COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

No. SJC-13499

COMMONWEALTH,

Appellant,

v.

VICTOR ARRINGTON,

Appellee.

On Appeal from an Order of the Suffolk County Superior Court

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS, INC., THE ELECTRONIC FRONTIER FOUNDATION, THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AND THE MASSACHUSETTS ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF APPELLEE AND AFFIRMANCE

Jessica J. Lewis (BBO #704229)
Jessie J. Rossman (BBO #670685)
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
MASSACHUSETTS, INC.
One Center Plaza, Suite 850
Boston, MA 02108
(617) 482-3170
jlewis@aclum.org
jrossman@aclum.org

Counsel continued on next page

Daniel K. Gelb (BBO #659703)
VICE CHAIR, FIRST CIRCUIT
NATIONAL ASSOCIATION
OF CRIMINAL DEFENSE
LAWYERS AMICUS COMMITTEE
GELB & GELB LLP
900 Cummings Ctr., Suite 207-V
Beverly, MA 01915
dgelb@gelbgelb.com

Nicola Morrow* (on the brief)
Michael J. Price (on the brief)
NATIONAL ASSOCIATION
OF CRIMINAL DEFENSE
LAWYERS
1660 L St. NW, 12th Floor
Washington, DC 20036
(202) 872-8600
nmorrow@nacdl.org

Nathan Freed Wessler (BBO #680281)
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad St. 18th Fl.
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Jennier Stisa Granick (on the brief)
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm St.
San Francisco, CA 94111
(415) 343-0758
jgranick@aclu.org

Hannah Zhao (on the brief)
Andrew Crocker (on the brief)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St.
San Francisco, CA 94109
(415) 436-9333
zhao@eff.org

Chauncey B. Wood (BBO #600354)
MASSACHUSETTS ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS
55 Union St., 4th Floor
Boston, MA 02108
(617) 248-1806
cwood@woodnathanson.com

* New York bar admission pending

Counsel for Amici Curiae

November 28, 2023

CORPORATE DISCLOSURE STATEMENT

Pursuant to Supreme Judicial Court Rule 1:21, the American Civil Liberties Union of Massachusetts, Inc. (ACLUM) represents that it is a nonprofit corporation incorporated under the laws of the Commonwealth of Massachusetts; the American Civil Liberties Union (ACLU) represents that it is a District of Columbia non-profit membership organization and 501(c)(4) organization; the Massachusetts Association of Criminal Defense Lawyers (MACDL) represents that it is a 501(c)(6) organization under the laws of the Commonwealth of Massachusetts; the National Association of Criminal Defense Lawyers, Inc. (NACDL) represents that it is a 501(c)(6) organization under the laws of the District of Columbia; and the Electronic Frontier Foundation (EFF) represents that it is a 501(c)(3) organization under the laws of the Commonwealth of Massachusetts. ACLUM, ACLU, MACDL, NACDL, and EFF do not issue any stock and none of the organizations has a parent corporation.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST

The American Civil Liberties Union (ACLU) and the American Civil Liberties Union of Massachusetts (ACLUM) are membership organizations dedicated to the principles of liberty and equality embodied in the constitutions and laws of the Commonwealth and the United States. The rights they defend through direct representation and amicus briefs include the right to be free from unreasonable searches and seizures and to ensure the reliability of government evidence. *See, e.g.*, *Commonwealth v. Mora*, 485 Mass. 360 (2020) (amicus); *Commonwealth v. Almonor*, 482 Mass. 35 (2019) (amicus); *Commonwealth v. Augustine*, 467 Mass. 230 (2014) (direct representation); *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (direct representation); *Bridgeman v. Dist. Att'y for the Suffolk Dist.*, 476 Mass. 298 (2017) (direct representation); *United States v. Jones*, 565 U.S. 400 (2012) (amicus).

