast Guard officer who had arrested the defendants on the mothership, and Ramos, the ICE officer who had taken custody of the GPS on land.").

52. *See* Buchok, *supra* note 19, at 1047 (noting the "potential vulnerabilities of GPS evidence to intentional tampering").

machine-related evidence, the level of sophistication of the technology plays a factor in the amount of effort needed when laying the foundation for admissibility.[53] With simple machines that are used every day, an elaborate foundation may be unnecessary, but as the level of machine sophistication rises, so does the requisite foundation.[54] An expert witness may be required.

Normally, a witness must be qualified as an expert in order to provide testimony on scientific, technical, and specialized matters.[55] An expert can be qualified through education, experience, or possession of a unique skill set.[56] Due to the everydayness of GPS, however, courts have not required witnesses to meet even this low threshold of expertise.[57] Courts can instead defer to Rule 201, which "permits the court to take judicial notice of 'a fact that is not subject to reasonable dispute because it: (1) is generally known within the trial court's territorial jurisdiction; or (2) can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.'"[58] In *United States v. Brooks*, the Eighth Circuit, upholding the district court's decision to admit evidence without expert testimony, noted that "[c]ommercial GPS units are widely available, and most modern cell phones have GPS tracking capabilities. Courts routinely rely on GPS technology to supervise individuals on probation or supervised release, and, in assessing the Fourth Amendment constraints associated with GPS tracking, courts generally have assumed the technology's accuracy."[59]

The Ninth Circuit has similarly suggested that the courts could simply take judicial notice of Google Earth in order to confirm the precise whereabouts of a defendant.[60] In *United States v. Lizarraga-Tirado*, the Ninth Circuit considered what it called a question "born of . . . newfound technological prowess."[61] The question before the court was whether a

53. MUELLER & KIRKPATRICK, *supra* note 35, § 8:13.

54. *Id.*

55. *Id.* § 7.8.

56. *Id.*

57. *See* Buchok, *supra* note 19, at 1040 ("The question of where GPS evidence stands under the *Daubert* standard [incorporated into Rule 702] is not entirely clear, as there is little case law specifically on point. An examination of GPS technology under the *Daubert* reliability factors, however, leads to the conclusion that courts would likely find GPS evidence admissible.").

58. *See* United States v. Brooks, 715 F.3d 1069, 1078 (8th Cir. 2013) (quoting FED. R. EVID. 201).

59. *Id.*

60. United States v. Lizarraga-Tirado, 789 F.3d 1107, 1109 (9th Cir. 2015) ("[W]e can take judicial notice of the fact that the tack was automatically generated by the Google Earth program. . . . Specifically, we can access Google Earth and type in the GPS coordinates, and have done so . . . .") (citation omitted).

61. *Id.* at 1108.

digital "tack" created through the use of GPS coordinates and Google Earth was properly admitted at trial.[62] The defendant in *Lizarraga-Tirado* was arrested near the Mexican border and contested whether he had actually entered U.S. territory. One of the arresting border patrol agents made a contemporaneous recording of the coordinates of the arrest site using her handheld GPS device; the government then used Google Earth to create a satellite image to show the location of the defendant at the time of the arrest. Although the defendant failed to raise an authentication objection, the Ninth Circuit offered that the "proponent of Google-Earth-generated evidence would have to establish Google Earth's reliability and accuracy."[63] This could be done via a Google programmer or someone who works with the program frequently, or "through judicial notice of the program's reliability, as the Advisory Committee notes specifically contemplate."[64]

Taking judicial notice removes the need for an in-court witness to testify and makes the proffered evidence more difficult to challenge.[65] As judges assume GPS technology works because they are comfortable with it, prospective challenges to the admissibility of the evidence become more tenuous. But defendants should be prepared to attack the specific device in question—as well as the technology itself.

Authentication presents the lowest hurdle that GPS evidence needs to clear. The issues are simple and require fairly straightforward proof, but there are legitimate objections that merely taking judicial notice of its reliability raises serious concerns.[66] But the introduction of GPS evidence raises further statutory—and even constitutional—considerations. For example, *Lizarraga-Tirado* also touched upon hearsay issues and Confrontation Clause concerns. The defendant argued that the satellite image was hearsay because "it asserts that it 'accurately represented the desert area where the agents worked,' and the tack and coordinates are hearsay because they assert 'where the agents responded and its proximity to the border.'"[67] In response, the Ninth Circuit first determined that a

62. *Id.*

63. *Id.* at 1110.

64. *Id.*

65. Kelso L. Anderson, *Admission of GPS Evidence Signals Brave New World*, ABA LITIGATION NEWS, Feb. 20, 2014, http://apps.americanbar.org/litigation/litigationnews/mobile/article-gps-technology-evidence.html.

66. *Id.*

67. *Lizarraga-Tirado*, 789 F.3d at 1109. In the published opinion, the Ninth Circuit never addressed which hearsay exception allowed the underlying statement: the agent's recording of the coordinates. Presumably, this recording came in through the recorded-recollection exception, which

satellite image is not hearsay, based on its previous determination that, similarly, a photograph is not hearsay "because it makes no 'assertion.'"[68] The court then reasoned that the tack is also not hearsay, since that tack is automatically generated by Google Earth. Emphasizing the role of the human declarant in the Rules, the court noted that the digital tack here "isn't made by a person; it's made by the Google Earth Program."[69] The court noted that "machine statements" still present evidentiary concerns, but these are addressed by authentication.[70] As for Sixth Amendment concerns, the Ninth Circuit concluded that "[b]ecause the satellite image and tack-coordinates pair weren't hearsay, their admission also didn't violate the Confrontation Clause."[71] But while the digital tack of *Lizarraga-Tirado* did not raise these concerns, GPS evidence elsewhere has. The following parts examine when the proffered location information raises hearsay and constitutional questions.

