Annual ADFSL Conference on Digital Forensics, Security and Law

2017
Proceedings

May 16th, 1:30 PM

Downstream Competence Challenges and Legal/Ethical Risks in Digital Forensics

Michael M. Losavio
University of Louisville, michael.losavio@louisville.edu

Antonio Losavio
University of Central Florida, amlosa01@gmail.com

DOWNSTREAM COMPETENCE CHALLENGES AND ETHICAL/LEGAL RISKS IN DIGITAL FORENSICS

Michael M. Losavio
Department of Criminal Justice
University of Louisville
Louisville, KY USA
michael.losavio@louisville.edu

Antonio Losavio
University of Central Florida
amlosa01@gmail.com
Orlando, FL, USA

ABSTRACT

Forensic practice is an inherently human-mediated system, from processing and collection of evidence to presentation and judgment. This requires attention to human factors and risks which can lead to incorrect judgments and unjust punishments.

For digital forensics, such challenges are magnified by the relative newness of the discipline and the use of electronic evidence in forensic proceedings. Traditional legal protections, rules of procedure and ethics rules mitigate these challenges. Application of those traditions better ensures forensic findings are reliable. This has significant consequences where findings may impact a person's liberty or property, a person's life or even the political direction of a nation. Conversely, a legal, procedural or ethical failure leads to a failure in the mission of the system of justice and of public security

We examine this for digital forensics and outline a framework to mitigate the risk of a forensic and security failure.

Keywords: digital forensics, competence, legal, ethical, ineffective assistance of counsel

1. INTRODUCTION

A regime of public security under rule of law should be fair and reliable. The human factor is massively important. One aspect of this is the use of by investigators and technicians of digital and computational forensics to identify the source of criminal conduct and, potentially, the offender responsible. This permits deterrence and incapacitation as to those offenders and others who may seek to emulate them. It requires a definable certainty in application; arbitrary security produces no deterrence and chaotic enforcement. The human factor in forensic systems used for the detection, recovery and prevention of future

compromises must be recognized, addressed and fortified.

Digital and computational forensics within the system of justice require compliance and testing under systems for checking reliability that have evolved over millennia. They include three particular components to assure the reliability of outcomes that, properly applied, incorporate the reliability mechanisms of other disciplines to best assure correct outcomes. Those are gateway rules of reliability, means to assess the "weight" of the evidence and a framework of laws, procedures and ethics to protect the integrity of the juridical and fact-finding process.

This last component is a vital to protecting the integrity and authenticity of the other two technical components. As an interdisciplinary forensic domain, digital forensics must incorporate that integrity. The failure to do so, if only through ignorance, may lead to the failure of the forensic mission, the acquittal of the guilty, conviction of the innocent, and doubts about the justice in the system of justice.

2. THE FRAMEWORK FOR FORENSIC RELIABILITY AND EFFECTIVENESS IN THE UNITED STATES

Fundamental to the Anglo-American legal system is an adversarial testing process. That testing process can only be effective when both the prosecuting state and the accused defendant can properly put forward and test the evidence relating to guilt or innocence. Murphy argues the current structure of our adversarial process is ill-suited to validate the integrity and weight of evidence from high-level systems, such as digital forensics; this is due, in part, to a process that is not transparent and relies heavily on a balance of skills and counsel rather than oversight validated by the court or other third-party validation sources. [1]

2.1 The Legal Standard for Ineffective Assistance of Counsel under clearly established Supreme Court precedent

The Sixth Amendment to the Constitution of the United States provides that

> "In all criminal prosecutions, the accused shall enjoy the right ...***to have the Assistance of Counsel for his defence.***" (emphasis added)

The United States Supreme Court said "the right to counsel is the right to the *effective assistance of counsel*" (emphasis added) [2]. To be of effective assistance, counsel's advice must be "within the range of competence demanded of attorneys in criminal cases."