The Electronic Frontier Foundation ("EFF") is a member-supported non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for thirty years. With over 38,000 active donors, EFF represents the interests of people impacted by new technologies in court cases and

broader policy debates surrounding the application of law in the digital age. EFF has special familiarity with and interest in constitutional issues that arise with new forensic technologies and has served as amicus in cases regarding a criminal defendant's right to confront forensic software and black-box technology. *E.g.*, *State v. Arteaga*, 476 N.J. Super. 36 (App. Div. 2023); *People v. Easley*, 38 N.Y.3d 1010 (2022); *United States v. Ellis*, No. 19-369, 2021 WL 1600711 (W.D. Pa. Apr. 23, 2021); *State v. Pickett*, 466 N.J. Super. 270 (App. Div. 2021); *People v. Johnson*, No. F071640, 2019 WL 3025299 (Cal. Ct. App. July 11, 2019) (unpublished). EFF has also participated in the Government Accountability Office's inquiry regarding forensic technology, which was prompted by concerns from elected federal officials about the use of these technologies in criminal proceedings. *See* U.S. Gov't Accountability Office, *Forensic Technology: Algorithms Used in Federal Law Enforcement* (May 12, 2020).

The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL is the only nationwide professional bar association for public defenders and

private criminal defense lawyers, with tens of thousands of members and affiliates throughout the country. NACDL is particularly interested in cases arising from surveillance technologies and programs that pose new challenges to personal privacy. It operates a dedicated initiative that trains and directly assists defense lawyers handling such cases to help safeguard privacy rights in the digital age. NACDL has also filed numerous amicus briefs in this Court and the Supreme Court on issues involving digital privacy rights, including in *Carpenter*, 138 S. Ct. 2206; *Riley v. California*, 573 U.S. 373 (2014); and *Jones*, 565 U.S. 400.

The Massachusetts Association of Criminal Defense Lawyers (MACDL) is an incorporated association representing more than 1,000 experienced trial and appellate lawyers who are members of the Massachusetts Bar and who devote a substantial part of their practices to criminal defense. MACDL devotes much of its energy to identifying, and attempting to avoid or correct, problems in the criminal justice system. It files amicus curiae briefs in cases raising questions of importance to the administration of justice.

RULE 17(C)(5) DECLARATION

Amici declare that (a) no party or party's counsel authored the brief in whole or in part; (b) no party or a party's counsel contributed money that was intended to fund preparing or submitting the brief; (c) no person or entity—other than the amici curiae, their members, or their counsel—contributed money that was intended to fund preparing or submitting the brief; and (d) neither amici curiae nor their counsel represents or has represented any of the parties to the present appeal in another proceeding involving similar issues, nor were amici a party or represented a party in a proceeding or legal transaction that is at issue in the present appeal.

INTRODUCTION

Both this Court and the United States Supreme Court have made clear that courts must perform a crucial "gatekeeper" role regarding the admission of expert scientific and technical testimony. *Commonwealth v. Lanigan*, 419 Mass. 15, 26 (1994); *see also Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 148–50 (1999). A robust application of the relevant standards is especially essential where, as here, proprietary algorithms are involved, to avoid violations of defendants' constitutional rights and wrongful convictions predicated on unreliable

evidence. As the superior court properly concluded, that standard was not met in this case. To protect the fair administration of justice in an era of rapidly developing new technologies that rely on opaque or proprietary algorithms, amici urge this Court to affirm the superior court's decision not to admit the "frequent location history" (FLH) in this case on the testimony of Mr. Christopher Kindig. Doing so will confirm that information generated by new proprietary or black-box technologies cannot be admitted until and unless the government can produce an expert who has sufficient access to and knowledge about the technology's algorithm and can provide testimony that will satisfy the *Daubert-Lanigan* standard for reliability.

ARGUMENT

I. The Commonwealth did not satisfy the *Daubert-Lanigan* standard to admit expert testimony on frequent location history in this case.

A. Expert testimony can only be admitted where the court has enough information to determine that the witness is qualified and the evidence is sufficiently reliable.

"For expert testimony to be admissible," the judge must determine that the proposed witness is "qualified as an expert to testify to a specific subject matter," and "that the expert testimony is

sufficiently reliable to reach the jury." *Commonwealth v. Rintala*, 488 Mass. 421, 426 (2021); *see also* Mass. G. Evid. § 702 (2023).

