

RECEIVED

Jun 09 2026

SC Court of Appeals

STATE OF SOUTH CAROLINA
IN THE COURT OF APPEALS

Appeal from Marion County

Honorable Michael Nettles, Circuit Court Judge

THE STATE,

RESPONDENT,

V.

TERRY ALLEN PAIGE, JR.,

APPELLANT

APPELLATE CASE NO. 2025-001075

FINAL BRIEF OF APPELLANT

W. CHANDLER NORVILLE
Appellate Defender

South Carolina Commission on Indigent Defense
Division of Appellate Defense
PO Box 11589
Columbia, SC 29211-1589
(803) 734-1330

ATTORNEY FOR APPELLANT

TABLE OF CONTENTS

TABLE OF CONTENTSi

TABLE OF AUTHORITIES..... ii

STATEMENT OF ISSUES ON APPEAL 1

STATEMENT OF THE CASE2

STANDARDS OF REVIEW3

ARGUMENTS

I.

The trial court erred in admitting vehicle location data derived from a vehicle “infotainment” system because the process used to collect the data was insufficiently reliable4

Relevant facts4

Discussion7

A. The trial court was not presented with evidence sufficient to find the evidence reliable under *Council*..... 10

B. Software that makes use of secret, proprietary source code, when entered through expert witnesses who have never seen that source code, much less understand it, should be considered inherently unreliable..... 16

II.

The trial court erred in imposing a five-year sentence for possession of a weapon during the commission of a violent crime when it had already imposed a life sentence.20

Relevant facts20

Discussion20

CONCLUSION22

TABLE OF AUTHORITIES

United States Cases

Crawford v. Washington, 541 U.S. 36 (2004)..... 17

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993)..... *passim*

Maryland v. Craig, 497 U.S. 836 (1990) 17

Melendez-Diaz v. Massachusetts, 557 U.S. 305 (2009)..... 15, 16

Ohio v. Roberts, 448 U.S. 56 (1980)..... 17

United States v. Scheffer, 523 U.S. 303 (1998)..... 12

South Carolina Cases

Clark v. Cantrell, 339 S.C. 369, 529 S.E.2d 528 (2000) 3

Holmes v. South Carolina, 547 S.C. 319 (2006)..... 17

Matter of the Care and Treatment of Bilton, 432 S.C. 157, 851 S.E.2d 442 (Ct. App. 2020)..... 11

State v. Council, 335 S.C. 1, 515 S.E.2d 508 (1999) 8, 10, 11, 19

State v. Franks, 432 S.C. 58, 849 S.E.2d 580 (Ct. App. 2020)..... 9

State v. Harris, 318 S.C. 178, 456 S.E.2d 433 (Ct. App. 1995)..... 3

State v. Meador, 425 S.C. 625, 825 S.E.2d 53 (Ct. App. 2019) 8

State v. Phillips, 430 S.C. 319, 844 S.E.2d 651 (2020) 8, 10

State v. Plumer, 439 S.C. 346, 350, 887 S.E.2d 134, 137 (2023)..... 20

State v. Sidell, 262 S.C. 397, 205 S.E.2d 2 (1974)..... 3

State v. Sledge, 428 S.C. 40, 832 S.E.2d 633 (Ct. App. 2019)..... 20

State v. Tapp, 398 S.C. 376, 728 S.E.2d 468 (2012)..... 8

State v. White, 382 S.C. 265, 676 S.E.2d 684 (2009)..... 3

Other Jurisdictions

K.W. v. Armstrong, 180 F.Supp.3d 703 (D. Idaho 2016)..... 16

Perma Research & Development v. Singer Co., 542 F.2d 111 (2d Cir. 1976) 15

Solon v. United States, 2013 WL 12321956 (D. Wyo. May 24, 2013)..... 12

State v. Melsky, 2013 WL 1776037 (N.J. Sup. Ct. App. Div. Apr. 26, 2013) 19

State v. Schwartz, 447 N.W.2d 422 (Minn. 1989)..... 16

United States v. Washington, 498 F.3d 225 (4th Cir. 2007) 15

Rules

Rule 702, SCRE *passim*

Statutes

S.C. Code Ann. § 16-23-490(A) 20

Other Authorities

3 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 373 (1768)..... 17

Andrea Roth, *Machine Testimony*, 126 YALE L. J. 1972 (2017)..... 14

Andrea Roth, *Trial by Machine*, 104 GEO. L. J. 1245 (2016) 18

Christian Chessman, *A “Source” of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CAL. L. REV. 179 (2019)..... 14, 17, 18, 19

Christopher S. Meffert, et al., *Deleting Collected Digital Evidence by Exploiting a Widely Adopted Hardware Write Blocker*, 18 DIGITAL INVESTIGATION 87, 88 (2016), <https://doi.org/10.1016/j.diin.2016.04.004> (last accessed Dec. 1, 2025) 5, 12, 13