The test for granting relief due to ineffective assistance of counsel was set out by the Supreme Court in the case *Strickland v. Washington* [3]*;* the Supreme Court held that in order to grant relief from a conviction on allegations of the ineffective assistance of counsel:

> First, the defendant must show that counsel's performance was deficient. This requires showing that counsel made errors so serious that counsel was not functioning as the "counsel" guaranteed the defendant by the Sixth Amendment. Second, the defendant must show that the deficient performance prejudiced the defense. This requires showing that counsel's errors were so serious as to deprive the defendant of a fair trial, a trial whose result is reliable.

The Supreme Court in *Strickland* said "The purpose of the Sixth Amendment guarantee of counsel is to ensure that a defendant has the assistance necessary to justify reliance on the outcome of the proceeding.

The state itself bears the risk of ineffective assistance of counsel being given a defendant. [4]

A defendant alleging the ineffectiveness of counsel's assistance must show that counsel's representation "fell below an objective standard of reasonableness." [5]

In discussing the nature of that standard, the Supreme Court stated, "Counsel also has a duty to bring to bear such skill and knowledge as will render the trial *a reliable adversarial testing process*" (emphasis added) [6]. Prejudice may be presumed for "... various kinds of state interference with counsel's assistance" and the complete denial of counsel. [7] Outside of this small group of cases, ineffective counsel may only be remedied if prejudice to a defendant may be shown; the test for prejudice is

> The defendant must show that there is a reasonable probability that, but for counsel's unprofessional errors, the result of the proceeding would have been different. A reasonable probability is a probability sufficient to undermine confidence in the outcome [8].

The Supreme Court specifically rejected a requirement that the showing of prejudice was that it was more likely than not that the error affected the outcome. "... [W]e believe that a defendant need not show that counsel's deficient conduct more likely than not altered the outcome in the case" [9].

The touchstone is that the outcome is reliable [10]. Thus, claims of ineffective assistance of counsel due to the failure to use computer forensic expertise, at their core, assert the outcome of the case is not reliable because computer forensic expertise was essential in understanding a case and preparing a defense.

One example of this may be the kind of case represented by the *State of Connecticut v. Amero* prosecution of a substitute teacher due to flawed testimony regarding online activity relating to pornography.

Where competent analysis of such systems is blocked, as may occur with child pornography prosecutions, a *de facto* claim of ineffective assistance of counsel may be made as well as interference with a defendant's ability to make out a defense to allegations against him.

2.2 Warning Signs- Ineffective Assistance of Counsel and Digital Evidence

A 2011 study of litigators found law schools were not yet preparing law graduates for dealing with electronic evidence or digital forensics and recommended continuing education for judges, prosecutors and practicing attorneys in this area [11]. Though the survey respondents found significant impact of digital forensics evidence in litigation, there was also a reluctance to use digital forensics experts for testimonial purposes, preferring to restrict them to the examination of media.

Another analysis of legal and ethical issues and liabilities between attorneys and digital forensics experts concluded that an adaptive framework that both clearly defines and separates the responsibilities of those parties, along with adherence to "best practices," would best promote the effective use of electronic evidence and the avoidance of risk [12].

Yet another 2011 study noted that this system requires an effective adversarial system with the effective assistance of counsel for defendants in criminal prosecutions; this was

all the more critical given the growing use of digital forensics in legal matters in the United States [13].

Under the American legal system, the failure of an effective assistance of counsel due to issues relating to digital forensics and evidence can be grounds to reverse and vacate a judgment and sentence; conversely, unrecognized it may lead to the conviction of an innocent party.

2.3 Case Law

The problem of the properly qualified lay witness versus expert witness has been an issue in state cases.

In *Wilder v. State*, 191 Md. App. 319, *cert. denied*, 415 Md. 43 (2010), a conviction was reversed where, over objection, a police detective was improperly permitted to give lay opinion testimony. This addressed how he had been able to track the defendant's movements "through GPS or cell tower hits" that the court found should have been made by a properly qualified expert *Id.* at 354.

