

**[J-51-2022] [MO: Todd, C.J.]
IN THE SUPREME COURT OF PENNSYLVANIA
MIDDLE DISTRICT**

COMMONWEALTH OF PENNSYLVANIA,	:	No. 93 MAP 2021
	:	
Appellee	:	Appeal from the Order of the
	:	Superior Court dated January 8,
v.	:	2021, reargument denied March 10,
	:	2021, at No. 2427 EDA 2019
	:	Affirming the Montgomery County
JAMAL WALLACE,	:	Court of Common Pleas, Criminal
	:	Division, Judgment of Sentence
Appellant	:	dated May 23, 2019 at No. CP-46-
	:	CR-0004008-2018.
	:	
	:	ARGUED: September 15, 2022

CONCURRING OPINION

JUSTICE WECHT

DECIDED: February 22, 2023

The Majority concludes that GPS data transmitted from an ankle monitor—which placed Jamal Wallace at the intersection of Spruce and Willow Streets in Norristown on the night of the relevant assault¹—does not constitute hearsay under the plain language of the Pennsylvania Rules of Evidence.² In doing so, it effectuates a significant change in our law to which I cannot assent. For decades, Pennsylvania courts have analyzed the admission of computer-generated evidence under the business records exception to the rule against hearsay.³ While this Court’s precedent may not compel endorsing that

¹ Wallace himself was not wearing the ankle monitor. Rather, his co-defendant, Mason Clary, was wearing it as a condition of his release on state parole. The statement of a third man, C.S., placed both Wallace and Clary at the shooting. See Notes of Testimony (“N.T.”), 3/5/19, at 225-26.

² See Maj. Op. at 17; Pa.R.E. 801(a).

³ See Pa.R.E. 803(6).

evidentiary categorization today, the Majority discards the *status quo* using logic that threatens to erode evidentiary protections and reinvent how courts treat the output of machines. For the reasons that follow, I concur in the result only.

In the interest of clarity to the bench and bar, two critical distinctions must be made at the outset. First, computer-*stored* evidence and computer-*generated* evidence present different analytical starting points.⁴ Emails, word processing files, and voice recordings are examples of assertions that human beings make and store electronically, and the hearsay framework applies to them as comfortably as it would to a handwritten letter or to a recording on a cassette tape.⁵ But evidence generated by a computer—such as a test result in a laboratory, a reading from a radar gun, records of phone calls, or ATM receipts—poses a different challenge, in that it becomes less clear the degree to which human beings, as opposed to the computer itself, are responsible for the output.⁶ This second category might be separated further into evidence that requires human operation or initiation (*i.e.*, a DNA test) and that which does not (*i.e.*, metadata).

The next critical distinction, which pertains to computer-generated evidence, is between the individual responsible for designing the algorithm, program, or machine at issue and the individual who operates it. In the case *sub judice*, someone developed and programmed the ankle monitors and the GPS system that Attenti—the company that contracted with the Pennsylvania Board of Probation and Parole to supply electronic

⁴ See Rudolph J. Peritz, *Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence*, 80 NW. U. L. REV. 956, 980 (1986).

⁵ See, e.g., *Commonwealth v. Fitzpatrick*, 255 A.3d 452, 470-72 (Pa. 2021) (analyzing an email under the hearsay framework).

⁶ See generally Andrea Roth, *Trial by Machine*, 104 GEO. L.J. 1245, 1270-76 (2016); Brian Sites, *Machines Ascendant*, 3 GEO. L. TECH. REV. 1, 23-24 (2018); Adam Wolfson, Note, “*Electronic Fingerprints*”: *Doing Away with the Conception of Computer-Generated Records as Hearsay*, 104 MICH. L. REV. 151, 151 (2005).

monitoring equipment—used to track state parolees; but it presumably was not the same person who provided this particular information about this particular ankle monitor in service of the Commonwealth’s case.