As to the former, the "crucial issue" is "whether the witness has sufficient 'education, training, experience and familiarity' with the subject matter of the testimony." *Rintala*, 488 Mass. at 426 (quoting *Commonwealth v. Frangipane*, 433 Mass. 527, 533 (2001)). An expert witness must have sufficient access to, and knowledge of, the evidence he or she is meant to explain. "[A] judge's discretion can be abused when an expert witness is permitted to testify to matters beyond an area of expertise or competence." *Id.* at 426 (quoting *Frangipane*, 433 Mass. at 533).

As to the latter, the proponent must "demonstrate the reliability or validity of the underlying scientific theory or process." *Lanigan*, 419 Mass. at 26. "Simply stated, if the process or theory underlying an expert's opinion lacks reliability, that opinion should not reach the trier of fact." *Rintala*, 488 Mass. at 427 (cleaned up). Although "in most cases general acceptance will be the significant and often only issue," to establish reliability, this Court has adopted in part the *Daubert* test to provide alternate means to demonstrate reliability for a new theory or process whose "novelty prevents it from having attained general

acceptance in the relevant scientific community." *Canavan's Case*, 432 Mass. 304, 310 (2000) (cleaned up); *see also Lanigan*, 419 Mass. at 25–26; *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993). Specifically, *Lanigan* set forth five nonexclusive *Daubert-Lanigan* factors to help judges assess the reliability of proposed scientific and technical evidence:

> whether the scientific theory or process (1) has been generally accepted in the relevant scientific community; (2) has been, or can be, subjected to testing; (3) has been subjected to peer review and publication; (4) has an unacceptably high known or potential rate of error; and (5) is governed by recognized standards.

Commonwealth v. Powell, 450 Mass. 229, 238 (2007).[1]

These factors are designed to protect parties from seemingly compelling, but unreliable or opaque scientific evidence. Strict adherence to this standard is important, as demonstrated by the litigation regarding breath alcohol tests. Massachusetts General Laws chapter 90, section 24(1)(e) provides that "evidence of the percentage, by weight, of alcohol in the defendant's blood . . . as indicated by a chemical test or analysis of his breath, shall be admissible" in Operating

[1] The *Daubert-Lanigan* factors apply not only to "scientific evidence," but also more broadly to "technical[] and other specialized knowledge." *Commonwealth v. Davis*, 487 Mass. 448, 453 (2021) (citing *Commonwealth v. Pytou Heang*, 458 Mass. 827, 844 (2011)).

Under the Influence prosecutions. Nevertheless, in 2015 this Court held that a defendant was still entitled to *Daubert-Lanigan* hearings to assess the reliability of new breathalyzer technology before it could be admitted as evidence against him. *See Commonwealth v. Camblin*, 471 Mass. 639, 648 (2015). In so doing, the Court emphasized its "important gatekeeper role" in deciding reliability. *Id.* at 648.[2]

B. The *Daubert-Lanigan* standard has not been met in this case.

Amici agree with the superior court's findings and the Appellee's arguments that the *Daubert-Lanigan* standard has not been met here, and briefly emphasize two points.

First, under the *Daubert-Lanigan* standard, the government's offered expert witness in this case, Mr. Kindig, was not qualified to

[2] In later litigation regarding the reliability of another iteration of breathalyzer technology that additionally revealed the Office of Alcohol Testing's (OAT) withholding of evidence, this Court ultimately concluded that the "extensive nature of OAT's misconduct," coupled with defendants' inability "to receive a fair *Daubert-Lanigan* hearing," for this new technology "resulted in the violation of the right to due process for approximately 27,000 defendants." *Commonwealth v. Hallinan*, 491 Mass. 730, 731 (2023). While *Hallinan* addressed the aftermath of years of untested evidence, its holding underscores the import of ensuring that new technology may only be introduced on the testimony of an expert with sufficient access to and information about the processes undergirding the specific model or device at issue.

testify about FLH evidence. Of the 200 investigations he has worked on, only twenty-three involved "analyzing mobile devices." TRI/9–10. Mr. Kindig's testimony does not reveal whether any of those cases involved FLH evidence. More importantly, Mr. Kindig lacks access to the proprietary technology he was called to explain. Indeed, Mr. Kindig himself testified that he does not understand how the algorithm works and stated his belief that "only Apple engineers would [k]now that, it's proprietary." Arrington Br. 38 n.7.