In the murder case of *Coleman-Fuller v. State*, 192 Md. App. 577 (2010), despite defendant's objection prior to trial, the prosecution was permitted to introduce cell tower data placing the defendant at the scene of the crime through a police detective "instead of an expert witness." *Id.* at 580. The motion was denied. This, too, was reversed as the detective had "rendered an opinion on [the defendant]'s location at the time of the calls," and it was "clearly error" for this testimony to be admitted through a lay witness and not a duly qualified expert. *Id.* at 619.

Table 1
2016 USDC cases

Claim	Outcome
Failing to object to "false testimony" of prosecution computer expert[15]	Dismissed
1) failure to obtain an independent analysis of defendant's computer 2) failure to require authentication pictures and video clips[16]	Dismissed 1) failure to show ineffective assistance-no demonstration that failure to conduct analysis was outside a reasonable attorney's "range of competence" 2) failure to show prejudice
failure to review materials on federal "view only" computer failure to object to forged/inauthentic electronic documents [17]	Dismissed 1) no evidence such a computer existed 2) no showing that the lack of objection was tactical nor of any impact on case outcome
Failure to challenge computer data proving predicate convictions [18]	Dismissed 1)No showing of prejudice as sufficient prior convictions without computer alleged
Failure to timely reveal defense expert report of third-party introduction of contraband on his computer [19]	Dismissed 1)insufficient showing that plea was involuntary due to lack of knowledge of redundant second report
Failure to access and examine computer for exculpatory evidence [20]	Dismissed, as 1) no specific exculpatory evidence presented. 2)evidence was that purported documents were never successfully deployed. 3)evidence of guilt overwhelming (600 prosecution exhibits) Thus, no prejudice shown

The Maryland Court of Appeals, in the context of ineffective assistance of counsel failure to object to such evidence, noted such a challenge would require a full record to establish any strategic grounds a trial attorney may have had for not making objection to insufficiently qualified testimony [14].

Subsequently, in the murder case of *Payne & Bond v. State*, 211 Md. App. 220 (2013) a detective, over objection, testified to inferences regarding cell phone tower location and recipient reception.

Table 1
2016 USDC cases

Claim	Outcome
Failing to object to "false testimony" of prosecution computer expert [15]	Dismissed
1) failure to obtain an independent analysis of defendant' s computer 2) failure to require authentication pictures and video clips [16]	Dismissed 1) failure to show ineffective assistance-no demonstration that failure to conduct analysis was outside a reasonable attorney's "range of competence" 2) failure to show prejudice
failure to review materials on federal "view only" computer failure to object to forged/inauthentic electronic documents [17]	Dismissed 1) no evidence such a computer existed 2) no showing that the lack of objection was tactical nor of any impact on case outcome
Failure to challenge computer data proving predicate convictions [18]	Dismissed 1)No showing of prejudice as sufficient prior convictions without computer alleged
Failure to timely reveal defense expert report of third-party introduction of contraband on his computer [19]	Dismissed 1)insufficient showing that plea was involuntary due to lack of knowledge of redundant second report
Failure to access and examine computer for exculpatory evidence [20]	Dismissed, as 1) no specific exculpatory evidence presented. 2)evidence was that purported documents were never successfully deployed. 3)evidence of guilt overwhelming (600 prosecution exhibits) Thus, no prejudice shown

2.4 At the Extremes – IAC claims & Digital Forensics in U.S. District Court 2015-2016

The United States District Court cases examined from the two-year span of 2016-2015 of such cases involving claims of ineffective assistance of counsel in relation to work with computers. The cases span the country, from Pennsylvania, Nevada, North Carolina, South Carolina, California, Tennessee, New Jersey, Virginia, West Virginia and Alabama. Although a relatively small sampling with 12 cases-six in each of the two years- this represents a significant increase over previous years in the adjudication of such claims.