The Majority observes that our Rules of Evidence, for purposes of the hearsay rule, define a statement as “a *person’s* oral assertion, written assertion, or nonverbal conduct,”⁷ and thereby concludes that, because “the relevant assertion . . . was not made *by a person* but collected electronically by the GPS monitoring device,” it “cannot constitute hearsay.”⁸ The Majority finds no barrier to such a conclusion in *Commonwealth v. Le*, 208 A.3d 960 (Pa. 2019), or in *Commonwealth v. Carter*, 932 A.2d 1261 (Pa. 2007), because “the contested evidence [in those cases] was merely *presumed to be* hearsay for purposes of analyzing a hearsay exception.”⁹ The Superior Court, meanwhile, appeared to conclude that the GPS system itself was the declarant.¹⁰

While I agree that *Le* and *Carter* do not compel any particular result here,¹¹ that treatment of these cases fails to grapple with the complexity of the question before us. A

⁷ Pa.R.E. 801 (emphasis added).

⁸ Maj. Op. at 17 (emphasis in original).

⁹ *Id.* (emphasis in original); *id.* at 18 (finding that the portions of *Le* and *Carter* upon which Wallace relies constitute, “[a]t best . . . *dicta*”).

¹⁰ *Commonwealth v. Wallace*, 244 A.3d 1261, 1271 (Pa. Super. 2021) (citing with approval *United States v. Lizarraga-Tirado*, 789 F.3d 1107, 1109-10 (9th Cir. 2015) (holding that, because “the program makes the relevant assertion,” there is “no statement as defined by the hearsay rule”); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) (“a statement is something uttered by a person, so nothing ‘said’ by a machine . . . is hearsay”) (cleaned up); *People v. Rodriguez*, 224 Cal.Rptr.3d 295, 314 (Cal. App. Ct. 2017) (“there was ‘no statement being made by a person’”); *Wisconsin v. Kandutsch*, 799 N.W.2d 865, 879 (Wis. 2011) (“the report was generated as the result of an automated process free of human intervention”) (cleaned up)).

¹¹ In *Le*, this Court found that a challenge to the admission of phone records had not been preserved, and therefore did not consider the merits. 208 A.3d at 970-71. In *Carter*, (continued...)

computer program does not make statements. Like any other tool of fallible human design, people *use* it *to* make statements. After all, “[a] computer program is nothing more than an organized series of commands given by a human computer programmer,” and “[e]very action taken by a computer is taken only at the command of a human programmer.”¹² Just as a clock cannot wind itself to line up with Eastern Standard Time, a computer cannot teach itself how to locate an ankle monitor on a plane of coordinates, nor can it instruct itself to do so in a particular instance. Furthermore, for an assertion to be “collected” from somewhere,¹³ it must be made in the first place.

The Majority seems to suggest that courts analyzing computer-generated evidence like cell phone records and drug test results on hearsay grounds have simply ignored the clear textual commands of federal and state rules of evidence. In *Melendez-Diaz v. Massachusetts*, the United States Supreme Court scrutinized the admission of a lab report identifying a white powdery substance as cocaine under the business records

this Court explicitly reached its conclusion “regardless of whether [a lab report fell] within” the business record exception. 932 A.2d at 1269.

¹² Christian Chessman, Note, *A “Source” of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 181 (2017). While “program sophistication and speed may create the illusion that the programs function autonomously,” all of the computer’s actions stem from source code created by a human. *Id.* at 182. As Chessman further opines:

[p]rogram output is neither neutral nor objective because programs are, at their base, written human speech. That humans are one step removed from program output is not equivalent to the removal of the human element. If computer programs are no more reliable . . . than human statements, then many established concerns about human witness testimony readily apply to evidence produced by computer programs, including bias, malfeasance, and even simple mistakes. Thus, computer programs are not more reliable than human statements because they are human statements--and no more than human statements.

Id. at 185-86.

¹³ Maj. Op. at 17.

exception.¹⁴ Like our rules, the Federal Rules of Evidence define “statement” as “a *person’s* oral assertion, written assertion or nonverbal conduct.”¹⁵ But that definition did not hinder or impede the Court’s analysis. Years earlier, and before this Court’s comments in *Le* and *Carter*, the Superior Court held that cell phone records—which showed that the last phone number the defendant dialed before the murder was the victim’s—were admissible under the business records exception.¹⁶ The Commonwealth Court similarly has considered a former employee’s drug test results under the same framework.¹⁷ Examples like this from both state courts and federal courts abound.¹⁸ I find it improbable that judge after judge has overlooked the word “person” in deciding these cases. The more likely explanation for their conclusions, in my view, is that those

¹⁴ 557 U.S. 305, 321 (2009).

