MEMORANDUM

To: Senate Business, Labor, and Economic Affairs
From: Jimmy Weg, Weg Computer Forensics, LLC (wegcomputerforensics.com)
512 S. Roberts, Helena, MT 59601; 406-449-0565
RE: HB 354 – Montana Private Investigator Statute and Computer Forensic Examiners
Date: March 5, 2009

Thank you for considering HB354, which will revise Montana's private investigator statutes. My interest lies only in Section 3, which proposes an exemption for forensic practitioners at 37-60-105(k). In fact, I was the instigator of that amendment, when I raised the issue at a meeting of the Board of Private Investigators in March 2008. At that meeting, the Board voted unanimously (with one abstention) to adopt what is suggested in 37-60-105(k). The Board agreed that the practice of forensics should not be regulated as private investigation.

I am employed full time by the Montana Department of Justice, Division of Criminal Investigation (DCI). There, I established state's Computer Crime Unit eight years ago. I am recognized internationally as a computer forensics expert. I also engage in a part time, private computer forensics practice outside of my state job. Because of my responsibilities as a peace officer at DCI, I do not do any private work that involves the criminal justice system. I am a proponent of this bill on my own behalf and not as a state employee.

I sought an audience before the Board of Private Investigators because I was concerned that forensic computer examiners might be considered private investigators (PIs). In fact, we are very different from PIs. We work in laboratories and examine computers and digital evidence. We don't interview suspects or witnesses, conduct surveillance, or engage in the customary PI activities. We often work for licensed PIs and attorneys.

The PI statutes were not designed to regulate the forensic sciences. For example, if forensic computer examiners were required to have a PI license, private DNA labs also would require a PI license. Montana has no certified forensic computer examiners who do criminal defense work. Criminal defendants must look to examiners in other states. None of the examiners who have practiced here are licensed PIs. Should computer examiners be deemed PIs, it would preclude criminal defendants from obtaining an independent computer examination by an expert. As a matter of fact, the American Bar Association has officially urged state legislatures to refrain from regulating forensic examiners as PIs.

HB 354 also addresses issues regarding fire investigators. I have no position on that aspect of the bill. However, if the Committee takes exception to the fire investigation provisions, I hope that you will see a distinction between that portion and the one that covers the forensic sciences. Below, I will present a more technical discussion of the issues.

I. Introduction

Forensics is defined as "the art or study of argumentative discourse; the application of scientific knowledge to legal problems; especially: scientific analysis of physical evidence."[1] The use of physical evidence, e.g., tire tracks, bullets, blood, and DNA are well accepted in our courts. Television shows like *CSI* and *Law & Order* have reinforced this acceptance.

Less well known is the role of digital or computer forensic examiner in criminal and civil litigation. *Computer forensics* is the acquisition and examination information found on computers and other digital devices. Nearly everything that someone does on a computer leaves traces.

Computer forensics is increasing in importance in both public and private litigation for a number of reasons, not the least of which is that computers and the Internet represent the fastest growing technology tools in human history. Digital devices are increasingly the target, instrument, and keeper of everyday activities.

This importance can be noted in *American Bar Association Resolution 301* on computer forensics (a copy is included). It urges state legislatures, to refrain from requiring private investigator (PI) licenses for persons engaged in computer forensics. PI licensing statutes were enacted before the practice of computer forensics was envisioned. The PI licensing statutes were not designed to require persons conducting technical and scientific investigations to obtain a PI license. Montana's PI licensing statute does not provide any assurance to the public that a computer forensics examiner (CFE) is qualified to practice computer forensics. The Montana Board of Private Security agrees with this proposition, and voted to enact the amendment that is before you now.

II. Private Investigators and Computer Forensics Examiners

Private Investigator means "a person . . . who for any consideration makes or agrees to make any investigation with reference to . . . gathering evidence to be used before any court, board, officer, or investigating committee."[2]

Competent computer forensics examinations must be conducted by a CFE. Typically, a CFE is a person who holds a professional certification or degree and has training, education, and experience in the collection, preservation, examination, and analysis of digital information. CFEs interpret and examine data from computers, networks, or other digital media provided to them by another person who owns, controls, or possesses the items.

Like other forensic scientists, CFEs furnish facts gleaned from the analysis of digital data to law enforcement, attorneys, or PIs, who develop or apply these facts in further investigation. CFEs report their findings, similar to a medical examiner who may find a poison in the examination of deceased person. For example, a CFE may assist a "missing persons"

---

[1] Forensics. *Merriam-Webster's Collegiate® Dictionary, Eleventh Edition* and *Webster's Third New International Dictionary, Unabridged. [MERRIAM-WEBSTER ONLINE]*. Retrieved November 22, 2008, from http://www.merriam-webster.com/dictionary/Forensics

[2] MCA 37-60-101(19)

investigation through the forensic recovery of deleted emails that, when turned over to a PI, provide clues to help the PI find the missing person. However, it is beyond the scope of the CFE to act on the found emails and look for the missing person.

