B28 Unintended Consequences: Digital Forensics Literacy and the Legal System

Barbara E. Endicott-Popovsky, PhD, and Donald J. Horowitz, JD, 4311 11th Ave NE, Ste 400, Seattle, WA 98105*

After attending this presentation, attendees will be able to achieve a retrospective of where the legal system stands with regard to digital evidence literacy, learn the potential consequences to the legal system if changes aren't initiated, and gain a description of one university's way forward.

This presentation will impact the forensic science community by voicing concerns over the alarming gap in the legal community's understanding of digital evidence. While the rule of law makes society a dependable environment in which to prosper and flourish, the lack of a predictable legal infrastructure has dire consequences.

Trust binds a society together. The rule of law makes society a dependable environment in which to prosper and flourish. The lack of a predictable legal infrastructure has dire consequences.[1] In this context, one must recognize that there is an alarming gap in the legal community's understanding of digital evidence, the technology community's understanding of how the legal system works, and how both can work constructively together.

In this presentation, one case is examined from a small community where the consequences of an inappropriate court ruling and a potential miscarriage of justice were avoided more as a matter of serendipity than of insight. Case specifics were examined, reminiscent of Amero,[2] and conclusions drawn about what this means generally to the state of digital evidence and its use in the justice system. Additionally, the evolution was traced of the general effectiveness of digital forensics evidence presentations and rulings, then extrapolate going forward as to where the evolution of technology may lead.[3-8]

Societal understanding, judgment, and decisions will always lag the development of technology; however, the consequences to the stability of the legal system as it slowly adapts to the changing nature of digital evidence and all that this implies, is staggering. Allowing the current state of digital evidence literacy to continue will likely include: decreasing trust in the predictability of legal decisions affecting the e-economy and, thus, the e-economy itself, and a general impedance of the progress of the Information Age—as online business and communications may increasingly no longer be viable or sustainable. It is incumbent upon those informed members of the technical community who are watching this potential train wreck evolve, to engage in dialogue with those communities that are impacted by the innovations but need help in digesting them and using them. Likewise, the technical community needs help in better understanding the practical ways the justice system—its laws, procedures, and decision process—work so that going forward, more relevant and effective innovations can be produced. Further, the legal system needs help in evaluating the validity and weight of evidence and other information in developing laws that affect judicial decisions.

One initiative being launched at a university law school in conjunction with an information school to deal with this problem will be presented. The goal of this study is that this example will ignite discussion not only about this effort but about what other efforts should be taken to improve the legal community's understanding of digital forensic evidence and the technical community's understanding of how the legal system works. Eventually, society does better understand technical innovation and adapts and evolves. In the meantime, inequities and even tragedies inevitably occur. This presentation will encourage dialogue about what this community can do to apply what has been most effective in understanding and using other forms of scientific evidence.

References:

1. H. Varian, "The PBIs on Economics of Computer Security," presentation at School of Information Management, Univ. of Calif., Berkeley, 10 Nov. 1998; www.ischool.berkeley.edu/~hal/ Talks/security.pdf.
2. N. Willard, "The Julie Amero Tragedy," Center for Safe and Responsible Use of the Internet, Feb. 2007; http://csriu.org/onlinedocs/AmeroTragedy.pdf.
3. B. Endicott-Popovsky, B. Chee, and D. Frincke, "Calibration Testing of Network Tap Devices," *Advances in Digital Forensics III*, Springer, 2007, pp.1–13.
4. M. Lawson and R. Lawson, *Expert Witness Testimony*, Global CompuSearch, 2003.
5. "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors," NIJ Special Report, U.S. DOJ, Jan. 2007; www.ojp.usdoj.gov/nij/pubs-sum/211314.htm.
6. M. Wilson and J. Hash, "Building an Information Technology Security Awareness Training Program, NIST special publication 800-50.D, U.S. Nat'l Inst. Standards and Technology, 2003.
7. B. Endicott-Popovsky, D. Frincke, and V. Popovsky, "Designing a Computer Forensics Course for an Information Assurance Track, *Proc. 8th CISSE*, U.S. Military Academy at West Point, 2004, pp. 59–64.
8. D. Frincke and M.-Y. Huang, "Editorial: Systematic Advances in Forensic Engineering (SADFE),"*Proc. 2nd Int'l Workshop Systematic Approaches to Digital Forensic Eng.*, IEEE CS, 2007, pp. viii–xii.

Digital Evidence, Literacy, Legal System