Although some asserted claims reflect the rococo nature of ineffective assistance of counsel claims, this sampling indicates key areas that may

bring into question the effectiveness of the adversarial process. Primary was a failure to properly examine prosecution evidence against a defendant, with a particular focus on failure to properly use a computer forensic expert in this process. Another recurring issue relates to authentication of electronic evidence and a failure to either do so or object to the failure of such authentication.

Table 2
2015 USDC cases

Claim	Outcome
Failure to investigate third party placement of contraband on devices [21]	Dismissed 1)evidence in discovery indicated strict oversight by defendant 2)reasonable action by counsel
Failure to request jury instruction inferring exculpatory evidence when government destroyed computer [22]	Dismissed 1)trial court ruled that no bad faith spoliation by government, so instruction was not warranted
Failure to subpoena computer records showing IP address of threats was victim' s own computer [23]	Dismissed 1)evidence "unequivocal" threats came via son's computer and email account in order to make ex-wife think son was threatening her; "The Court is at a loss for words."
Failure to secure independent computer forensic expert [24]	Discovery order GRANTED 1)sufficient showing of specific exculpatory items that discovery might permit
Failure to investigate access by computer repair service placing contraband; failure to investigate independent expert's analysis of email origin; failure to investigate alibi witnesses [25]	Dismissed 1)insufficient showing of time/date issues that repairs led to contraband 2)email irrelevant as guilty plea was to child pornography possession 3)insufficient showing of alibi correlation as defense Thus, counsel not ineffective
Failure to move to suppress evidence from search of home and computer due to staleness [26]	Dismissed

Although nearly all of these claims were dismissed as insufficient, they serve as a bellwether of future scrutiny regarding computer forensic practices. The one case where the order granted further discovery came where the defendant was able to specifically point to areas and evidence that an independent computer forensics expert would have been able to recover in support and exculpation of the defendant. In nearly all other cases the failure to define with specificity how a defendant was prejudiced led to their failure; this may change with greater sophistication in the framing of these types of claims that must then be met by proffers of proper procedures and evidence by the prosecution.

3. ETHICAL CONCERNS

Ethics in science and research are important, especially when they involve people. Researchers at most American universities are familiar with the requirements of the

Institutional Review Boards (IRB) that oversee research processes that involve human subjects. The role of the IRB is to minimize risk to those human research subjects and to reflect proper respect for their rights as autonomous individuals.

Further, for digital and computational forensics science, ethics may be subsumed and viewed as issues of professional ethics from several perspectives, offering guidance in the development and application of computational forensic systems.

Ethics is viewed as a core competency of forensics practice [27] computer science education [28] and legal/judicial practice [29]. By touching each of these domains digital and computational forensics must comply with all of their ethical restraints.

An ethical breach by either counsel or the digital forensics expert may be grounds for a mistrial, impeachment, sanctions, admonition from the court and a post-trial challenge for prosecutorial misconduct or defense ineffective assistance of counsel. Such a breach undermines the reliability and integrity of the judicial process and brings the outcome into question.

3.1 Professional Ethics in Forensics

Forensic sciences, by definition, may have judged in judicial fora. One vetting mechanism before the finder of fact is to test the honesty and competence of the expert witness. Forensic societies have advocated and adopted their own codes of ethics to police their own disciplines and best assure their credibility against claims of bias.

The AmericanAcademy of Forensics Sciences (AAFS) Code of Ethics and Conduct generally prohibits conduct by any member adverse to the mission of AAFS to promote the forensic science [30].

In particular, AAFS expressly prohibits members from making:

a) “any material misrepresentation of education, training, experience or area of expertise” or

b) “any material misrepresentation of data upon which an expert opinion or conclusion is based”

Though brief, the AAFS Code differs from those of the ACM and IEEE in that it provides for a full due process procedure to adjudicate violations. Where found, graded punishments of censure, suspension or expulsion may be given the violator. Ethics proceedings alleging unethical conduct can be highly contentious.