C. HEARSAY AND ITS EXCEPTIONS

Depending on the data, courts can consider records generated through GPS devices as hearsay. Hearsay is defined as "an out-of-court statement offered to prove . . . the truth of the matter asserted."[72] The Rules define a "statement" as a "person's oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion."[73] The person making the statement is referred to as the "declarant."[74] The rationale behind the exclusion of hearsay is that these assertions should be considered untrustworthy since the out-of-court declarant is not subject to a sworn oath, the pressures of testifying in front of a judge or jury, or cross-examination by an adversarial opponent.[75] These requirements aim to exclude evidence that "lack[s] the conventional indicia of reliability."[76] If GPS evidence were to be treated as hearsay, the interpretation would be

pertains to a "record that: (A) is on a matter the witness once knew about but now cannot recall well enough to testify fully and accurately; (B) was made or adopted by the witness when the matter was fresh in the witness's memory; and (C) accurately reflects the witness's knowledge." FED. R. EVID. 803(5). This presumption is bolstered by the Ninth Circuit's opinion noting that the agent testified "about whether she had recorded the GPS coordinates accurately." *Lizarraga-Tirado*, 789 F.3d at 1109.

68. *Lizarraga-Tirado*, 789 F.3d at 1109.

69. *Id.* at 1110.

70. *Id.*

71. *Id.*

72. MUELLER & KIRKPATRICK, *supra* note 35, § 8:2.

73. FED. R. EVID. 801(a).

74. *Id*. 801(b).

75. DAVID F. BINDER ET AL., HEARSAY HANDBOOK § 3.2 (4th ed.), Westlaw (database updated Sept. 2016).

76. Chambers v. Mississippi, 410 U.S. 284, 298 (1973).

that the "statement" concerns a representation of the defendant's whereabouts.[77]

The FRE provides a list of exceptions to the rule against hearsay, including exceptions that apply "regardless of whether the declarant is available as a witness" at trial.[78] For the purposes of the admission of GPS evidence, two of these exceptions are of interest: the business records exception and the public records exception. Rule 803(6), known as the business records exception, provides an exception for records "made at or near the time by" a person with knowledge that were "kept in the course of a regularly conducted activity," when making the records was a "regular practice of that activity."[79] The exception further requires "testimony of the custodian or another qualified witness" to ensure that these conditions are met.[80] However, "[i]n 2000, the exception was amended to dispense with the need for any kind of live foundational testimony and to permit the proponent to use a certification procedure instead."[81] Either through testimony or certification, the proponent of the business record must present that these records were regularly and routinely kept. The regularity and routine requirements aim to contribute to the trustworthiness of the records.[82] Rule 803(8), the public records exception, pertains to records that set out "(i) the office's activities; (ii) a matter observed while under a legal duty to report, but not including, in a criminal case, a matter observed by law-enforcement personnel; or (iii) in a civil case or against the government in a criminal case, factual findings from a legally authorized investigation."[83] Of particular interest for the use of GPS evidence are the second and third clauses, which prohibit the use of records containing certain information against criminal defendants. While "matter observed" seems to be incredibly broad, the phrase has been interpreted to include only simpler, more concrete records, as opposed to those that involve interpretation or evaluation.[84]

As noted above, Rule 801(a) defines a statement as being made by a

77. *See* Ruise v. State, 43 So. 3d 885, 886 (Fla. Dist. Ct. App. 2010) (applying Florida's rules of evidence).

78. FED. R. EVID. 803.

79. *Id*. 803(6).

80. *Id.*

81. MUELLER & KIRKPATRICK, *supra* note 35, § 8:78. The certification process includes a statement "given under penalty of perjury" to lay the foundation for a business record. *Id.*

82. *Id.* § 8:77.

83. FED. R. EVID. 803(8).

84. MUELLER & KIRKPATRICK, *supra* note 35, § 8:88.

person, so statements made by machines seem not to qualify as hearsay.[85] But when machines churn out what the human controller is asserting or inputting, these machine "statements" can be subject to hearsay analysis.[86] Courts have emphasized the difference between computer-generated and computer-stored when determining if records in question should be subject to hearsay analysis.[87] Computer-generated records are created purely by machine processes, like an automated system log; as opposed to computer-stored records, which have a more direct human originator, like a Word file. GPS data can at times fit both bills, as they can be generated by a machine—an automated truck fleet log, for example—and stored on a computer, such as when a user enters coordinates to determine a location.

Often, the nature of the evidence will be self-evident. Nevertheless, the role of the human agent is important in making these distinctions, so it is worth considering for the purposes of GPS evidence. For example, take a device recovered from a suspect's car and the data subsequently downloaded from it. There is little assertion being made by any human, but humans are still involved in the construction of evidence. One would still need to prove whose car the device came from, and a person would be relied upon to make that determination. If a device malfunctions or there are errors with its output, someone would need to describe what took place and why the underlying data is still trustworthy. Further, if a human initiated the tracking, as in the bank-robbery hypothetical above, this would raise testimonial concerns—the reason or motivation behind the tracking becomes important, as examined below. The level of human agency is heightened further with the use of a digital tack, as seen in *Lizarraga-Tirado*.[88] These location pins can be placed by a law enforcement agent or an individual using a social media page. This is clearly an assertion about that individual's whereabouts.

Hearsay is a difficult concept to master.[89] To make things more interesting, layered hearsay exists when an out-of-court statement contains

85. *Id.* § 8:13. *See also* Adam Wolfson, Note, *"Electronic Fingerprints": Doing Away with the Conception of Computer-Generated Records as Hearsay*, 104 MICH. L. REV. 151, 160 (arguing that "computer-generated records," which lack any human assertions, should not be considered hearsay).

86. MUELLER & KIRKPATRICK, *supra* note 35, § 8:13.

87. *See* Commonwealth v. Thissel, 928 N.E.2d 932, 937 n.13 (Mass. 2010).