Darrel Ince, et al., *The Case for Open Computer Programs*, 482 NATURE 485 (2012) 18, 19

Edward Hannan, *Computer-Generated Evidence: Testing the Envelope*, 63 DEF. COUNS. J. 353 (1996)..... 13

Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where are We*,
29 HASTINGS COMM. & ENT. L. J. 421 (2007)..... 9

Louis Brandeis, *What Publicity Can Do*, HARPER’S WEEKLY, Dec. 20, 1913..... 17

Peer Review, MERRIAM-WEBSTER COLLEGIATE DICTIONARY (11th ed. 2003) 11

President’s Council of Advisors on Science and Technology, *Report to the President: Forensic
Science in Criminal Courts: Ensuring Scientific Validity of Feature Comparison Methods*
(Sep. 2016), [https://obamawhitehouse.archives.gov/sites/
default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf) (last accessed
Dec. 1, 2025)..... 15

Yeonghun Shin, et al., *Digital Forensics Case Studies for In-Vehicle Infotainment Systems Using
Android Auto and Apple CarPlay*, 22 SENSORS 7196 (2022),
<https://doi.org/10.3390/s22197196> (last accessed Dec. 1, 2025)..... 12, 13

STATEMENT OF ISSUES ON APPEAL

I. Whether the trial court erred by refusing to exclude vehicle location data obtained from a vehicle “infotainment” system on the ground that the process used to obtain the data is insufficiently reliable?

II. Whether the trial court erred in imposing a five-year sentence for possession of a weapon during the commission of a violent crime when it also imposed a life sentence?

STATEMENT OF THE CASE

On May 5, 2022, the Marion County grand jury indicted Appellant for murder, burglary in the first degree, and possession of a weapon during the commission of a violent crime. R. 358-63. The case was tried on May 19, 2025, before the Honorable Michael Nettles and a jury. R. 1. Ralph Wilson, Jr., represented Appellant. R. 1. Todd Tucker represented the state. R. 1. On May 23, 2025, the jury convicted Appellant on all counts. R. 353-54. Judge Nettles sentenced Appellant to life imprisonment for murder, fifteen years for burglary first, and five years for the gun charge, to run concurrently. R. 355.

This appeal follows.

STANDARDS OF REVIEW

As to Issue I: “A trial court’s decision to admit or exclude expert testimony will not be reversed absent a prejudicial abuse of discretion.” *State v. White*, 382 S.C. 265, 269, 676 S.E.2d 684, 686 (2009). “The qualification of an expert witness and the admissibility of the expert’s testimony are matters largely within the trial court’s discretion.” *State v. Harris*, 318 S.C. 178, 181, 456 S.E.2d 433, 435 (Ct. App. 1995).

As to Issue II, the trial court has broad discretion when sentencing a defendant within statutory limits. *State v. Sidell*, 262 S.C. 397, 398, 205 S.E.2d 2, 3 (1974). However, the trial court abuses that discretion when its ruling is based on an error of law. *Clark v. Cantrell*, 339 S.C. 369, 389, 529 S.E.2d 528, 539 (2000).

ARGUMENTS

I.

The trial court erred in admitting vehicle location data derived from a vehicle “infotainment” system because the process used to collect the data was insufficiently reliable.

Relevant facts

On October 25, 2023, at around 9:20 a.m., Gloria Swinton was murdered in her home. Appellant was eventually charged with her murder, and the case proceeded to trial. Appellant’s first trial ended in a mistrial after some “outburst” from a member of the decedent’s family. R. 23, ll. 8-14. The second trial began on May 19, 2025. The portion of the evidence challenged by Appellant here was technological evidence related to data downloads from a vehicle.

The technology at issue is a software program created by a corporation called Berla. R. 82-84. Essentially, the software allows police officers to download saved data from a vehicle’s “infotainment,” or “IVI” system, which was described as the “center screen that carries...anything you would see on the screen,” and interpret that data. R. 82. Berla must design different software for every single car manufacturer, because every manufacturer includes different data in their systems. R. 106, ll. 8-12.

Before trial, Appellant moved to suppress the evidence gathered from his vehicle’s infotainment system. R. 77. During a pretrial hearing, the state called Jason Morgan from the Pennsylvania State Police to testify. R. 80. Morgan was the system analyst who gathered the data from the vehicle that was presented at trial. R. 89, ll. 2-9. However, he was the second Pennsylvania police officer to do so; the original system analyst was also a Pennsylvania State Police officer who had retired since doing the data gathering, which resulted in that data being deleted. R. 89-90.