Additional testimony from Mr. Kindig further illustrates the problem:

> Q: Okay. So, again, there's a beginning point and an end point and a secret middle part; right?
> A: Correct.
> Q: Okay. And that's, I take it proprietary and closely guarded by Apple?
> A: That would be my understanding, yes.
> Q: Okay. So, we know that we've got this data over here and then we've got this frequent location here, and how it gets from data to frequent location history, we know it's because of an algorithm, but we don't really know how the algorithm works; right?
> A: That's correct, yes.

TRII/50. As to the "confidence" field generated in one of the reports, Mr. Kindig told the Superior Court, "There hasn't been a significant amount of testing research to determine what that field represents, so I can't confidently tell you what that determination — like what that

determination means as far as Apple is concerned." *Id.* at 58–59. This testimony did not and cannot establish Mr. Kindig's qualifications to testify. Expert testimony is valuable only if it is found to be rooted in knowledge and experience with the subject of the testimony; otherwise, such testimony is not only useless, but has the potential to seriously mislead triers of fact. *See Kumho*, 526 U.S. at 151–53. Indeed, it is crucial that trial judges ensure that expert witnesses are verifiably competent to testify about the evidence in question because juries—and even judges—tend to over-rely on expert witness testimony.[3]

Second, Mr. Kindig designed and conducted his own FLH reliability tests, which were not subject to any of the rigorous standards that typically govern validation studies.[4] These ad hoc tests consisted

---

[3] *See, e.g.*, Jonathan Koehler, N.J. Schweitzer, & Michael Saks, *Science, Technology, or the Expert Witness: What Influences Jurors' Judgments About Forensic Science Testimony?*, 22 Psychol. Pub. Pol'y & L. 401, 411 (2016) (concluding that "[t]he danger in failing to apply *Daubert's* tough reliability test on the front end is that jurors will presume that admitted forensic evidence is accurate evidence, and cross-examination that exposes substantive scientific weaknesses will be ignored"); Demosthenes Lorandos, *Expert Evidence Post*-Daubert*: the Good, the Bad, and the Ugly*, 43 Litig. 18, 23–24 (2017) (explaining that "the obligation of trial judges is to protect the truth-finding process from exposure to unreliable opinion testimony that, coming from an expert, may be accepted for reasons unrelated to the merits").

[4] *See* Jeanna Matthews, Bruce Hedin, & Marc Canellas, *Trustworthy Evidence for Trustworthy Technology: An Overview of Evidence for*

of using what he characterized as a "closely modeled phone and operating system" and going to a handful of different locations "in order to recreate or generate some frequent location data" and then assessing the reliability of that data. TRII/19. To conduct the tests, Mr. Kindig "enabled location services, WiFi and Bluetooth . . . [and] picked a series of locations . . . to test to generate frequent locations." *Id.* at 23. However, the locations visited did not include the crime scene location in this case, *id.* at 25, and no evidence was provided indicating that the same settings (i.e., "location services, WiFi and Bluetooth") that were enabled on the test phone had also been enabled on the evidence phone at the relevant time. Mr. Kindig acknowledged that he conducted his test on a different model iPhone, running a different operating system version, than the phone in evidence. *Id.* at 19, 105–06. He admitted that

---

Assessing the Trustworthiness of Autonomous and Intelligent Systems, L. Comm. of the IEEE Global Initiative and IEEE-USA A.I. Pol'y Comm. (2022); Marc Canellas, *Defending IEEE Software Standards in Federal Criminal Court*, 54 Computer 6 (2021); Letter from IEEE-USA to National Institute of Standards and Technology, Re: RFC Response: Digital Investigative Techniques: A NIST Scientific Foundation Review (NISTIR 8354-DRAFT) (July 11, 2022) (furnishing recommendations for validating digital forensics tools); Letter from IEEE-USA to National Institute of Standards and Technology, Re: RFC Response: NIST Internal Report 8351-DRAFT *DNA Mixture Interpretation: A NIST Scientific Foundation Review* (Nov. 18, 2022) (furnishing recommendations for testing and validating DNA software).

there "could be differences between the algorithms" that generated the FLH data in his test and the FLH data that the government wants to use as evidence in this case. *Id.* at 107–08. Although he asserted that he doesn't "believe [these changes are] anything that's significant," *id,* the "mere assertion that a methodology is reliable" is insufficient to meet the relevant standard. *Canavan's Case*, 432 Mass. at 315 (citing *Kumho,* 526 U.S. at 157). Mr. Kindig's tests are analogous to an attempt at validating a breath alcohol device through testing performed on a different model running a different software version, the conclusions of which this Court would surely reject. *Cf. Hallinan*, 491 Mass. at 737–38.