88. *See* United States v. Lizarraga-Tirado, 789 F.3d 1107, 1109 (9th Cir. 2015) ("If the tack is placed manually and then labeled (with a name or GPS coordinates), it's classic hearsay . . . . [A] user could place a tack, label it with incorrect GPS coordinates, and thereby misstate the true location of the tack."). However, the tack in *Lizarraga-Tirado* was generated by entering coordinates and not, for example, relying on a cell phone to drop a "pin" to determine location.

89. *See* BINDER, *supra* note 75, § 2:1 (noting that "the hearsay objection is overused" and "[m]any lawyers object every time a witness starts to relate what someone else has said").

another out-of-court hearsay.[90] Layered hearsay, double hearsay, multiple hearsay or hearsay within hearsay may be admissible "if each part of the combined statements conforms with an exception to the rule" against hearsay.[91] For the purposes of this note, it is worth pausing to examine what is being treated as hearsay and what is not. GPS data can be seen as two "statements." The first statement is from the GPS device itself: GPS device says, "Defendant is here." This is non-hearsay. As demonstrated above, this is a machine-generated statement, not subject to hearsay analysis due to the lack of a human declarant. When the record of that GPS statement is created, another statement is being proffered: Record says, "GPS device says, 'Defendant is here.'" While this might appear to be an example of layered hearsay, the record only provides one level of hearsay––the outer statement being made by the record. Once that record fits into an exception, like the business records exception, the evidence is admissible. As one state court examining the evidentiary status of GPS data stated, "[t]he GPS data is clearly hearsay because it purports to show Appellant's locations . . . and it is being offered for the truth of the matter asserted, *i.e.*, to prove that Appellant was in the locations away from his residence reflected in the GPS data."[92] Further hearsay questions may arise when determining whether the "Defendant" who is supposedly "here" is really the Defendant at trial. Someone will have to provide statements that establish that "Defendant" was "here," and those statements will similarly be subjected to the rule against hearsay.

When admitted as a hearsay exception, GPS evidence is often treated as a business record. However, often times, law enforcement agents are involved—in varying degrees of control—with the creation of these records. In these instances, the restrictions of the public records exception are potentially circumvented, as the evidence is admitted through the less stringent business records exception. Perhaps because the business records exception is entitled "Records of a Regularly Conducted Activity,"[93] the business records exception has been, at times, misconstrued to extend to "records that are official public documents or entries made by agencies of government."[94] In practice, records can be both public and business. But using the business exception over the public one may be an attempt, intentional or incidental, to avoid the restrictions of Rule 803(8).[95] In some

90. MUELLER & KIRKPATRICK, *supra* note 35, § 8:136.
91. FED. R. EVID. 805.
92. Ruise v. State, 43 So. 3d 885, 886 (Fla. Dist. Ct. App. 2010).
93. FED. R. EVID. 803(6).
94. MUELLER & KIRKPATRICK, *supra* note 35, § 8.84.
95. *Id.*

criminal cases, lab reports have been admitted under the business records exception, and these reports (and arguably certain police reports that contain investigative findings) would be excluded if they were subject to the restrictions of the public records exception. By treating this data as a business record instead of a public record, courts would be removing a procedural safeguard against criminal defendants—the requirement that someone has to testify about the circumstances surrounding the assertive statements. Examining the specifics of when GPS data is admitted through the business records exception reveals whether these safeguards are being honored.

Three cases show how GPS evidence is admitted as hearsay through the business records exception. The first provides an example of what is arguably the proper treatment of GPS evidence as a business record. In *United States v. Wood*, the district court determined that GPS evidence was properly admitted against a criminal defendant through the business records exception.[96] In *Wood*, the defendant was a truck driver accused of making an "unscheduled detour" to pick up marijuana.[97] The government introduced GPS evidence detailing the driver's route, and the witness who testified about the accuracy of the records owned the trucking company.[98] The trucking company leased the GPS devices and accessed the information through another trucking company's website.[99] The company owner testified that he would "frequently" check on the location of trucks by calling the drivers and confirming their whereabouts on the website, leading the court to credit Jain's testimony that he "relied upon the GPS tracking information in the regular course of his business and that the GPS records created in this manner were maintained in the ordinary course of . . . business."[100] Critically, the business *regularly* kept this type of record, rather than waiting to begin generating GPS information only once a crime was suspected.

The next case provides an example of how the routine nature of business records can arguably be improperly stretched. In *United States v. Brooks*, the Eighth Circuit considered the admissibility of GPS tracking evidence under the business records exception against a defendant accused of robbing a credit union.[101] During the robbery, the credit union's teller

96. United States v. Wood, No. 08-CR-92A, 2009 U.S. Dist. LEXIS 60335, at *9 (W.D.N.Y July 15, 2009).

97. *Id.* at *3.

98. *Id.* at *5.

99. *Id.* at *5–*6.

100. *Id.* at *6, *10.

101. United States v. Brooks, 715 F.3d 1069, 1073 (8th Cir. 2013).

placed a GPS tracking device in a stack of money, which the police and the credit union's security company tracked.[102] Police later found the device in a white sedan, which matched an eyewitness's description of the getaway vehicle, along with other evidence.[103] At trial, an executive for the security company testified about the "overall accuracy and reliability of GPS technology."[104] This by itself—testifying to a process and proving that it works—would solve any authentication problems for machine-generated evidence. As for hearsay concerns, however, the Eighth Circuit concluded that the evidence was properly admitted as a business record, since "when one of [the security company's] customers activates a . . . device, the company routinely keeps the GPS data on the company server."[105] As opposed to *Wood*, in which the GPS data was routinely being logged by a trucking company, here in *Brooks*, the creation of the GPS data was initiated by the commission of the crime.