When asked about his qualifications, Morgan admitted that he had never been qualified by a court as an expert witness. R. 85, l. 2. He had no training in any sort of digital forensics, other than a week-long training required by Berla. R. 91, ll. 15-20. He had no knowledge about whether Berla's program had ever been subjected to peer review. R. 92, ll. 16-18. He knew nothing about how Berla's code works. R. 93, ll. 6-8. He knew nothing about the "debugging" procedures for that code or even what programming language Berla is written in. R. 94-96. When asked whether Berla employed write blockers—which would stop its code from being edited by anyone outside of Berla¹—Morgan responded that he did not know what write blockers were. R. 97, ll. 7-9. When asked about specific peer reviewed studies regarding Berla's software, Morgan was familiar with none. R. 97-98. Morgan was also unfamiliar with the software's error rate. R. 93.

Next, the state called Mark Restori, a former Pennsylvania State Police officer who had since retired. R. 100, ll. 7-11. Restori was the officer who downloaded the since-deleted original data from Appellant's vehicle. He testified that he had been qualified as an expert witness in the field of infotainment systems one time in a federal court in Nevada. R. 102-03. He testified that he was never made aware of any problems with the software. R. 105, ll. 1-4. When asked about peer review of Berla's software, he was not familiar with any attempts to peer review the software, other than stating that other law enforcement agencies might report to Berla if they encounter problems with the software. R. 108, 120. He had no knowledge about Berla's code or the debugging process and testified that he does not "know it deeply. That's...for the engineers

¹ For a discussion on hardware and software write-blockers, and their respective advantages and disadvantages, see Christopher S. Meffert, et al., *Deleting Collected Digital Evidence by Exploiting a Widely Adopted Hardware Write Blocker*, 18 DIGITAL INVESTIGATION 87, 88 (2016), <https://doi.org/10.1016/j.diin.2016.04.004> (last accessed Dec. 1, 2025).

and people that design these systems to know.” R. 115-16. In response to examination by the trial court, he also testified that he did not know the error rate of the software. R. 124, ll. 10-13.

The trial court ruled that the evidence was admissible. R. 157. In support of its ruling, the trial court stated:

[W]e have expert testimony with regard to that, and I think that the *Daubert* standards would, indeed, apply. I think things have come out on the record that are relevant that this technology is used—according to the testimony, and it has been unrefuted—it is used worldwide. They also say that it’s used in law enforcement throughout the nation.² As far as the reliability of it, the information that comes out with regard to the data is corroborated by independent evidence...that has already been in the record about the trouble being in Dillion. He was up in Pennsylvania and/or Indiana, and he’s coming down this way, and the truck is there, which would verify that the data that is on this infotainment system is, indeed, accurate.

I do find that, in many respects, it is more reliable than the satellite location, because they at least use three different satellites. And I find it is more accurate than the cell phone locations. Also, the information with regard to the use of the phone that’s going through this system, that also corroborates the fact that the information is correct, that the truck is coming from Pennsylvania and/or Indiana down this way.

This is a little bit different in that, you know, when you talk about peer review and can these results be duplicated, I think a good example of that would be if you had a control test that, say, for instance, in a products liability case where they are saying that radar can adversely affect the cruise control in some way. Maybe there is some test to verify that. I think that would be something that needed to be tested, and could it be repeated, and if it could or could not would hinge on whether it is admissible. But this is a direct download of data. We’ve heard testimony that the only way to get the data out of there is by that chip that they put in there. And I’m not very technological savvy, but they have to put it in there. He also testified that he, nor anyone else, could put data into the system or take it out. So I think—or can be added to or deleted.

² Defense counsel asked Restori why the Marion County Sheriff’s Office needed to transport Appellant’s vehicle’s IVI system four states away to Pennsylvania if the technology was, in fact, widely accepted; Restori did not have an answer. R. 266-67.

R. 157, l. 12 – 159, l. 6. Immediately after the trial court’s ruling, defense counsel asked the trial court to declare Appellant indigent and provide him with an order for funds to hire an expert to counter the state’s. R. 159, ll. 12-16.³ Defense counsel asserted the trial court allowing the evidence in while not providing him with a counter expert would violate his rights to due process and confrontation. R. 159-62. The trial court stated that Appellant was “protected on the record” but would not make such an order. R. 162, ll. 13-22.

At trial, Restori was qualified as an expert witness, and the IVI data was permitted into evidence over Appellant’s objection. R. 249, 256. Morgan testified that Appellant’s vehicle left Lancaster, Pennsylvania at 1:17 a.m. and was tracked down Interstate 95 until it reached the decedent’s home at 9:18 a.m. on the day of the murder. R. 290-95. At 9:22 a.m., Appellant’s vehicle started again and left the decedent’s home. R. 297, l. 13. At this time, a cellphone named “Terry’s iPhone” connected to the vehicle. R. 297, ll. 16-18.

