F39 Black Boxes and Due Process: Transparency in Expert Software Systems

Dan Krane, PhD, 3640 Colonel Glenn Highway, Dept Bio Sci, Dayton, OH 45435; and Nathaniel D. Adams, BS, Wright State University, 3640 Colonel Glenn Highway, Dayton, OH 45435*

After attending this presentation, attendees will better understand the advances being made in the use of expert software systems for the analysis of forensic evidence and the legal ramifications of insufficient evaluation of such systems.

This presentation will impact the forensic science community, the legal community, and society by describing the difficulties surrounding the design, implementation, testing, and validation of such software from a computer science perspective and how these difficulties must be accounted for when admitting results from expert software systems as evidence in criminal proceedings.

Software has generally been used to assist the analysis of forensic evidence via two main routes: data visualization (such as spectrograms or electropherograms) and statistical calculations. Both of these routes have served primarily to expedite the work performed by human experts during their evaluations of complex data sets.

Methods for conventional analysis of evidence such as breath alcohol or DNA (and even ballot counting) are widely known, take a specific set of known input values, and produce results that can be independently confirmed by other experts using generally accepted approaches. Processes performed by humans are inherently subject to review by other humans. Human experts are rightly required to testify as to the validity of their conclusions by revealing their underlying measurements, calculations, and approaches.

Advances in our understanding of complex chemical and biological processes, statistics, and computational methods have brought us to the cusp of a new era — the development of expert software systems intended to evaluate evidence that cannot be interpreted by conventional human analysis. Where forensic scientists might summarize test results as "uninterpretable" or "inconclusive," expert software systems have begun to provide very definitive conclusions. This evolution of the use of software (from improving workflow to actually interpreting evidence) has critically important implications for the criminal justice system.

When computer software rather than human experts make decisions regarding the evaluation of evidence, an effective review of these software systems is required in order to fully evaluate the performance of the system. Expert systems must, necessarily, incorporate assumptions about the operating characteristics of the tests being evaluated. The accuracy of the conclusions reached by these systems depends on the accuracy of those underlying assumptions — *and* their implementation. If independent experts cannot identify those assumptions (ideally, by examining the underlying source code), then it is very difficult to assess the reliability of the expert systems. An early proof of this point came from an in-depth, independent review of the source code used by the Alcotest 7110 MKIII-C breath alcohol analyzer software (not even an expert system). The use of this software as an unscrutinized "black box" allowed simple programming mistakes to go undetected for years.

Unlike human analysts who can sometimes struggle to explain how their approaches are objective and based on experimentally validated rules, expert systems have the distinct advantage of being based on source code that unambiguously details the exact means by which they arrive at conclusions. If an adversary objects to some portion of an expert system's approach to solving a problem, it should be possible to scrutinize the validation study, algorithm, or source code and to precisely identify the basis of the disagreement. While it may be difficult to critically review the source code of some expert systems, failure to have the opportunity to review the entire basis of an expert computer system's conclusions raises serious and legitimate concerns about due process. Lack of access in these contexts operates, in essence, as a failure to fully have the opportunity to understand or confront significant, perhaps even the most significant, evidence in a case. Expert software systems must be held to the same standards of transparency that we have come to expect of human experts.

If the source code of a black box system were disclosed, the box would be open to independent scrutiny. The main justification for maintaining black box software is the protection of intellectual property. Courts will need to decide whether the desire for secrecy (in order to protect a perceived commercial advantage) outweighs the right of defendants to fully examine the evidence against them.

Black Box, Probabilistic Genotyping, Due Process