The timing raises the question of whether the business record was created in anticipation of litigation, a red flag for potential untrustworthiness under the FRE.[106] The opponent of the record in question would argue that such a record is "favorable to the preparing party" and would not be required to put forth evidence affirming the record's untrustworthiness; rather, that determination depends on how the record was produced.[107] While *Brooks* did not address this directly,[108] the court may have come to the conclusion that the record was prepared for a law enforcement purpose, not to establish a fact at trial, and was therefore still sufficiently trustworthy. The bank argued that the tracker was placed to recover the money, not just to secure the robber's conviction.[109] Further, the regular practice was to initiate tracking in response to any bank robbery. The counterargument, however, would be that tracker was placed after the bank was robbed, and therefore the GPS data was produced in order to use it against the robber at trial. Because the record does not contain a human agent making a more speculative evaluation, like a written accident report, the GPS data here may ultimately be considered trustworthy. But the anticipation-of-litigation exception to the business

102. *Id.*
103. *Id.* at 1074.
104. *Id.* at 1077.
105. *Id.* at 1079.
106. FED. R. EVID. 803(6) advisory committee's note to 2014 amendment.
107. *Id.*
108. The defendant in *Brooks* did object to the records, on the grounds that "they were developed primarily for a law enforcement purpose." *Brooks*, 715 F.3d at 1079. However, the objection was based on a constitutional concern, not a hearsay issue. The constitutional concern is examined in Part III.D.
109. *Id.* at 1080.

records rule is worth noting, especially as the use of GPS tracking expands.

A third example shows how law enforcement's involvement with the collection of records can arguably frustrate the purpose behind the distinction between public and business records. In *State v. Jackson*, the prosecution used GPS evidence to confirm the location of a suspect who was wearing an electronic monitoring device at the time of an alleged assault.[110] Besides testimony from the victim and responding officers, the "State introduced evidence from defendant's electronic monitoring device in order to place defendant at the scene of the assault."[111] To testify about the device and how it generated the data to be admitted as evidence, the state called on a police sergeant who was "the supervisor of the electronic monitoring unit" of the local police department.[112] The sergeant testified about the specific device the defendant was wearing, how it worked, and how the data was collected into an "event log."[113] Despite the defendant's argument that this was inadmissible hearsay, the court held that "the GPS tracking evidence was properly admitted as a business record,"[114] notwithstanding the fact that North Carolina's evidence code has a parallel rule to FRE 803(8) providing safeguards for criminal defendants.[115] This lack of adherence to the Rules may cause an additional harm to the defendant: while there still was an in-court witness, it was a law enforcement agent testifying about the accuracy of the system, not a

110. State v. Jackson, 748 S.E.2d 50, 53 (N.C. Ct. App. 2013). Twenty-one states have adopted business records exceptions that are substantially similar to Federal Rule 803(6). CLIFFORD S. FISHMAN & ANNE T. MCKENNA, 1 JONES ON EVIDENCE § 33:4 (7th ed.), Westlaw (Jan. 2016 update). North Carolina's parallel rule to Federal Rule 803(6) is as follows:

> Records of Regularly Conducted Activity.—A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if (i) kept in the course of a regularly conducted business activity and (ii) it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by affidavit or by document under seal under Rule 902 of the Rules of Evidence made by the custodian or witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. Authentication of evidence by affidavit shall be confined to the records of nonparties, and the proponent of that evidence shall give advance notice to all other parties of intent to offer the evidence with authentication by affidavit. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

N.C. GEN. STAT. § 8C-1, Rule 803 (2015).

111. *Jackson*, 748 S.E.2d at 53.

112. *Id*. at 54.

113. *Id.*

114. The opinion states that the "defendant's primary contention concerning the admissibility of the tracking evidence is that the State failed to establish a proper foundation to verify the authenticity and trustworthiness of the data," likely suggesting no objection to its consideration as a business record was made. *Id.* at 55.

115. N.C. GEN. STAT. § 8C-1, Rule 803.

representative from a company. The bias of juries towards police as witnesses[116] becomes an unnecessary factor. Again, a relaxed approach erodes protections for the defendant.

These three cases together demonstrate how evolving GPS technology can diminish the safeguards established by the rules of evidence. *Wood* shows how established, continuous business records can be used to reveal an employee of that business breaking the law. *Brooks* shows how a company in the business of surveillance can work hand-in-hand with law enforcement personnel to obtain a conviction. And *Jackson* shows a further blurring of the lines, with law enforcement serving as the "business" itself.

This blurring of the lines between business and public has serious ramifications for the criminal defendant: one requires live testimony, the other does not. The protection of requiring an in-court witness for certain records was constitutionalized in a sense by the Supreme Court in *Crawford v. Washington*, which fortified a defendant's right to cross-examine witnesses.[117]

D. THE CONFRONTATION CLAUSE

The Confrontation Clause provides criminal defendants with a constitutional safeguard when GPS data is introduced against them at trial. For example, the defendant in *Brooks* raised concerns that the "GPS tracking reports and related testimony violated his rights under the Sixth Amendment's Confrontation Clause."[118] The Confrontation Clause states that "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him."[119] This could be read broadly to mean that all witnesses must testify against the defendant.[120] In *Crawford v. Washington*, however, the Court clarified that a defendant's confrontation right did not apply to *all* out-of-court statements but to a "specific type of out-of-court" statement, namely "testimonial" hearsay.[121] *Crawford* did not offer a definitive answer as to what constitutes testimonial hearsay; instead, it "described the class of testimonial statements covered by the Confrontation Clause,"[122] including "statements

116. *See, e.g.*, Vida B. Johnson, *Bias in Blue: Instructing Jurors to Consider the Testimony of Police Officer Witnesses with Caution*, 44 PEPP. L. REV. 245, 256 (2017).

117. *See* Crawford v. Washington, 541 U.S. 36, 55–59 (2004).

118. United States v. Brooks, 715 F.3d 1069, 1077 (8th Cir. 2013).

119. U.S. CONST. amend. VI.

120. *Crawford*, 541 U.S. 36, 42 (2004).