After beginning deliberations, the jury requested a printout of all infotainment data logs that were produced at trial. R. 349, ll. 2-4. Defense counsel and the state agreed that these were not in evidence, and the jury was given the PowerPoint presentation used by Morgan during his testimony. R. 351, ll. 10-13. The jury convicted Appellant on all counts. R. 353-54.

Discussion

The state did not establish that the vehicle infotainment system produced sufficiently reliable data or that its witnesses were qualified to testify about it. The evidence should have been excluded under Rule 702, SCRE.

³ This was a continuation of a request that Appellant had made of the court at any earlier time, though not on the record. *See* R. 161, ll. 17-20 (the court addresses prior *ex parte* communications with defense counsel).

“If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise.” Rule 702, SCRE. The proponent of scientific evidence must establish three elements before that evidence is admitted: (1) it will assist the trier of fact; (2) the expert witness is qualified; and (3) the underlying science is reliable. *State v. Phillips*, 430 S.C. 319, 325, 844 S.E.2d 651, 654 (2020); *accord*, *State v. Council*, 335 S.C. 1, 20, 515 S.E.2d 508, 518 (1999) (both *citing* Rule 702, SCRE). When scientific evidence is sought to be presented, the trial court must make a “preliminary assessment of whether the reasoning or methodology underlying the testimony is scientifically valid and of whether that reasoning or methodology properly can be applied to the facts in issue.” *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 592-93 (1993). The trial court should employ four key factors of analysis: “(1) the publications and peer review of the technique; (2) prior application of the method to the type of evidence involved in the case; (3) the quality control procedures used to ensure reliability; and (4) the consistency of the method with recognized scientific laws and procedures.” *Council*, 335 S.C. at 20, 515 S.E.2d at 517. Further, in the case of scientific techniques, “the court ordinarily should consider the known or potential rate of error.” *Daubert*, 509 U.S. at 594.

Further, “the reliability of a witness’s testimony is not a prerequisite to determining whether or not the witness is an expert.” *State v. Tapp*, 398 S.C. 376, 388, 728 S.E.2d 468, 474 (2012). Rather, the witness’s expertise, the reliability of their process, and their ability to assist the jury are all separate threshold determinations which must be made prior to the admission of evidence. *State v. Meador*, 425 S.C. 625, 646, 825 S.E.2d 53, 65 (Ct. App. 2019).

At the outset, it is important to note the differences between Berla's software and other types of software that have been found reliable by this state's courts. At first glance, data gathered from a vehicle's IVI may appear near identical to cell site location information (CLSI). CLSI location data has been deemed reliable in South Carolina. *State v. Franks*, 432 S.C. 58, 77, 849 S.E.2d 580, 590-91 (Ct. App. 2020). But CLSI data is different from Berla's software, and in any event, the process employed by the state in *Franks* to enter the CLSI data into evidence is in stark contrast to the state's showing in this case.

In *Franks*, the state offered a Greenville County Sheriff's Office sergeant to introduce location data that he had gathered. *Id.* at 69, 849 S.E.2d at 586. The sergeant testified that he was given cell phone records in an Excel spreadsheet and then used a software called GeoTime to sort the data making it easier to read. *Id.* He also independently verified the results given to him by that software. *Id.* The *Franks* evidence was gathered by receiving records of phone calls. *Id.* When phone calls are made, they connect to the nearest cell tower, which is located at a fixed, known location. *Id.*; Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where are We*, 29 HASTINGS COMM. & ENT. L. J. 421, 426 (2007) (explaining how cellular "triangulation" works). By contrast, IVI data uses satellites—which are not at fixed locations—to determine the location of a moving vehicle. R. 158. This is entirely different, because cell phone tower location is "uninterrupted." McLaughlin, *supra* at 426. As long as a person is speaking on the phone, that phone is connected to a cell tower. *Id.* IVI data, on the other hand, is not uninterrupted and can be affected by satellites being out of position or even driving in large cities with several tall buildings. Further, the CLSI data in *Franks* was further put through another program, "Esri," which was created by the wireless provider itself for the purpose of mapping coordinates. 432 S.C. at 70, 849 S.E.2d at 586. The employ of software

created by the same company that stores the CLSI to map the CLSI is an entirely different question than the use of outside, proprietary data to pull information off of a vehicle's IVI system.

The Berla software data utilized in this case was not established to be reliable, and the trial court abused its discretion in failing to exclude it for two reasons. First, the trial court was not presented with any evidence by which it could have made a proper reliability determination under the four-factor *Council* test. Second, software using proprietary source code, when entered through expert witnesses who have never seen that source code, much less understand it, should be considered inherently unreliable.