¹⁵ F.R.E. 801(a) (emphasis added).

¹⁶ See *Commonwealth v. McEnany*, 732 A.2d 1263, 1272-73 (Pa. Super. 1999); see also *Commonwealth v. Lewis*, 1673-1679 EDA 2021, 2022 WL 3714540 (Pa. Super. Aug. 29, 2022) (non-precedential decision) (admitting cell phone records under the business records exception).

¹⁷ See *Turner v. Unemployment Compensation Bd. of Review*, 899 A.2d 381, 386-87 (Pa. Cmwlth. 2006)

¹⁸ See *Kilgore v. State*, 763 S.E.2d 685, 687 (Ga. 2014) (holding that phone records were admissible under the business records exception to the hearsay rule); Ga. Code Ann. § 24-8-801 (defining “statement” as the “oral or written assertion or nonverbal conduct of a person”) (cleaned up) (emphasis added); *People v. McDaniel*, 670 N.W.2d 659, 661 (Mich. 2003) (“The laboratory report at issue is, without question, hearsay.”); M.R.E. 801(a) (defining “statement” as “an oral or written assertion or nonverbal conduct of a person”) (cleaned up) (emphasis added); see also *United States v. Moore*, 923 F.2d 910, 914 (1st Cir. 1991) (holding that computer-generated “loan histories” constituted hearsay); *United States v. Bonomolo*, 566 Fed.Appx. 71, 73-74 (2nd Cir. 2014) (admitting computer-generated spreadsheets detailing federal grants under the business records exception to the rule against hearsay); *Perkins v. Rock-Tenn Serv., Inc.*, 700 Fed.Appx. 452, 461 (6th Cir. 2017) (admitting computer-generated evidence of notices being sent under the business records exception to the rule against hearsay).

courts have *sub silentio* endorsed Wallace's position, and recognized that some "person" (e.g., a designer or an operator) was responsible for the statement's creation.¹⁹

Critically, Wallace is not calling for total exclusion of the GPS evidence. Rather, he asserts that, because "a human created [the] algorithm" in question, an individual "with actual knowledge of how it works should be available for cross-examination on its reliability[.]"²⁰ The Commonwealth offered the testimony of David Dethlefsen, "a sales representative for Attenti who had absolutely no idea how the GPS system worked," who could not comment upon the "process of generating or obtaining the records," or "whether the process had produced accurate results."²¹ Dethlefsen

had not had any training on how to determine if the data was accurate, he did not think any calibration was performed on the devices, and he noted that the accuracy of the device was determined using a proprietary algorithm which was not given to the defense or evaluated by experts.

¹⁹ The Majority defends its treatment of these cases by positing that those courts have engaged in the "common practice" of "forego[ing] addressing what might be viewed as a more difficult legal question . . . where it maybe resolved on an alternative basis." Maj. Op. at 21 n.21. But would the more straightforward and simpler resolution not have been to forego any analysis of exceptions by determining that the proffered evidence fell outside of the hearsay framework in the first place? Per the Majority's rationale, there is no difficult legal question to avoid, because computers are not people. Furthermore, none of the cases in question stated an assumption that the proffered evidence was hearsay for purposes of analyzing an exception, nor did they hold that the proffered evidence was inadmissible. Rather, they held that evidence was admissible under the business records exception *to the hearsay rule*. See *Kilgore*, 763 S.E.2d at 687 (holding that cell phone records "were admissible under the business records exception to the hearsay rule"); *McEnany*, 732 A.2d at 1273 ("[W]e are satisfied that the Commonwealth presented sufficient evidence to justify a presumption of the trustworthiness of [the cell phone records] so as to offset *the hearsay character* of the evidence.") (emphasis added); *Bonomolo*, 556 Fed.Appx. at 73 ("Rule 803(6) creates an exception to the hearsay rule"). A necessary analytical prerequisite to any such finding, unless it has been assumed, is that the evidence *is* subject to the hearsay rule, and can only be saved by an exception. To admit something as a business record is to deem it hearsay.