The *Daubert-Lanigan* standard exists, in large part, to aid the truth-seeking function of judicial proceedings. *See Daubert*, 509 U.S. at 589 ("under [*Daubert*] the trial judge must ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable"). Because the *Daubert-Lanigan* factors are not satisfied here, admitting the FLH evidence in this case would undermine the precepts set out by the doctrine, violate Mr. Arrington's rights, and threaten to erode the standard for the analysis of novel technologies in the future.

II. A strong *Daubert-Lanigan* standard is essential to guard against introduction of unreliable evidence from other proprietary and black-box algorithms.

Strong enforcement of the *Daubert-Lanigan* standard provides a critical bulwark against introduction of unreliable or unsubstantiated evidence that may taint the trial process and lead to wrongful convictions. In resolving this case, the Court should be mindful that FLH is far from the only information generated by proprietary or black-box algorithms that the government uses during the criminal investigative process. Any weakening of the *Daubert-Lanigan* protections would create an intolerable risk that evidence from any such systems—including probabilistic genotyping, facial recognition technology, and gunshot detection systems—could be introduced at trial without a competent and knowledgeable expert adequately establishing their reliability. Amici highlight a few examples of such algorithms here, to highlight the broader stakes of the Court's decision in this case.

A. Probabilistic genotyping

Probabilistic genotyping (PG) software programs purport to be able to do what traditional DNA tests cannot: express the likelihood that an individual's DNA is present in a sample comprised of scraps of

multiple individuals' genetic material.[5] These systems rely on complicated algorithms comprised of many tens of thousands of lines of code, and generate results based on a set of often undisclosed factors and assumptions. The algorithms generate a "likelihood ratio," which is stated as the relative probability that a suspect's DNA is contained in the multi-contributor sample compared to a random person from a particular reference population.[6]

As a federal blue-ribbon panel on forensic science has cautioned, probabilistic genotyping algorithms "require careful scrutiny," not least because "the programs [from different companies] employ different mathematical algorithms and can yield different results for the same mixture profile."[7] Yet the private companies that offer these algorithms to law enforcement regard their technology as proprietary trade secrets and routinely seek to keep their algorithms concealed. Excessive

---

[5] *See* Andrea Roth, *Machine Testimony*, 126 Yale L.J. 1972, 2018–19 (2017).

[6] *See* William C. Thompson, Laurence D. Mueller, & Dan E. Krane, *Forensic DNA Statistics: Still Controversial in Some Cases*, 36 The Champion 12, 17 (Dec. 2012).

[7] President's Council of Advisors on Sci. & Tech., *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* 79 (2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

secrecy has hampered the ability of defendants to test prosecution experts' claims about the reliability of the technology. *See, e.g.*, *State v. Pickett*, 466 N.J. Super. 270 (App. Div. 2021). When defendants have been able to fully test the reliability of the software, including through review of source code and cross-examination of prosecution experts, they have uncovered major flaws. Review of one algorithm used in thousands of prosecutions in New York "demonstrated the software . . . was unreliable, did not work as intended, and had to be eliminated." *Id.* at 278. After another algorithm maker, STRmix, was forced to disclose its source code in 2015, "analysts discovered coding errors that led to misleading results." *Id.*

In light of the complexity of the algorithms, prosecutors in jurisdictions across the country have recognized that if they are to seek introduction of probabilistic genotyping results, it must be through testimony of experts deeply familiar with the technology. *See*, *e.g.*, *United States v. Lewis*, 442 F. Supp. 3d 1122, 1126 (D. Minn. 2020) (testimony by co-founder of STRmix); *People v. Davis*, 75 Cal. App. 5th 694, 713–14 (2022) (same). Robust application of the *Daubert* standard requires as much; if such evidence is ever to be admissible, it can only be through introduction and adversarial testing of testimony

of competent experts. Any weakening of the *Daubert-Lanigan* standard would undermine that protection.