A. The trial court was not presented with evidence sufficient to find the evidence reliable under *Council*.

Council requires that the trial court should typically employ four key factors of analysis: “(1) the publications and peer review of the technique; (2) prior application of the method to the type of evidence involved in the case; (3) the quality control procedures used to ensure reliability; and (4) the consistency of the method with recognized scientific laws and procedures.” *Council*, 335 S.C. at 20, 515 S.E.2d at 517. Further, to the extent that the Supreme Court has partially adopted *Daubert*, the trial court should also have been apprised of “the known or potential rate of error.” *Daubert*, 509 U.S. at 594.⁴ The state's witnesses established zero of these elements.

⁴ In *State v. Phillips*, our Supreme Court made numerous references to a “*Daubert/Council* hearing.” See 430 S.C. at 341, 343, 844 S.E.2d at 662-63. Appellant submits this means one of two things. First, it could mean that the Supreme Court recognized that the *Daubert* and *Council* standards were so similar to each other as to obviate the need to distinguish between them. Second, it could mean, as two of the justices believed, that the Supreme Court was implicitly adopting *Daubert*. *Phillips*, 430 S.C. at 344, 844 S.E.2d at 664 (Beatty, C.J., concurring in the judgment, joined by Hearn, J. (“the majority’s instruction regarding a ‘*Daubert/Council*’ hearing is confusing and constitutes an implicit adoption of *Daubert*”). This question need not be

Peer review and publications of the technique. Neither Morgan nor Restori was familiar with any attempt to peer review Berla's software. In fact, Restori suggested that the "peer review" process was law enforcement agencies notifying Berla when they encountered a problem. This is not peer review. Peer review requires review by *peers*—other *experts* in the same field. *See, e.g., Peer Review, MERRIAM-WEBSTER COLLEGIATE DICTIONARY* (11th ed. 2003). Neither witness could identify any peer review study that had ever been conducted on Berla's software, and when confronted by defense counsel with—purported—peer reviews of the Berla software, neither had ever heard of them.

Prior application of the method to the type of evidence in the case. Restori testified that he had performed "hundreds" of prior data extractions using the Berla software. However, this testimony is insufficient to establish that he has previously applied the specific method in this case to the specific evidence in this case a significant number of times. The testimony was that every single car manufacturer creates their IVI systems differently, meaning that Berla must create different software for every individual make and model of vehicle. R. 106. It is not clear what the differences between the different software are, because neither of the state's purported experts testified to that effect.

Further, the fact that the software has been used several times before does not, on its own, grant the software reliability. Several other types of scientific methods are frequently used in a variety of contexts yet are still deemed unreliable under Rule 702. *See, e.g., Matter of the Care and Treatment of Bilton*, 432 S.C. 157, 851 S.E.2d 442 (Ct. App. 2020) (penile plethysmograph

addressed in this case. The only portion of the *Daubert* standard that truly diverges from the *Council* standard is the rule that the trial court should generally consider the error rate of any potential scientific procedures. The trial court understood this to be the law of South Carolina, as it both inquired about the error rate and stated explicitly that it was ruling under *Daubert*. R. 157 ("I think that the *Daubert* standards would, indeed, apply").

evidence unreliable despite frequent use as treatment tool); *United States v. Scheffer*, 523 U.S. 303 (1998) (polygraph unreliable despite frequent use by government as national security tool).

Quality control procedures used to ensure reliability. Neither of the state's witnesses who testified about the Berla software provided any testimony that could have shown the trial court that Berla is subjected to reliable quality control procedures. As already mentioned, neither witness could testify about whether Berla used write-blockers in its software. Write-blockers are enormously important to any computer programming, because they protect the integrity of the data thereon. Meffert, et al., *supra*, 18 DIGITAL INVESTIGATION at 88. Due to their importance, write-blockers are frequently deployed by experts in digital forensics around the nation. *See, e.g., Solon v. United States*, Case No. 2:11-cv-303-CAB, 2013 WL 12321956 at *33 (D. Wyo. May 24, 2013) (federal agent's testimony regarding using write-blockers in CSAM detecting software as a matter of course). And even when write-blockers are used, if programmers are not careful, malicious actors can wreak havoc on stored data by tricks so simple as sending the law enforcement agencies that use Berla an email with a malicious link. Meffert, et al., *supra*, 18 DIGITAL INVESTIGATION at 93. Data could be "easily" modified by a malicious actor, and "it will be difficult for the devices to detect the modification." Yeonghun Shin, et al., *Digital Forensics Case Studies for In-Vehicle Infotainment Systems Using Android Auto and Apple CarPlay*, 22 SENSORS 7196, 7197 (2022), <https://doi.org/10.3390/s22197196> (last accessed Dec. 1, 2025). Since, like the state's witnesses here, "many law enforcement agency practitioners have only received training for using digital forensic tools and many do not possess a background in cyber security and/or computing," the potential for these threats compromising evidentiary data while

going entirely unnoticed is far too high to consider such evidence “reliable.” Meffert, et al., *supra*, 18 DIGITAL INVESTIGATION at 93.⁵