²⁰ Wallace Br. at 33.

²¹ *Id.* at 46.

Instead, it was based on a company secret, and the accuracy was certainly not evaluated by peer review studies.²²

In other words, Dethlefson indicated that he had neither designed nor operated the technology that located Clary's ankle monitor, and he implied that someone else at Attenti knew how it worked. Wallace's most compelling argument is that this testimony confirms that Dethlefsen cannot be the declarant because he was in no way responsible for the statement coming into existence,²³ and that this case therefore equates to the traditional hearsay scenario of an individual saying, "Someone told me that John Doe stole the victim's car, and I have reason to believe that she was telling the truth."

The Majority suggests that "[t]he best way to advance the truth-seeking process with respect to [machine-generated] 'statements' is not through cross-examination of the machine operator, but through the process of authentication."²⁴ I am (at best) skeptical of this contention. Authentication is a relatively low threshold,²⁵ asking only whether the proffered evidence is what it purports to be.²⁶ Wallace does not contest that the print-out

²² *Id.* at 47 (citing N.T., 3/5/19, at 161).

²³ The same can be said of Clary's parole agent, Harry Gaab. Although he collected the GPS data from Attenti, he was not responsible for its creation nor was he knowledgeable about its function or accuracy.

²⁴ Maj. Op. at 21 (quoting *United States v. Lamons*, 532 F.3d 1251, 1264-54 (11th Cir. 2008)); see also Pa.R.E. 104(e) (establishing that even when a "court rules that evidence is admissible"—i.e., that it is relevant and authentic—"this does not preclude a party from offering other evidence relevant to the weight or credibility of that evidence.")

²⁵ See, e.g., *United States v. Lundy*, 676 F.3d 444, 453 (5th Cir. 2012) ("the low threshold for authentication"); *Mullens v. State*, 197 So. 3d 16, 25 (Fla. 2016) ("authentication is a relatively low threshold that only requires a *prima facie* showing that the proffered evidence is authentic; the ultimate determination of the authenticity of the evidence is a question for the fact-finder").

²⁶ See Pa.R.E. 901; see also *Commonwealth v. Brooks*, 508 A.2d 316, 318 (Pa. Super. 1986) ("Generally, two requirements must be satisfied for a document to be admissible: it must be authenticated and it must be relevant. In other words, a proponent (continued...)")

of coordinates and movements that the prosecution submitted is GPS data, or that it originated from Attenti's supervision of Clary. In other words, he concedes that it is what it purports to be. Wallace instead asserts that without someone from Attenti to substantiate this evidence and answer questions about what conclusions might be drawn therefrom, allowing it into court in the first place would be prejudicial. He certainly might have been able to convince the jury not to trust or ascribe weight to the GPS data after its admission, but the same could be said of any out-of-court statement.²⁷ The entire hearsay framework stems from the basic premise that it is often best to exclude allegedly untrustworthy evidence before it can shape a factfinder's perception of the events in question. That is the ruling that Wallace seeks, and to shoehorn determinations about the trustworthiness, weight, and credibility of the GPS data into an authentication inquiry misunderstands both the purpose of Rule 901 and the nature of his challenge.²⁸

In light of my understanding that computers do not make statements "in a vacuum,"²⁹ my doubts as to the ability of an authentication challenge to remedy the

must show that the document is what it purports to be and that it relates to an issue or issues in the truth determining process.").

²⁷ See Laurence H. Tribe, Comment, *Triangulating Hearsay*, 87 HARV. L. REV. 957, 958 (1974) (describing how "the perceived untrustworthiness" of out-of-court acts and utterances has led "the Anglo-Saxon legal system to exclude [them] as hearsay despite [their] potentially probative value").

²⁸ If the concern animating Wallace's challenge is that the algorithm underlying Attenti's GPS monitoring system is faulty or otherwise unreliable, the best way to raise it would not be through hearsay or authentication. There are other ways of discrediting evidence. Wallace could have enlisted an expert in GPS evidence to discuss its shortcomings, or subpoenaed employees at Attenti more familiar with the nuts-and-bolts of the technology than Dethlefsen. Defendants in his position are not without a path to meaningfully challenge this type of evidence, but it may not lead through hearsay or authentication.