Such sanctions may have a significant impact on the credibility and weight of scientific analysis. The analyst may use AAFS membership to validate his or her expertise [31]. Such claimed validation or even general qualifications may be attacked by showing the analyst is not a member of AAFS [32], [33].

The Code of Conduct for La Société canadienne des sciences judiciaires of is more detailed than that of the AAFS. [34] It mandates candor, confidentiality, disclosure, documentation and preservation of work product and standards for technical analysis, including “general acceptance” of the technique and use of standards and controls to assure repeatable results. But it does not have detailed provisions for sanctions for violating these rules.

The Australian and New Zealand Forensic Sciences Society Code of Ethics incorporates some of these features, but expands upon application of the scientific method, reporting, pre-trial conduct, court conduct and relations with clients, including a ban on contingent fees [35]. While requiring members to adhere to this

code, there is no code-specific mechanism for enforcement or sanctions for violations; ANZFSS does have a general provision for expulsion of members.

Violations of or non-compliance with these ethical precepts may be grounds to challenge the credibility of an analyst applying computational techniques.

3.2 Interrelationship with requirements for Legal and Judicial Ethics

Where the forensics expert is retained by a judge or lawyer to provide analysis, the ethical obligations of the judge or lawyer carry over to conduct by the forensics expert.

Fundamental to this ethics framework in the United States are the rules of professional conduct governing attorneys [36]. The rules of professional conduct for attorneys mandate they act to assure *anyone* they employ, retain or work with conduct themselves in accordance with the professional obligations of the attorney. This includes both the rules of professional conduct but also the rules of court in cases involving litigation. Failure to do so puts the attorney at risk of ethical sanctions, court sanctions and civil liability. The commentary to Rule 5.3 notes the protective measures must account for the lack of legal training and that non-lawyer assistants, staff and retained experts often *"are not subject to professional discipline"* (emphasis added) [37].

Some of the ethical obligations transferred to analysts include:

Competence
Diligence
Confidentiality of Information
Conflict of Interest
Candor toward the Tribunal
Fairness to Opposing Party and Counsel
Meritorious Claims and Contentions
Truthfulness in Statements to Others
Respect for Rights of Third Persons [36]

Violation of ethical obligations by the forensic analyst can lead to severe sanctions and possibly even the exclusion of the expert analysis [38]. These sanctions are in addition to challenges to the credibility of the analyst and her analysis.

Given the severity of sanctions for violations of ethics in computing, forensic science and conduct before a judicial forum, computational techniques in forensic analysis must be applied in accord with all of these ethics rules.

4. OBSERVATIONS AND CONCLUSIONS

In moving from the laboratory into the system of justice, digital and computational forensics and its benefits are embedded in a basic framework of legal and ethical rules. Development of computational systems for forensic analysis must integrate this framework into those systems. This may best be done understanding and applying these fundamental requirements for legal evidentiary reliability and professional ethics in the course of moving from the laboratory to the courtroom.

This basic framework may not be sufficient in the long-term. Risks of misuse continue precisely because new scientific techniques, including those employing computational analysis, are more arcane and less susceptible to public and private scrutiny. Greater technical sophistication, proprietary and confidential technologies and growing jury deference to expert analysis lead to less testing of reliability in both the laboratory (peer review) and the courtroom (cross-examination.) Indeed, there may be an ever-greater long-term risk of misuse of digital and computational forensics as only proprietary corporations and government laboratories

support prosecutorial efforts can afford to test these systems.

The sheer power of digital and computational forensics for data analysis and matching from new data sources go beyond improved investigations; it is a proactive tool to identify perpetrators in ways not possible before. Computational techniques offer unprecedented benefits for criminal justice analysis, but offer new risks. It is all the more important that the development, application and use of CF occur in an ethical environment that addresses those risks before people are injured in their rights and persons.