Further, the use of this type of complex computer software, when introduced by witnesses that have no knowledge of its underlying components, presents numerous issues. Neither of the state’s witnesses were computer scientists, nor did they demonstrate even rudimentary knowledge of how the Berla software worked. When asked about it, Restori simply responded that the innerworkings of the system was “for the engineers and people that design these systems to know.” R. 115-16. Without any knowledge of the program and how it works, the state’s witnesses could not inform the trial court, for example, whether “the sources of the input data are accurate,” whether “no relevant data has been overlooked,” or whether “the assumptions used to quantify non-measured items are reasonable.” Edward Hannan, *Computer-Generated Evidence: Testing the Envelope*, 63 DEF. COUNS. J. 353, 358 (1996).

The sheer complexity of modern computer programs demonstrates the need for state’s witnesses to have some base-line knowledge of the programs that provide the evidence they are testifying to. Berla, like every other computer program, is, at its core, made up of source code. Hundreds of thousands of lines of source code which does not resemble readable English and is incomprehensible to anyone besides experienced computer programmers. One single typo, such as a misplaced parenthesis, can have a material and “prejudicial” impact on the way the software as a whole works. Christian Chessman, *A “Source” of Error: Computer Code, Criminal*

⁵ The trial court held that “this is a direct download of data,” and “the only way to get the data out of there is by that chip that they put in there.” R. 158-59. While technically accurate, this misses the point. The data can be altered from outside of the computer. The Pennsylvania State Police could have been the victim of the sort of malicious cyber-attack that computer science experts warn is a very real, very present possibility. Meffert, et al., *supra*; Shin, et al., *supra*. Or they might not have been the victim of such an attack. The point is that the trial court, based on the evidence presented to it, could not possibly have known.

Defendants, and the Constitution, 105 CAL. L. REV. 179, 186-87 (2019). No amount of caution by even the most experienced programmers can avoid these “miscodes,” they are “inevitable; bugs and misconfigurations are inherent in software.” Andrea Roth, *Machine Testimony*, 126 YALE L. J. 1972, 1994 (2017). Without any knowledge of the “debugging” process, it is not possible for the state’s witnesses to have provided the trial court with a sufficient baseline of Berla’s quality control procedures. *Cf.*, Chessman, *supra*, 105 CAL. L. REV. at 184 (the “general public perception” is “that computers automatically enhance the accuracy of evidence,” but “computer scientists *flatly reject that notion*” (emphasis added)). The proper witnesses would have been “the engineers and people that design these systems” that Restori testified were responsible for ensuring the system used to convict Appellant was reliable. *See id.* at 188 (computer programs which combine several areas of complex expertise suggest that some witnesses will be experts in some areas but make errors in others, due to an incomplete grasp of the other expertise).

The consistency of the method with recognized scientific laws and procedures. Neither of the state’s witnesses were scientists. And neither of the state’s witnesses had any knowledge or training in digital forensics, computer science, cyber-security, or some related field. Apart from a week-long training created by Berla itself, they possessed no qualifications to even use Berla’s devices. Neither witness was qualified to opine as to the consistency of Berla’s software with recognized scientific laws and procedures, and neither attempted to.

Error rate. Finally, neither witness knew of the error rate of Berla’s software. This means that the trial court was not apprised of any known or potential rate of error for Berla’s software. It was not possible, therefore, for the trial court to rule in compliance with *Daubert*, despite its statements on the record that it was. *See Daubert*, 509 U.S. at 594 (trial court should consider

error rate). Restori and Morgan's ignorance of the error rate further permitted them to suggest to the jury that the Berla software was infallible. R. 282 ("you can download these...a thousand times over by a thousand different people, and it gives you the same results"). This permitted the state to "overstate the probative value of their evidence, going far beyond what the relevant science can justify."⁶ Put succinctly by a federal circuit judge, the state's failure to present this evidence through witnesses with actual, relevant expertise essentially "accept[ed] the product of a computer as the equivalent of Holy Writ," which would come as a great surprise to "one of the many who have received computerized bills and dunning letters for accounts long since paid." *Perma Research & Development v. Singer Co.*, 542 F.2d 111, 121 (2d Cir. 1976) (Van Graafeiland, J., dissenting); *cf. also, United States v. Washington*, 498 F.3d 225, 230 (4th Cir. 2007) (acknowledging that technicians using a gas chromatograph machine could not independently verify the results because they only relied on the analysis performed by the machine); *Melendez-Diaz*, 557 U.S. at 318 ("Forensic evidence is not uniquely immune from the risk of manipulation").