²⁹ Wallace Br. at 37; see also *supra* note 5. The Majority counters that, per Rule 901(b)(9), a proponent of evidence "may be asked to prove that a machine or process produces an accurate result." Maj. Op. at 22. This point is not persuasive for two reasons. (continued...)

prejudice that Wallace foresees, and a bevy of case law that I find persuasive,³⁰ I would hold that the GPS data used to locate Wallace constituted hearsay, and I respectfully disagree with the Majority's contrary conclusion. The statement—that Clary and therefore Wallace were at the intersection of Spruce and Willow Streets in Norristown at 8:21 PM on April 6, 2018—was not Dethlefsen's or Gaab's to make. It was made out of court, either by the designer of Attenti's GPS tracking system or the operator of that system who documented Clary's movements, and repeated by Dethlefsen and Gaab for the truth of the matter asserted. I concur in the result, however, on the grounds that the GPS data was admissible under the business records exception to the hearsay rule.

The business records exception is found in Pa.R.E. 803, which provides in pertinent part:

The following are not excluded by the rule against hearsay, regardless of whether the declarant is available as a witness:

. . .

(6) *Records of a Regularly Conducted Activity*. A record (which includes a memorandum, report, or data compilation in any form) of an act, event or condition if:

(A) the record was made at or near the time by--or from information transmitted by--someone with knowledge;

(B) the record was kept in the course of a regularly conducted activity of a "business", which term includes business,

First, this language in no way indicates a requirement ("may be asked"), and it appears in a non-exhaustive list of examples. See Pa.R.E. 901(b). Second, the Majority's reading is inverted. The language it cites allows the proponent of "[e]vidence *describing a process or system*" to authenticate that evidence by showing that the process or system "produces an accurate result." *Id.* (emphasis added). But Wallace is not challenging evidence that *describes* Attenti's GPS system, he is challenging its *result*. In fact, what he seeks is evidence that describes the system. Per Rule 901(b)(9), the proponent of evidence describing a GPS system could demonstrate its authenticity by showing—by way of tests or examples—that it accomplishes its intended purpose. It does not follow, however, that the appropriate avenue for challenging a result of that system lies in authentication.

³⁰ See *supra* notes 13-17 and accompanying text.

institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit;

(C) making the record was a regular practice of that activity;

(D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and

(E) the opponent does not show that the source of information or other circumstances indicate a lack of trustworthiness.³¹

As long as an “authenticating witness can provide sufficient information relating to the preparation and maintenance of the records to justify a presumption of [their] trustworthiness,” the proponent of a business record has provided “a sufficient basis . . . to offset the hearsay character of the evidence.”³² Though Dethlefsen could not have qualified as the declarant given his lack of knowledge about how Attenti’s GPS tracking worked, he unquestionably qualified as a custodian of the company’s records because he had access to them and could provide information about their preparation and maintenance.³³

Wallace’s argument that the GPS data does not qualify as a business record because it was prepared in anticipation of litigation is unavailing. In *Melendez-Diaz*, the United States Supreme Court explained that:

[d]ocuments kept in the regular course of business may ordinarily be admitted at trial despite their hearsay status. See Fed. Rule Evid. 803(6). But that is not the case if the regularly conducted business activity is the production of evidence for use at trial. Our decision in *Palmer v. Hoffman*, 318 U.S. 109, (1943), made that distinction clear. There we held that an

³¹ Pa.R.E. 803(6).

³² *In re Indyk’s Estate*, 413 A.2d 371, 373 (Pa. 1979).