121. *Id.* at 51.

122. Melendez-Diaz v. Massachusetts, 557 U.S. 305, 309 (2009) (citing *Crawford*, 541 U.S. at 51–52).

that were made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial."[123] As the Court worked through its definition of testimonial hearsay, it stated that "[m]ost of the hearsay exceptions cover[] statements that by their nature [a]re *not* testimonial—for example, *business records*."[124]

The Court would later clarify the characterization of business records, as more cases forced a reexamination of what is considered testimonial. For example, *Davis v. Washington* and *Michigan v. Bryant* further developed the "emergency exception," treating statements given to police as nontestimonial when there is an immediate risk of harm and the statement would assist the officer in preventing that harm.[125] *Bryant* pushed courts to look at the "purpose of the interrogation" to determine the motives of the witness and the interviewing police officer in determining whether the goal was to end an ongoing emergency.[126]

Business records and computer-generated reports provide their own wrinkles to the Confrontation Clause doctrine. As noted above, strictly mechanically produced records are not hearsay, since the role of the human agent is central to hearsay's definition.[127] Under this framework, purely machine-generated records are not hearsay, they cannot be testimonial, and they are therefore arguably not subject to the Confrontation Clause.[128] However, the question remains over what do with the human intervener who produces the specific records against a criminal defendant. In recent decisions, the Supreme Court has recognized the role of human error when relying on machine-generated reports.

In *Melendez-Diaz v. Massachusetts*, the Court determined that "results of . . . forensic analysis" submitted against a criminal defendant without a testifying analyst "violated [the defendant's] Sixth Amendment right."[129] The *Melendez-Diaz* prosecution had submitted certificates—permissible under the amended Rules—stating the results of forensic tests on a seized controlled-substance; they simply reported that "the substance was found to contain: Cocaine."[130] The Court held that the Confrontation Clause required the analyst to testify, and noted that "an analyst's lack of proper

123. *Crawford*, 541 U.S. at 52.

124. *Id.* at 56 (emphasis added).

125. *See* Michigan v. Bryant, 562 U.S. 344, 370–378 (2011); Davis v. Washington, 547 U.S. 813, 822 (2006); MUELLER & KIRKPATRICK, *supra* note 35, § 8:27.

126. *See Bryant*, 562 U.S. at 367–70.

127. FISHMAN & MCKENNA, *supra* note 110, § 34A:31.

128. *Id.*

129. Melendez-Diaz v. Massachusetts, 557 U.S. 305, 308–10, 329 (2009).

130. *Id.* at 308.

training or deficiency in judgment may be disclosed in cross-examination."[131] The Court also addressed the argument that such certificates should be admissible as official and business records by pointing out that, "like police reports generated by law enforcement officials," the certificates were testimonial because they were "calculated for use essentially in the court, not in the business."[132] Departing slightly from its position in *Crawford*, the Court looked to the purpose behind the creation of the records to determine whether they were testimonial. Records "created for the administration of an entity's affairs" are not testimonial, but those records created to establish "some fact at trial" are testimonial.[133] The facts of *Melendez-Diaz* allowed a non-complicated answer to this either-or question: the analysts' statements were "prepared specifically for use at . . . trial"[134] and were therefore testimonial. Additionally, in *Bullcoming v. New Mexico*, the Court held that the analyst who actually performed the test must testify in order to satisfy the Confrontation Clause.[135] Again, the Court pointed out that the possibility of human error required the testing analyst to testify, since the test in question "require[d] specialized knowledge and training" and "[s]everal steps are involved in the . . . process, and human error can occur at each step."[136]

Testimonial hearsay presents another concept to master.[137] While *Crawford* initially seemed to indicate that business records may be nontestimonial,[138] *Melendez-Diaz* made clear that analysts who prepare documents that are testimonial in nature are required to testify at trial in order to satisfy a defendant's Confrontation Clause rights.[139] In a sense, *Crawford* and subsequent case law constitutionalize limitations on the use of the business records exception to avoid the public records exception's limitations on their use in a criminal case: when a person acting as an agent of law enforcement is preparing a record for use against a criminal

131. *Id.* at 320.

132. *Id.* at 321–22 (citation omitted).

133. *Id.* at 324.

134. *Id.*

135. Bullcoming v. New Mexico, 564 U.S. 647, 652 (2011) (holding that "surrogate testimony" does not satisfy the Confrontation Clause: "The accused's right is to be confronted with the analyst who made the certification, unless that analyst is unavailable at trial, and the accused had an opportunity, pretrial, to cross-examine that particular scientist.").

136. *Id.* at 654.

137. *See* G. Michael Fenner, *Today's Confrontation Clause (After* Crawford *and* Melendez-Diaz), 43 CREIGHTON L. REV. 35, 49 (2009) ("Much of the litigation occurring as this is written involves the question of what out-of-court statements are testimonial.").

138. Crawford v. Washington, 541 U.S. 36, 56 (2004).

139. *Melendez-Diaz*, 557 U.S. at 311.

defendant, that agent is likely required to testify.[140] In *Melendez-Diaz*, the documents in question were a "solemn declaration or affirmation made for the purpose of establishing or proving some fact."[141] *Melendez-Diaz* rejected the argument that witnesses need not testify when the testimony at issue is the result of "neutral scientific testing" and stressed that the Confrontation Clause was a *procedural* guarantee, requiring evidence to be assessed through cross-examination.[142]

In admitting GPS evidence as business records, prosecutors would likely prefer to submit the business records and certify them as the amended rules allow. However, when certain kinds of these records are produced by law enforcement personnel, or at its specific direction, these records arguably become testimonial. For example, if a company, in the ordinary course of its business, keeps a record of where its drivers go, that is arguably nontestimonial, since the purpose is primarily for the business. The company may have an interest in reducing fraud, monitoring driver's efficiencies, or increasing transparency to its consumers.[143] However, if law enforcement requests that a specific driver is tracked and a specific record is created, that data arguably *is* testimonial. As *Crawford* states, this type of record qualifies as one that "would lead an objective witness reasonably to believe that the statement would be available for use at a later trial."[144]

An analogy to a more popular example may prove helpful. An analyst who tests blood samples of a suspect for a DNA match, or to determine blood-alcohol content, is contacted by the police to produce a document of the analyst's findings.[145] Even if that analyst certifies that all the ordinary protocols were followed, and the analyst acted in an "independent" and "non-adversarial" position, that analyst is required to testify at trial because the report is generated to aid in a police investigation.[146] However, the potential for DNA errors is well documented.[147] Errors include sample mix-ups, contamination, and fraud.[148] One questions whether the same

140. *See generally Crawford*, 541 U.S. 36.