B. Facial recognition technology

Facial recognition technology (FRT) is a tool that relies on proprietary algorithms to attempt to identify unknown individuals. Different FRT systems function differently, but in general they use machine-learning algorithms that are trained to extract unique biometric signatures (often called faceprints) from photos of faces, and to compare those faceprints to attempt to match different images of the same person. The companies that make FRT source code, algorithms, and training datasets consider the technology proprietary.[8]

There are significant concerns about the reliability of FRT. These concerns include the well-documented risk of misidentification due to suboptimal photo quality, manipulation of photos by police personnel

[8] *See* U.S. Gov't Accountability Office, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses* 20, 33 (July 2020); Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It.*, N.Y. Times (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ ("The facial recognition software that law enforcement agencies use isn't currently available for public audit, and the algorithms that power the detection and identification software are often closed-box proprietary systems that researchers can't investigate.").

prior to conducting searches, and racial and gender bias in false-match rates of FRT algorithms, among other issues.[9] The adverse consequences of reliance on flawed FRT are not hypothetical; innocent people have been wrongfully arrested and jailed due to law enforcement's overreliance on this secretive, proprietary, and unreliable technology.[10]

Facial recognition technology is "novel and untested" by courts. *State v. Arteaga*, 476 N.J. Super. 36, 57 (App. Div. 2023). Even in parts

---

[9] *See, e.g.*, Christian Rathgeb et al., *Reliable Detection of Doppelgängers Based on Deep Face Representations*, 11 IET Biometrics 215 (2022) (FRT generates candidate lists that necessarily consist primarily of false positives who look like the suspect); Khari Johnson, *How Wrongful Arrests Based on AI Derailed Three Men's Lives*, Wired (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/; Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. Times (Aug. 6, 2023) (false arrest), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html; Sudhin Thanawala, *Facial Recognition Technology Jailed a Man for Days*, AP News (Sept. 25, 2023) (false arrest), https://apnews.com/article/mistaken-arrests-facial-recognition-technology-lawsuits-b613161c56472459df683f54320d08a7; Khari Johnson, *The Hidden Role of Facial Recognition Tech in Many Arrests*, Wired (Mar. 7, 2022), https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/ (reporting NIST's finding that "even the best algorithms can be wrong more than 20 percent of the time"); Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence?*, The New Yorker (Nov. 13, 2023), https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence.

[10] *See supra* note 9.

of the country where FRT is used profligately (and often without meaningful oversight) in criminal investigations, amici are aware of no case in which prosecutors have yet attempted to introduce it as evidence at trial. That is likely substantially because of the protective effect of strong enforcement of *Daubert* or *Frye* admissibility standards. But relaxation of these standards would threaten to open the floodgates to introduction of results of these proprietary algorithms, even the makers of which acknowledge are not reliable enough to serve as evidence of guilt.[11] Given that the police personnel who operate FRT searches often lack basic knowledge of how the technology works, or even which algorithms they are using,[12] a robust threshold for admissibility in court

[11] *See, e.g.*, Clearview AI Service Agreement, attached as Ex. 3 to Complaint, *Reid v. Bartholomew*, No. 1:23-cv-04035 (N.D. Ga. Sept. 8, 2023), ECF No. 1-3 ("[Clearview AI] is neither designed nor intended to be used as evidence in a court of law.").

[12] *See, e.g.*, Dep. Tr. of Nathan Howell at 24:19–20, *Williams v. City of Detroit*, No. 2:21-cv-10827 (E.D. Mich. June 16, 2023), ECF No. 50-4 (Detroit Police Department crime analyst who runs FRT searches testifying that he has "no idea" what algorithm the Department uses for such searches); Dep. Tr. of Krystal Howard at 39:16–21, *Williams v. City of Detroit*, No. 2:21-cv-10827 (E.D. Mich. July 7, 2023), ECF No. 60-3 (Director of Michigan State Police unit that conducts FRT searches unable to testify to the accuracy threshold setting in the FRT algorithms used by the agency; states that "I think that [question] would be better for our vendor").

is critical to safeguarding against unreliable results of FRT searches tainting criminal trials.

