F3 Litigating the Admissibility of Black Box Forensic Software

Kevin Riach, JD, Fredrikson & Byron, PA, Minneapolis, MN 55402; Charles A. Ramsay, JD*, Ramsay Law Firm, PLLC, Roseville, MN 55113*

Learning Overview: After attending this presentation, attendees will have a better understanding of the practical issues unique to *Frye* and *Daubert* litigation regarding the admissibility black box forensic software and will have learned practical strategies to deal with those issues.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by improving the competence of lawyers and expert witnesses who face the challenge of litigating the reliability and admissibility of evidence generated by black box forensic science software.

The universe of "black box" forensic software has expanded rapidly in the past several years. From probabilistic genotyping to breath alcohol measurements to facial recognition, and more, a new wave of computer-generated evidence is becoming commonplace in criminal prosecutions. But the need for transparency in the forensic sciences and in criminal law is in tension with software developers' desire to protect the "special sauce" behind their programs. Not surprisingly, this tension has generated new challenges for lawyers and experts. Source code review, evaluation of software testing documentation, and wrangling over disclosure of proprietary technology are increasingly critical aspects of litigating the admissibility of forensic evidence in criminal cases.

This presentation will discuss the practical difficulties with litigating the admissibility of evidence generated by black box software, including the use of protective orders and Non-Disclosure Agreements (NDAs) by software developers, the need to evaluate and challenge computer-generated evidence from not just a forensic science but also a software engineering perspective, and how non-scientists can begin to approach understanding the mechanisms employed by complex software systems sufficiently to challenge those systems in court. The presenters will share their experiences litigating the admissibility of evidence generated by probabilistic genotyping software and computerized BrAC systems, and the lessons gained from those experiences.

Attendees will learn strategies for propounding discovery to the third-party companies that develop and sell black box forensic software, as well as strategies for litigating the inevitable disputes that arise from these discovery requests. Attendees will also learn how the discipline of software engineering applies when evaluating the admissibility of black box forensic software. This presentation will address specific validation and verification standards commonly applied in the software industry and relevant to forensic software, ways to incorporate those standards into a *Frye/Daubert* proceeding, and what objections lawyers can expect from forensic software developers to the use of these standards to evaluate a software program's reliability. This presentation will discuss resources available to lawyers to advance their understanding and obtain expert assistance with respect to these standards. Finally, attendees will gain insight into the trends in black box forensic software—what disciplines are likely to see a rise in the use of such software and how courts' views regarding the admissibility of such software have been changing over time.

Black Box, Litigate, Software

*Presenting Author