REFERENCES

[1] Murphy, Erin, The Mismatch between Twenty-First-Century Forensic Evidence and Our Antiquated Criminal Justice System, 87 S. Cal. L. Rev. 633 (2013-2014)

[2] *McMann v. Richardson*, 397 U.S. 759, 771, n. 14 (1970)

[3] *Strickland v. Washington*, 466 U.S. 668 (1984)

[4] *Kimmelman v. Morrison*, 477 U.S. 365 (1986)

[5] *Strickland,* 466 U.S. at 688.

[6] *Strickland*; *Hill v. Lockhart*, 474 U.S. 52, 58-58(1985)

[7] *Strickland,* 466 U.S. at 692; *United States v. Cronic*, 466 U.S. 648, 659, and n. 25. (1984)

[8] *Strickland*, 466 U.S. at 694

[9] *Strickland*, 466 U.S. at 693

[10] *Lockhart v. Fretwell*, 506 U.S. 364 (1993).

[11] Karon Murff, Hugh Gardenier, Martha Gardenier, Digital Forensics and the Law, Conference on Digital Forensics, Security and Law (2011)

[12] Harrington, Sean, (2011) Collaborating with a Digital Forensics Expert: Ultimate Tab-Team or Disastrous Duo?, William Mitchell Law Review Vol .38: Iss.1, Article 8

[13] Losavio, Michael and Keeling, Deborah, Computer Forensics and Electronic Evidence - Failure of Competent Computer Forensic Analysis and Other Computer-Related Acts as Ineffective Assistance of Counsel, 2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE) (available at IEEE Xplore DOI: 10.1109/SADFE.2011.6

[14] *Hollis v. State of Maryland*, case no. 1437, Court of Special Appeals of Maryland (September term, 2014) (unreported)

[15] *LeBlanc v. Tice,* 2016 U.S. Dist. LEXIS 171188

[16] *United States V. Byington*, 2016 U.S. Dist. LEXIS 163563

[17] *Bonfilio v. United States*, 2016 U.S. Dist. LEXIS 145142

[18] *Albritton v. United States* S, 2016 U.S. Dist. LEXIS65981

[19] *United States v. Vaskas*, 2016 U.S. Dist. LEXIS 44436

[20] *United States v. Hartsoe*, 2016 U.S. Dist. LEXIS 1509

[21] *United States v. Taylor*, 2015 U.S. Dist. LEXIS 147069

[22] *Dunn v. United States*, 2015 U.S. Dist. LEXIS 138159

[23] *Walker v. United States*, 2015 U.S. Dist. LEXIS 111152

[24] *Fenn v United States*, 2015 U.S. Dist. LEXIS 81413

[25] *Artfitch v. United States*, 2015 U.S. Dist. LEXIS 78679

[26] *United States v Simons*, 2015 U.S. Dist. LEXIS 41647

[27] M. Pollitt, *Core Competencies*, Digital Forensics Certification Board (2006)

[28] ABET Criteria for Accrediting Engineering Programs, Effective for Evaluations During the 2007-2008

Accreditation Cycle, Curriculum Standard IV-17.

[29] P. Denning, (2001) "Crossing the Chasm" Communications of the ACM, Vol. 44, No. 4, pp 21-25

[30] American Academy of Forensic Sciences Bylaws, Article II, Code of Ethics and Conduct

[31] *United States v. Hammer*, 404 F. Supp. 2d 676; DC MD Penn 2005

[32] *Dracz vs. American General Life Insurance Company*, 426 F. Supp. 2d 1373, DC MD Georgia 2006

[33 *United States v. Ferguson*, 2004 U.S. Dist. LEXIS30520, SD Ohio

[34] Code of Conduct for La Société canadienne des sciences judiciares, adopted November 5, 1994.

[35] Australian and New Zealand Forensic Science Society Code of Professional Practice, adopted August 2014

[36] American Bar Association *Model Rules of Professional Conduct*

[37] Rule 5.3, American Bar Association *Model Rules of Professional Conduct*

[38] *Fidelity Nat. Title v. Intercounty Nat. Title*, 412 F.3d 745 (7th Cir. 2005) (U.S.)