For these reasons, the trial court was not presented with evidence sufficient to find the IVI evidence reliable. Without this evidentiary basis, it was error to refuse to exclude the evidence. Appellant is entitled to a new trial.

⁶ President's Council of Advisors on Science and Technology ("PCAST"), *Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature Comparison Methods* (Sep. 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf (last accessed Dec. 1, 2025).

B. Software that makes use of secret, proprietary source code, when entered through expert witnesses who have never seen that source code, much less understand it, should be considered inherently unreliable.

Berla's software is a closely-guarded trade secret. This means it is not shared with the law enforcement agencies that employ it. Even if the officers who used Berla did understand computer science, this expertise would not help them because only Berla truly knows how its code works. This is inherently unreliable and should not be allowed as evidence in this state's courts, unless a strong showing of reliability is made. That showing was not made here.

Berla is a private corporation. R. 117. Their biggest—and likely only—customers are law enforcement entities. This presents a risk that the Supreme Court of the United States recognized: “A forensic analyst responding to a request from a law enforcement official may feel pressure—or have an incentive—to alter the evidence in a manner favorable to the prosecution.” *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 318 (2009). These same market forces incentivize private companies like Berla to keep the source code behind their software a closely held secret, lest other companies become competitors.

The main problem with the use of proprietary technology as evidence against a criminal defendant is that most times that sort of trade secret evidence cannot be subjected to cross-examination by the defense—the last safeguard of reliability. *See, e.g., State v. Schwartz*, 447 N.W.2d 422, 428 (Minn. 1989) (holding that laboratory information, while possessing general scientific acceptance, is not admissible unless the laboratory complies with certain guidelines, including the “availability of their testing data and results”); *cf. also, K.W. v. Armstrong*, 180 F.Supp.3d 703, 718 (D. Idaho 2016) (finding that government reliance on secret, proprietary algorithm violates due process).

An adverse party's ability to confront evidence goes hand-in-hand with its reliability. *Cf.*, *Crawford v. Washington*, 541 U.S. 36, 62-68 (2004) (*overruling Ohio v. Roberts*, 448 U.S. 56 (1980) which had carved out a Confrontation Clause exception for out of court evidence that was judicially determined to possess indicia of reliability); *cf., also, Maryland v. Craig*, 497 U.S. 836, 845 (1990) (Confrontation Clause's chief concern is "to ensure the *reliability* of the evidence...by subjecting it to rigorous testing" (emphasis added)); *and cf., Holmes v. South Carolina*, 547 S.C. 319, 331 (2006) ("by evaluating the strength of only one party's evidence, no logical conclusion can be reached regarding the strength of contrary evidence offered by the other side to rebut or cast doubt"). Rather than the secret computer algorithms deployed to great effect by the state in this case, "open examination of witnesses...is much more conducive to the clearing up of truth." 3 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 373 (1768).

To be clear, this case is not about the Confrontation Clause. But analysis of the same provides a clue into why this sort of secret evidence is inherently unreliable. If this sort of evidence falls short of what the Confrontation Clause would require of *any* witness in a criminal case, how could it meet the *heightened* requirement for scientific or expert testimony under Rule 702?

Typically, the best test of reliability is cross-examination in open court.⁷ Delineated above, there are several potential issues with the accuracy and reliability of computer-generated evidence. Computer programs, at the end of the day, are tools. Chessman, *supra*, 105 CAL. L. REV. at 184. "Perhaps exceptionally fast, sophisticated, and useful tools, but tools nonetheless." *Id.* And just as the Rules of Evidence would not permit a hammer or a speedometer to assume

⁷ To quote former Chief Justice Louis Brandeis, "sunlight is the best disinfectant." Louis Brandeis, *What Publicity Can Do*, HARPER'S WEEKLY, Dec. 20, 1913, at 10.

the witness stand, they likewise require competent human testimony to explain how those tools were used.

Because of the lack of ability for the defense to truly test the reliability of such computer evidence through cross-examination, evidence produced by computers “merits *additional* scrutiny rather than relaxed scrutiny.” *Id.* Complex computer programs are beyond the understanding of lay jurors and even judges, making the detection of errors enormously difficult if not impossible. *Id.* “The prejudice flowing from the higher risk of uncaught error is compounded by the additional credibility that juries afford to computer-produced evidence based on erroneous assumptions of precision and impartiality.” *Id.* Erroneous assumptions that, again, cannot be effectively challenged, because the source code behind the programs that produce this evidence is a closely guarded secret. *See* Andrea Roth, *Trial by Machine*, 104 GEO. L. J. 1245, 1301 (2016) (without open-source codes, there is not even a “minimum level of accessibility and scrutiny” (*citing* Darrel Ince, et al., *The Case for Open Computer Programs*, 482 NATURE 485, 485 (2012))).