141. *Melendez-Diaz*, 557 U.S. at 310 (quoting *Crawford*, 541 U.S. at 51).

142. *Id.* at 318.

143. *See* FLEETISTICS, *supra* note 27.

144. *Crawford*, 541 U.S. at 52.

145. *See* Bullcoming v. New Mexico, 564 U.S. 647, 651 (2011).

146. *Id.* at 664.

147. *See, e.g.*, Jackie Valley, *Metro Reviewing DNA Cases After Error Led to Wrongful Conviction*, LAS VEGAS SUN (July 7, 2011, 2:52 PM), http://lasvegassun.com/news/2011/jul/07/dna-lab-switch-led-wrongful-conviction-man-who-ser.

148. *Police Use of DNA: Mistakes, Error and Fraud*, FORENSIC GENETICS POL'Y INITIATIVE, http://dnapolicyinitiative.org/police-use-of-dna-mistakes-error-and-fraud (last visited Sept. 10, 2017).

risks exist for the production of a GPS record and whether the Confrontation Clause should apply here. While GPS evidence may not generally be considered subject to such potential maladies, serious concerns about its accuracy still exist.[149] And due to the amount of weight such evidence is given, the procedural right to assess the evidence through cross-examination should remain a guarantee.

As for the defendant's Confrontation Clause concerns in *Brooks*, the Eighth Circuit acknowledged the Court's shift from *Crawford* to *Melendez-Diaz* and stated "certain business records still may run afoul of the Confrontation Clause if they are testimonial in nature."[150] The question, therefore, was whether the GPS evidence was testimonial. Brooks argued that the reports were testimonial since the GPS evidence was "developed primarily for a law enforcement purpose."[151] Looking to the Supreme Court's decisions in *Bullcoming*, *Bryant*, and *Davis*, the Eighth Circuit reasoned that the GPS reports "were used to track Brooks in an ongoing pursuit;" while the reports were later used at trial, "they were not *created* for this purpose."[152] By distinguishing the evidence from the reports in *Melendez-Diaz* and *Bullcoming*, the Eighth Circuit ruled that the GPS reports "were non-testimonial[] and their admission did not violate Brooks's Confrontation Clause rights."[153]

While neither *Wood* nor *Jackson* addressed Confrontation Clause concerns, *State v. Gardner* cited *Brooks* in addressing a parolee's conviction. *Gardner* concerned a released sex-offender who violated the terms of his supervised release, a violation which was confirmed through the GPS monitor he was wearing after multiple curfew violations.[154] The probation officer was notified about the parolee's failure to return to his "inclusion zone," and he "compiled a report based on the electronic data which was admitted into evidence to illustrate defendant's whereabouts."[155] The parolee appealed his conviction and argued that "the admission of the GPS tracking reports violated his rights" under *Crawford*.[156] The North

149. For example, in *Brooks*, the GPS device experienced a signal failure for five minutes. But no expert was required to testify about the reliability of the records. The court found GPS inherently reliable under Rule 201 and believed that the testimony of the security executive sufficiently laid the foundation for the evidence. United States v. Brooks, 715 F.3d 1069, 1078 (8th Cir. 2013). This relaxed approach to a technological malfunction raised alarms. *See* Kelso L. Anderson, *supra* note 65.

150. *Brooks*, 715 F.3d at 1079.

151. *Id.*

152. *Id.* at 1080.

153. *Id.*

154. State v. Gardner, 769 S.E.2d 196, 197 (N.C. Ct. App. 2014).

155. *Id.* at 198.

156. *Id.*

Carolina Court of Appeals, however, relied on *Brooks* to determine that these records were nontestimonial, since the records were "generated to monitor . . . compliance with . . . post-release supervision conditions" and not "purely for the purpose of establishing some fact at trial."[157] With this interpretation, *Brooks* opens the door to a requirement of not a "primary" but a "pure" purpose, whereby if some reasonable alternative purpose can be established then the defendant's Confrontation Clause right may be skirted. And as GPS data is generated for a variety of reasons, these reasonable alternatives become numerous, and the defendant's rights further diminished.

III. TRACKING MOMENTUM

At first glance, concerns over the admissibility of GPS evidence seem unlikely to raise any eyebrows. Often, the evidence in question is recovered from the vehicle of an individual who is charged with a crime, or connected to the monitoring device of a person recently released from confinement for the commission of a crime. However, most Americans carry some form of tracking technology every day. The information generated from this is being logged somewhere, and increasingly it is being logged at the request and direction of law enforcement personnel.[158] Yet Americans are growing more and more comfortable with the idea of constant surveillance.[159] The question then remains: are there adequate safeguards in place when GPS is gathered from and admitted against an individual?

A. CONFUSING THE PURPOSE OF GPS

Courts admitting GPS evidence have done so through the business records exception. When doing so against a criminal defendant, the admission of hearsay—even through an exception—implicates that defendant's confrontation rights. The exact nature of these rights, though, and which statements a defendant must be able to confront at trial, have undergone drastic changes due to the Supreme Court cases discussed above. *Crawford* and its definition of testimonial hearsay are still being refined.[160] In evaluating GPS evidence as nontestimonial hearsay, courts

157. *Id.* at 199.

