Chapter 21
Legal Issues for Research and Practice in Computational Forensics

Adel Elmaghraby
University of Louisville, USA

Deborah Keeling
University of Louisville, USA

Michael Losavio
University of Louisville, USA

ABSTRACT

We examine legal issues that must be considered in the use of computational systems in forensic investigations. There is a general framework for the use of evidence relating to legal proceedings, including computational forensic (CF) results, that all nations employ; we note some differences in procedures in different countries, although the focus in on Anglo-America practice as it is the most strict. Given the expert nature of computational systems and forensics using computation, special issues of reliability relating to science-based forensic conclusions must be addressed. We examine those generally (applicable to all CF) and as specifically applied to certain CF methods, examining two case studies on the possible use of CF methods in legal forums.

INTRODUCTION

These special issues of reliability require that the principles, method, application and expert using a CF system be validated as accurate, relevant, competent and appropriate for use by a finder-of-fact to an identified level of confidence. This testing for appropriate forensic use is especially important as conclusions from the results of these systems may have serious impact on the life and liberty of individuals.

Researchers in computational forensics may be challenged as to

DOI: 10.4018/978-1-60566-836-9.ch021

i) the evaluation of their system against the general legal framework for evidence,
ii) measurement of computationally-based conclusions against one or more tests for reliability and
iii) the weight of their conclusions in a judicial determination.

Early and ongoing assessments by computational forensic researchers can guide the process, protocol and evaluation of their work to assure appropriate use in forensic environments.

"Evidence" is a flexible term with flexible application. CF evidence, as with evidence in general, may fall along a spectrum of reliability. It may be appropriate for one type of use in the administration of justice but not another. Even if it has no use in a judicial forum, such as with lie-detector testing in U.S. courts, it may have private application to guide decision-making in private settings. Assessing, quantifying and establishing the reliability of a computational forensic system is essential for its forensic use and credibility.

BACKGROUND

Computational Forensics (CF) has been described as

... an emerging interdisciplinary research domain. It is understood as the hypothesis driven investigation of a specific forensic problem using computers, with the primary goal of discovery and advancement of forensic knowledge. CF works towards (1) in depth understanding of a forensic discipline, (2) evaluation of a particular scientific method basis and (3) systematic approach to forensic sciences by applying techniques of computer science, applied mathematics and statistics. (Franke and Srihari 2007)

Franke and Srihari (2007) assert that computational systems enhance forensic systems in several ways. These include production of objective, reproducible analytical conclusions, quality analysis of examination methods, examination of large data sets, visualization and pattern recognition. But they note significant concern about proper validation of computational forensic techniques to assure their reliability and the importance of a systematic approach to computational forensics, cooperation between forensic and computational scientists and continued peer -review and testing of computational forensic techniques.

Saks and Koehler (2005) note the lack of rigor in many forensic techniques, list the large error rates in some, as high as 60%-100% and advocate application of the basic research model of validation to all such techniques. Their model for proper forensic validation is that used for the validation of DNA match systems. Murphy (2007) details similar problems with adequate validation of forensic techniques, particularly with the expansion of supposedly science based methods. She notes the additional problem of proprietary forensic systems where external, third party of validation and peer review is difficult, if not impossible. (Murphy 2007)

Yet the potential for computational forensic techniques is tremendous, if not absolutely necessary for the investigation of distributed misconduct involving computing systems. The sheer scale of digital crime may necessitate the expansion of computational forensic systems for digital crime investigation. For example, Wong, Kirovski, and Potkonjak (2004) posit that computational forensic engineering of an analytical engine using statistical information can be effective in recognizing intellectual property infringement; such a computational forensic engine could overcome scale problems inherent in the