Defense counsel was able to cross-examine the state’s witnesses, but this is not nearly enough. With such complexity involved in the creation of this computer evidence, the traditional safeguards—like confrontation—are insufficient to fully explain to lay jurors the potential issues behind the curtain. *See id.* at 1270, 1300 (explaining that traditional “courtroom safeguards also seem an awkward fit” for scrutinizing “hidden subjectivities and errors that often go unrecognized and unchecked”). In this case, the two Pennsylvania police officers that the state presented as experts were woefully uninformed about the underlying science behind the technology that they propped up as infallible. Therefore, it was not possible for Appellant to meaningfully challenge this evidence—nor could it be in any case; cross-examining a machine is

science fiction. *See id.* at 1301. Simply, “a pixel cannot speak, and an algorithm cannot be cross-examined.” *State v. Melsky*, 2013 WL 1776037 at *4 (N.J. Sup. Ct. App. Div. Apr. 26, 2013) (unpublished). Had the state called experts who *were* informed about the inner workings of the software, they very likely would not have testified to the infallibility of Berla’s software; after all, the idea that software could ever be infallible is a position “flatly reject[ed]” by computer scientists. Chessman, *supra*, 105 CAL. L. REV. at 184. Appellant was not given the opportunity to even attempt to explain to the jury some of the myriad potential problems with software-generated evidence. In the absence of such scrutiny, such complex scientific evidence can never be “reliable.”

For these reasons, the state did not establish reliability before the trial court. Further, computer programs that rely on secret source codes to create evidence that cannot be meaningfully scrutinized by traditional courtroom protections are inherently unreliable. The trial court therefore abused its discretion in failing to exclude the Berla software evidence. *See* Rule 702, SCRE; *Council*, 335 S.C. at 20, 515 S.E.2d at 518. Appellant is entitled to a new trial.

II.

The trial court erred in imposing a five-year sentence for possession of a weapon during the commission of a violent crime when it had already imposed a life sentence.

Relevant Facts

During sentencing, the trial court sentenced Appellant to life imprisonment for murder, fifteen years' imprisonment for burglary first degree, and five years' imprisonment for possession of a weapon during the commission of a violent crime. R. 355. Appellant did not object to the sentence. R. 355.

Discussion

The five-year sentence required by S.C. Code Ann. § 16-23-490(A) expressly does not apply when the person sentenced is also sentenced to life imprisonment. The trial court's sentence to that effect should be vacated.

A person convicted of possession of a weapon during the commission of a violent crime faces a mandatory five-year sentence “in addition to the punishment provided for the principal crime.” S.C. Code Ann. § 16-23-490(A). The “five-year sentence does *not* apply,” however, “where...a life sentence without parole is imposed for the violent crime.” *Id.* (emphasis added). It is well settled that the sentence imposed by the trial court is an unlawful sentence. *State v. Plumer*, 439 S.C. 346, 350, 887 S.E.2d 134, 137 (2023). Further, although the sentence was not objected to, this Court is empowered to correct the sentence anyway. *Id.* (“it is inefficient and a waste of judicial resources to delay the inevitable by requiring the appellant to file a post-conviction relief action or petition for a writ of habeas corpus”); *State v. Sledge*, 428 S.C. 40, 59-60, 832 S.E.2d 633, 644 (Ct. App. 2019) (vacating five-year sentence for possession of a weapon during a violent crime despite no objection from trial defense attorney).

For these reasons, this Court should vacate the five-year sentence imposed for possession of a weapon during the commission of a violent crime.

CONCLUSION

For the foregoing reasons, as to Issue I, Appellant's convictions and sentences should be reversed, and this case should be remanded for a new trial. As to Issue II, Appellant's sentence for possession of a firearm during the commission of a violent crime should be vacated.



W. Chandler Norville
Appellate Defender

ATTORNEY FOR APPELLANT

This 9th day of June, 2026.

RECEIVED

Jun 09 2026

CERTIFICATE OF COUNSEL FOR APPELLANT

SC Court of Appeals

Counsel for appellant certifies that this Final Brief of Appellant contains all material proposed to be included by any of the parties and not any other material and that this Final Brief of Appellant complies to the best of my ability with the April 15, 2014 order from the South Carolina Supreme Court entitled "Revised Order Concerning Personal Identifying Information and Other Sensitive Information in Appellate Court Filings."

Respectfully Submitted,



W. Chandler Norville
Appellate Defender

South Carolina Commission on Indigent Defense
Division of Appellate Defense
PO Box 11589
Columbia, SC 29211-1589

ATTORNEY FOR APPELLANT

This 9th day of June, 2026.