158. *See, e.g.*, Andrea Peterson, *Some Companies Are Tracking Workers with Smartphone Apps. What Could Possibly Go Wrong?*, WASH. POST (May 14, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/05/14/some-companies-are-tracking-workers-with-smartphone-apps-what-could-possibly-go-wrong.

159. Yuki Noguchi, *Poll: Majority of American Comfortable with Surveillance*, NAT'L PUB. RADIO (June 12, 2013, 3:00 PM), http://www.npr.org/templates/story/story.php?storyId=191070342.

160. *See* Jeffrey Bellin, *Applying* Crawford*'s Confrontation Right in a Digital Age*, 45 TEX. TECH L. REV. 33, 45 (2012) ("*Crawford*'s testimonial-nontestimonial dichotomy is itself novel . . . .").

may distort the emerging body of law regarding confrontation rights and electronic evidence. Scholars have noted some controversy concerning the ease with which courts have admitted electronic evidence under the business records exception, since a growing amount of regularly conducted activity is captured via electronic means.[161] As these reports are generated routinely and constantly, the question for courts is whether these reports are testimonial and therefore implicate confrontation rights.[162] As Deirdre M. Smith stated plainly, "if it appears that the purpose behind the creation of electronic records involves a potential criminal prosecution, then the hearsay rule, as well as the Confrontation Clause, may foreclose admissibility."[163]

However, judicial determination of the primary purpose of an electronically generated record is difficult ,[164] and courts can often find *a* purpose that allows admissibility. For example, cell-phone records maintained by a telecommunications carrier do not, in and of themselves, implicate a criminal defendant's confrontation rights.[165] However, *Brooks* demonstrates how the purpose inquiry established by *Melendez-Diaz* can be contorted to allow admissibility. The Eighth Circuit found that the "primary purpose" of the bank security company's creation of the records was to locate a robber and recover stolen money.[166] In doing so, the court extended the concept of resolving a present emergency, as laid out by *Davis v. Washington*.[167] But in *Davis*, the emergency exception to *Crawford* covered statements made to address an ongoing emergency: specifically, calls made to a 9-1-1 operator stating that the caller was in immediate physical danger.[168] The nature of the record generation in *Brooks* is unquestionably not the same level of emergency, as the robber was fleeing the crime when the "statements" were being made. Nor, however, is that same record generation like a cell-phone carrier's routine generating of phone records. The records in *Brooks* were not created as part of an ongoing business enterprise but were instead made in direct response to a criminal activity. This, if not testimonial, is at least bordering on

161. *See, e.g.*, Symposium, *The Challenges of Electronic Evidence*, 83 FORDHAM L. REV. 1163, 1218–19 (2014).

162. *Id.* at 1219.

163. *Id.*

164. *Id.*

165. *See* United States v. Yeley-Davis, 632 F.3d 673, 679 (10th Cir. 2011) (allowing cell-phone records to be admitted through a Verizon agent's affidavit, in lieu of testimony, since the records were not created for litigation purposes and were therefore nontestimonial).

166. United States v. Brooks, 715 F.3d 1069, 1079 (8th Cir. 2013).

167. *See id.* at 1079–80.

168. Davis v. Washington, 547 U.S. 813, 817–18, 822 (2006).

testimonial. While a company executive did testify at trial in *Brooks*, the amended exception would allow a certified company record to suffice: no one would be required to give live testimony about the process at trial.

By analyzing the implications of GPS records as hearsay, the underlying policies of *Crawford* are stretched to include those who perform rudimentary administerial functions. In the face of *Crawford*, one scholar has suggested that courts reconsider the definition of "testimonial" when considering "electronic utterances."[169] Testimonial could, more broadly, include the Court's suggestion of "statements that were made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial."[170] This standard would likely apply to the records generated by *Brooks*, since an objective witness could reasonably believe that the GPS tracker placed on a defendant would later be used against him at trial.

B. PRIVACY SURRENDERED

The Sixth Amendment's Confrontation Clause provides a safeguard relating to how evidence is presented against a criminal defendant. The Fourth Amendment limits how evidence is obtained. Because GPS tracking is typically intrusive, its use often implicates Fourth Amendment privacy concerns. In *Katz v. United States*, the Fourth Amendment was interpreted to protect a person's "reasonable expectation of privacy."[171] In *United States v. Jones*, the Court determined that the attachment of a GPS device to "an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment."[172] While the majority in *Jones* put much emphasis on the physical attachment of the device to the individual's car,[173] two concurring opinions examined the issue as an intrusion upon an individual's "reasonable expectation of privacy" under *Katz*.[174] While the *Jones* decision has many implications for the future of electronic surveillance,[175] it is worth noting here for the proposition that

169. Bellin, *supra* note 160, at 44.

170. Crawford v. Washington, 541 U.S. 36, 52 (2004).

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

172. United States v. Jones, 565 U.S. 400, 402 (2012).

173. *Id.* at 949 ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information.").

174. *See id.* at 954–55 (Sotomayor, J., concurring); *id.* at 959–60 (Alito, J., concurring).

175. As Justice Alito noted:

> [T]he Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked. For example, suppose that the officers in the present case had followed respondent by surreptitiously activating a stolen vehicle detection system that came with

government control over how GPS evidence is obtained and presented by agents of the state is potentially problematic.[176] Notably, it has been pointed out that *Jones* stops short of requiring warrants for these searches.[177]

The protections an individual has under the Fourth Amendment do not extend to business records. "In . . . applying *Katz*'s test, the Supreme Court [has] held . . . that individuals have no reasonable expectation of privacy in certain business records owned and maintained by a third-party business."[178] In *Smith v. Maryland*, the "Supreme Court held that telephone users have no reasonable expectations of privacy in dialed telephone numbers" that are later retained in a "third-party telephone company's records."[179] In *United States v. Davis*, the Eleventh Circuit recently expanded this concept by holding that a cell-phone customer has no expectation of privacy of any of the information gathered by his carrier—including cell tower information that kept track of his geographic whereabouts.[180] Perhaps it is decisions such as these that have led some scholars to note how much "privacy norms are changing because of technology" and how the law is struggling to keep up with these changes.[181]

When GPS information is collected and recorded in business records, the generator of that information (typically a cell-phone customer) no longer possesses a privacy interest. In the application of the *Katz* test, the Supreme Court has held "that individuals have no reasonable expectation of privacy in certain business records owned and maintained by a third-party business."[182]

> the car when it was purchased. Would the sending of a radio signal to activate this system constitute a trespass to chattels?