C. Criminal risk assessment tools

At all levels of the criminal legal system, judges and other state actors are relying directly on algorithmic tools to make decisions about pretrial detention, bail, sentencing, and parole.[13] Among other things, these tools purport to predict the risk that an individual will require rehabilitative resources while on parole, commit another offense after conviction, pose a threat to public safety, or fail to appear in court. Developers have resisted efforts to provide sufficient transparency about how their systems are developed and tested. For example, in response to a comprehensive ProPublica study on COMPAS, Northpointe, which created the tool, refused to share its method of calculating risk scores on the theory that its methods are proprietary.[14]

Like other algorithmic systems, these tools are susceptible to bias. Sources of potential bias range from the disproportionate

---

[13] Erin Harbison, *Understanding 'Risk Assessment' Tools*, Bench & B. Minn. (Aug. 3, 2018), https://perma.cc/7W7N-75CX.

[14] Julia Angwin et al., *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

representation of people of color at all stages of the criminal legal process, to the possibility of bad data being used to teach the algorithm, to coding errors, to reliance on factors that are proxies for race and other protected categories.[15] Without sufficient transparency, there is no way for the public to know whether any of these flaws exist in a piece of software the government is using. For example, ProPublica's 2016 report on the widely used risk assessment tool COMPAS detailed its racially biased results. According to ProPublica's data, the algorithm mistakenly labeled Black defendants as higher risk twice as frequently as it mistakenly labeled white defendants as such.[16]

As with facial recognition technology, prosecutors do not yet appear to be attempting to offer outputs from these predictive algorithms as evidence of guilt at trial. The consequences of allowing introduction of results of such criminal risk assessment tools without rigorously testing their reliability, including by requiring testimony of a knowledgeable and competent expert, would be severe. As the Wisconsin Supreme Court explained in a different context,

---

[15] *See, e.g.*, Bernard E. Harcourt, *Risk as a Proxy for Race*, 27 Fed. Sent'g Rep. 237 (2015).

[16] *See* Angwin, *supra* note 14.

transparency, accuracy, and due process concerns require that "use of a COMPAS risk assessment must be subject to certain cautions." *State v. Loomis*, 371 Wis.2d 235, 243 (2016). Any weakening of the *Daubert-Lanigan* standard would risk allowing biased and unreliable algorithmic results to taint the trial process.

D. Gunshot detection tools

Tools like SoundThinking, formerly known as ShotSpotter, claim to be able to identify and geolocate gunshots by relying on acoustic sensors and proprietary algorithms. Evidence derived from these tools is opaque, due to the proprietary nature of the technology behind it, which lacks independent validation.[17] When pressed, the technology has been revealed to be far less accurate and reliable than proponents claimed. For example, in 2016, a ShotSpotter expert admitted in trial that the company reclassified sounds from a helicopter as a gunshot at the request of a police department customer, saying such changes occur "all the time" because "we trust our law

[17] *See* Jay Stanley, *Four Problems with the ShotSpotter Gunshot Detection System*, ACLU (updated Oct. 14, 2021), https://www.aclu.org/news/privacy-technology/four-problems-with-the-shotspotter-gunshot-detection-system.

enforcement customers to be really upfront and honest with us."[18] Revelations like this and independent studies have caused this opaque technology to come under the significant criticism from civil liberties organizations, municipal governments, and researchers concerned about the reliability and the opacity of the technology.[19]

As the Seventh Circuit has recognized, courts must undertake a "searching examination of ShotSpotter's methods under *Daubert*." *United States v. Godinez*, 7 F.4th 628, 638 (7th Cir. 2021). Courts have begun to grapple with questions regarding the reliability of this technology. *Compare People v. Hardy*, 65 Cal. App. 5th 312, 329–30 (2021) (holding that admission of ShotSpotter evidence was prejudicial to defendant and insufficient to convict), *with J.A.R. v. State*, No. 4D2022-2469, 2023 WL 7365563, at *4 (Fla. Dist. Ct. App. Nov. 8, 2023) (affirming trial court order admitting ShotSpotter evidence under

[18] *Id.*

[19] *Id.*; *see also* Matthew Guariglia, *It's Time for Police to Stop Using ShotSpotter*, EFF (July 29, 2021), https://www.eff.org/deeplinks/2021/07/its-time-police-stop-using-shotspotter; John M. Ferguson & Deborah Witzburg, Chi. Office of the Inspector Gen., OIG File #21-0707, *The Chicago Police Department's Use of ShotSpotter Technology* (Aug. 2021); MacArthur Just. Ctr., *ShotSpotter Creates Thousands of Unfounded Police Deployments, Fuels Unconstitutional Stop-and-Frisk, and Can Lead to False Arrests*, https://endpolicesurveillance.com/.