³³ See *Virgo v. W.C.A.B. (Cnty. of Lehigh-Cedarbrook)*, 890 A.2d 13, 20 (Pa. Cmwlth. 2005) (“[I]t is not essential to produce either the person who made the entries or the custodian of the record at the time the entries were made or that the witness qualifying the business records even has personal knowledge of the facts reported in the business record.”).

accident report provided by an employee of a railroad company did not qualify as a business record because, although kept in the regular course of the railroad's operations, it was "calculated for use essentially in the court, not in the business." *Id.* at 114. The analysts' certificates—like police reports generated by law enforcement officials—do not qualify as business or public records for precisely the same reason. See [Fed.] Rule [Evid.] 803(8) (defining public records as "excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel").³⁴

Unlike the accident report in *Palmer* and the laboratory report in *Melendez-Diaz*, the GPS data at issue here did not spawn into being for purposes of this or any trial. Rather, as a company whose sole purpose is to track parolees, Attenti continuously produced and maintained records of Clary's movements. Furthermore, the records were not "calculated for use . . . in the court,"³⁵ as opposed to in business; tracking parolees *is* Attenti's business and, as the trial court noted, the records' primary purposes are "supervision and sanction" by Attenti's client, the Pennsylvania Board of Probation and Parole³⁶ The company would have kept them regardless of whether Clary ever violated parole, and though parole violations certainly may result in litigation, not all do. Accordingly, the GPS data here are more akin to the phone records that were admitted in *McEnany*³⁷ than they are to, for instance, results from a state police crime lab.³⁸

³⁴ *Melendez-Diaz*, 557 U.S. at 321-22 (cleaned up); see *contra Commonwealth v. May*, 898 A.2d 559, 565 (Pa. 2006) (admitting a police report under the business records exception).

³⁵ *Palmer*, 318 U.S. at 114.

³⁶ Tr. Ct. Op. at 14-16.

³⁷ See 732 A.2d at 1273 (emphasizing that the records were "generated at the moment a phone call is made").

³⁸ While I reserve judgment upon other questions in this vein should they come before this Court, it should be noted that my analysis is grounded in the record, and should not be construed as a *per se* rule. See N.T., 3/5/2019, at 154-57 (Dethlefsen testifying about what information is collected in Attenti's GPS records and his access to them). If, for instance, Attenti did not regularly maintain records of parolees' movements, and only (continued...)

I would affirm the Superior Court’s judgment on those grounds. Though it may not be felt in this case (because of the applicability of the business records exception), sooner or later, the Majority’s approach will prove untenable. Prosecutors will rely upon computer-generated evidence and, without having to demonstrate why that evidence should be entitled to a presumption of trustworthiness through an exception to the hearsay rule, wield it to put defendants on their back foot. They will shield their cases from evidentiary objections by laundering evidence and conclusions through algorithms and code. It will become defendants’ unenviable burden to convince jurors and judges that complex, inscrutable machinery—despite its “mechanical appearance and apparently simple output,” along with its “veneer of objectivity and certainty”³⁹—has erred. This Court’s guidance will have undercut the relevance of the business records exception⁴⁰ and bought into the fiction that when a series of human commands is complicated enough, no one is speaking at all.⁴¹

turned on a device or extracted GPS data at the direction of state police when a monitored individual was suspected to have committed a violation, the “anticipation of litigation” exception to the business records exception conceivably might apply.

³⁹ Roth, *Trial by Machine*, *supra* n.6, at 1269-70; see also *id.* (opining that complex computer programs and machines not only “obscured how the sausage is made, they obscure that their output is sausage at all”). For more on the “black box” problem, see Brian Sites, *Machines Ascendant: Robots and the Rules of Evidence*, 3 GEO. L. TECH. REV. 1, 23-24 (2018) (quoting Andrea Roth, *Machine Testimony*, 166 YALE L. J. 1972, 1977-78 (2017)).

⁴⁰ *Cf. Commonwealth Fin. Sys., Inc. v. Smith*, 15 A.3d 492, 499 (Pa. Super. 2011) (finding that computer-generated billing statements and account information were not admissible under the business records exception where the proponent of the evidence failed to “establish circumstantial trustworthiness”).

⁴¹ While the Majority suggests that “advancements in software systems may eventually call into question the efficacy of our hearsay and perhaps other evidentiary rules,” Maj. Op. at 23 n.22, I believe that day has come. In order to meet it, this Court does not need to “stretch . . . common sense meanings of oral or written statements under Rule 801.” *Id.* It could simply recognize that “[a] computer program is nothing more than an organized series of commands given by a human computer programmer,” and that (continued...)

“[e]very action taken by a computer is taken only at the command of a human programmer.” Chessman, *supra* note 12, at 181.