Id. at 962 (Alito, J., concurring). *See also* Jordan Miller, *New Age Tracking Technologies in the Post-*United States v. Jones *Environment: The Need for Model Legislation*, 48 CREIGHTON L. REV. 553, 557 (2015) (arguing that the "Alito rationale should become the prevailing rule").

176. State v. Danney, 283 P.3d 722, 725 (Idaho 2012) (rejecting defendant-appellant's argument that police officers had violated his Fourth Amendment rights by attaching a GPS device to his car, because he failed to object "that the placement . . . constituted a search in violation of the Fourth Amendment").

177. Orin Kerr, *What* Jones *Does* Not *Hold*, VOLOKH CONSPIRACY, (Jan. 23, 2012, 12:50 PM), http://volokh.com/2012/01/23/what-jones-does-not-hold ("[W]e actually don't yet know if a warrant is required to install a GPS device; we just know that the installation of the device is a Fourth Amendment 'search.'").

178. United States v. Davis, 785 F.3d 498, 507 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015).

179. *Id.* at 508 (citing Smith v. Maryland, 442 U.S. 735, 742–46 (1979)).

180. *Id.* at 511.

181. *See* Symposium, *supra* note 161, at 1170.

182. *Davis*, 785 F.3d at 507.

In a concurring opinion to *Jones*, Justice Sotomayor, discussing the Fourth Amendment implications of a warrantless GPS "search," expressed concerns about the government's use and maintenance of GPS records, especially law enforcement personnel's unmitigated access to GPS data and their ability to present it at trial:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . The Government can store such records and efficiently mine them for information years in the future. . . . And because GPS monitoring is cheap . . . it evades the ordinary checks that constrain abusive law enforcement practices.[183]

While the remedy provided by the Fourth Amendment—the exclusionary rule—has much more appeal to a criminal defendant, the Sixth Amendment and the Confrontation Clause's remedy is to have the person responsible for the statements against the defendant appear in court and be subjected to cross-examination. Although the collection of GPS information itself may be more difficult to challenge, the presentation of that information in a criminal trial must be subject to appropriate limitations.

CONCLUSION

Courts have recognized that while "technology [has] changed society's reasonable expectations of privacy," "'[l]aw enforcement tactics must be allowed to advance with technological changes.'"[184] Accordingly, courts have allowed law enforcement wide access to the business records that provide information regarding a person's whereabouts. While a court order is required to acquire these records, the burden on the government agent to obtain them is low.[185]

As this access is more freely granted, the role of agency between the government "requester" and the business-record provider arguably plays a greater and greater role in the discussion of fairness when the records are introduced as evidence. The purpose of creating these records—applicable to a testimonial hearsay analysis—is a salient question for courts to

183. United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring).

184. *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013) (citation omitted).

185. *See id.* at 604–06 (rejecting argument that the Secured Communications Act "violates the Fourth Amendment [by allowing] the United States to obtain a court order compelling a cell phone company to disclose historical cell site records merely based on a showing of 'specific and articulable facts,' rather than probable cause.").

consider when considering their admissibility. Courts now assume that phone users know the phone company will "connect calls, document charges, and assist in legitimate law-enforcement investigations."[186] As these purposes merge, the question of what business the companies are engaged in becomes murkier. Since GPS data is generated nearly continuously for every cell-phone-carrying member of the American public, the purpose behind the creation of the recording of that data is strictly business. Therefore, any purpose analysis within the testimonial hearsay framework is effectively rendered unnecessary. When a government agent intervenes, though, the line of inquiry should shift. The "objective witness" standard would demand that the record-creator and government-presenter establish, in person, the purpose for the surveillance, which at the very least provides criminal defendants with procedural constitutional protections.

Considering the manner in which GPS evidence is created is the first step in determining its admissibility. Absent some involvement of a human agent, GPS evidence more neatly falls within the category of computer-generated records and should therefore be considered non-hearsay. Yet when a human agent is involved in the creation of a record, courts should honor the limitations of the public records exception and a defendant's rights under the Confrontation Clause. Courts should analyze the purpose for which the data is generated when undertaking a *Crawford* analysis. Often, the purpose includes eventual use at trial, rendering that data testimonial and requiring an in-court declarant.

Yet criminal defendants often do not get a chance to confront any witnesses. In *Melendez-Diaz*, the Court noted that very few cases go to trial, and that most defendants stipulate to this type of evidence.[187] This seldom-invoked right to trial by jury, combined with a system—GPS—that is perceived to be practically error-proof, may lead some to question just how far *Crawford* should extend and if these procedural safeguards are necessary. But concerns about the invasiveness of GPS data, which are arguably inadequately addressed through the Fourth Amendment's current landscape, can at least find a voice in the courtroom through the requirement of live, in-person testimony about how and why records are produced. The trend—in both the public's and courts' perception—is towards a reduction in what is considered private information. By extending Sixth Amendment protections to cover testimonial GPS

186. *Davis*, 785 F.3d at 511.
187. Melendez-Diaz v. Massachusetts, 557 U.S. 305, 325–28 (2009).

evidence, courts can—at a minimum—make sure that criminal defendants' constitutional rights are not completely lost.