Daubert standard). Even courts that have allowed introduction of such evidence at trial have done so only upon testimony of individuals with actual knowledge of the proprietary systems. *See, e.g.*, *J.A.R.*, 2023 WL 7365563, at *1 (court heard testimony from "a forensic services manager at ShotSpotter, Inc., with seven years of experience"). Robust application of the *Daubert* standard requires at least as much.

CONCLUSION

For the foregoing reasons, amici urge the Court to affirm the superior court's order to exclude the FLH evidence in this case. Doing so will confirm that new proprietary or black-box technologies cannot be admitted until and unless the government can produce an expert who has sufficient access to and knowledge about the technology's algorithm and can provide testimony that will satisfy the *Daubert-Lanigan* standard for reliability.

Date: November 28, 2023

Respectfully submitted

/s/ Jessica J. Lewis

Jessica J. Lewis (BBO #704229)
Jessie J. Rossman (BBO #670685)
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
MASSACHUSETTS, INC.
One Center Plaza, Suite 850
Boston, MA 02108
(617) 482-3170
jlewis@aclum.org
jrossman@aclum.org

Daniel K. Gelb (BBO #659703)
VICE CHAIR, FIRST CIRCUIT
NATIONAL ASSOCIATION
OF CRIMINAL DEFENSE
LAWYERS AMICUS COMMITTEE
GELB & GELB LLP
900 Cummings Ctr., Suite 207-V
Beverly, MA 01915
dgelb@gelbgelb.com

Nicola Morrow* (on the brief)
Michael J. Price (on the brief)
NATIONAL ASSOCIATION
OF CRIMINAL DEFENSE
LAWYERS
1660 L St. NW, 12th Floor
Washington, DC 20036
(202) 872-8600
nmorrow@nacdl.org

Counsel continued on next page

Chauncey B. Wood (BBO #600354)
MASSACHUSETTS ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS
55 Union St., 4th Floor
Boston, MA 02108
(617) 248-1806
cwood@woodnathanson.com

Nathan Freed Wessler
(BBO #680281)
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad St. 18th Fl.
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Jennier Stisa Granick (on the brief)
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm St.
San Francisco, CA 94111
(415) 343-0758
jgranick@aclu.org

Hannah Zhao (on the brief)
Andrew Crocker (on the brief)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St.
San Francisco, CA 94109
(415) 436-9333
zhao@eff.org

* New York bar admission pending

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 17(c)(9) of the Massachusetts Rules of Civil Procedure, I, Jessica Lewis, hereby certify that the foregoing brief complies with the rules of court that pertain to the filing of amicus briefs, including, but not limited to:

> Mass. R. A. P. 16(e) (references to the record);
> Mass. R. A. P. 17(c) (cover, length, and content);
> Mass. R. A. P. 20 (form and length of brief); and
> Mass. R. A. P. 21 (redaction).

I further certify that the foregoing brief complies with the applicable length limitation in Mass. R. A. P. 20 because it is produced in the proportional font Times New Roman at size 14 points and contains 4,071 total non-excluded words as counted using the word count feature of Microsoft Word 365.

Date: November 28, 2023 *Jessica J. Lewis*
Jessica J. Lewis (BBO #704229)

CERTIFICATE OF SERVICE

Pursuant to Mass. R. A. P. 13(e), I hereby certify, under the penalties of perjury, that on this date of November 28, 2023, I have made service of a copy of the foregoing brief in the above captioned case upon all attorneys of record by electronic service through eFileMA.

Date: November 28, 2023 *Jessica J. Lewis*
Jessica J. Lewis (BBO #704229)