Montana's private investigator statutes could be mistakenly construed to include CFEs. Inherent in the term "private investigation" is the notion that PIs investigate a person or incident, and the PI may conduct interviews and surveillance that do not involve giving notice to a target. In contrast, a CFE works in a lab, examining electronic storage devices.

III. Differences Between CFEs and Private Investigators

Computer forensics involves the gathering, analysis, and presentation of data that is secured with the full knowledge and consent of the owner of the data. PIs operate in a fundamentally different way from CFEs. CFEs and private investigators have different responsibilities:

1. A CFE is a forensic scientist who assists courts in understanding digital evidence in determining facts. If a CFE is required to obtain a PI license, all forensic scientists, e.g., DNA labs, must be licensed.

2. A CFE serves in other litigation support: electronic discovery services, information security, computer network security, and video data analysis. CFEs are monitored by courts (as expert witnesses), businesses (as owners of the data), and by attorneys. CFEs are often retained by PIs.

3. Requiring a CFE to be licensed as a PI may
    a. provide false assurance to consumers that a CFE-PI is qualified in computer forensics. A licensed PI is not required to be qualified in computer forensics.

    b. Provide false assurance that a CFE is a qualified private investigator. A CFE is not necessarily qualified to be a PI; and,

    c. diminish citizens' access to justice by reducing the pool of qualified CFEs Montana presently has no certified CFEs who conduct criminal defense work.

Thank you for your time in reviewing this memo and the other information that I have provided. Questions and comments are welcome.

AMERICAN BAR ASSOCIATION

ADOPTED BY THE HOUSE OF DELEGATES

AUGUST 11-12, 2008

RECOMMENDATION

RESOLVED, That the American Bar Association urges State, local and territorial legislatures, State regulatory agencies, and other relevant government agencies or entities, to refrain from requiring private investigator licenses for persons engaged in:

- computer or digital forensic services or in the acquisition, review, or analysis of digital or computer-based information, whether for purposes of obtaining or furnishing information for evidentiary or other purposes, or for providing expert testimony before a court; or

- network or system vulnerability testing, including network scans and risk assessment and analysis of computers connected to a network.

FURTHER RESOLVED, That the American Bar Association supports efforts to establish professional certification or competency requirements for such activities based upon the current state of technology and science.

REPORT

This Resolution responds to a trend among state legislatures and regulatory bodies to require persons engaged in providing digital forensic and network testing services,[1] including expert testimony, to be state-licensed private investigators. The Resolution encourages state legislatures, regulatory agencies, and other governmental entities to refrain from such requirements because:

1. Investigation and expert testimony in computer forensics and network testing should be based upon the current state of science and technology, best practices in the industry, and knowledge, skills, and education of the expert.

2. The traditional role of private investigators is significantly different from that of a computer forensic or network testing professional and many licensed private investigators have little or no training in these areas. Private investigation licenses are not adequate determinants of competency in a field driven by technological innovation and science.

3. Numerous professional certifications are available to computer forensic and network testing professionals that are based on rigorous curricula and competency examinations. The experience, certifications, knowledge, and skills of a computer forensic expert are more suited to the skills required than a state private investigator license that enables one to work broadly in the investigation field.

4. The public and courts will be negatively impacted if e-discovery, forensic investigations, network testing, and other computer services can be performed only by licensed private investigators because not all licensed private investigators are qualified to perform computer forensic services and many qualified computer forensic professionals would be excluded because they are not licensed.

5. Private investigator licenses are not needed to ensure reliable evidence in litigation. Trial judges are vested with broad discretion in determining whether expert testimony is relevant and reliable; the Supreme Court has set forth a list of factors that may be used to guide them in making this determination (state licensing requirements are not a factor).

6. Data and systems are spread around the world as a result of a globally connected network and widespread use of the Internet. Thus, forensic examinations and network testing frequently involve multiple jurisdictions. A patchwork of differing

---

[1] Network testing is generally considered to be within the science of digital forensics. It is stated here separately because (1) it can require skills and activities that are not included within the first bullet of the resolution but can be interpreted as within the scope of forensic activities. A June 2007 decision from the Texas Department of Public Safety's Private Security Bureau (PSB) defined the term "private security consulting company" to include firms engaged in network scans and vulnerability testing. This ruling has since been amended. *See* "Computer Network Vulnerability Testing Firms – AMENDED January 15, 2008," Opinions Issued in Response to Questions from Industry & Public, Texas Dept. of Public Safety, Private Security Bureau; *see also* Mark J. Zwillinger, "e-Alert – State Laws Requiring the Licensing of Computer Forensic Investigators," Jan. 8, 2008.

state licensing requirements for computer forensic and network testing assistance will create jurisdictional complexities that will hamper business operations and court proceedings, disadvantage litigants, and may deprive courts of hearing the best available evidence.

7. There is very little supporting evidence that public safety or consumer protection would be served by such licensing requirements.

State Action

P.I. License for Computer Forensic Examiners
A State by State Breakdown[2]

Required by Law or Pending	Opinion by Regulatory Body or Common Knowledge that License is Required	License Possibly Required But No Specific Statements
Illinois, Texas, Michigan, Georgia, Rhode Island, South Carolina, North Carolina (pending)	Massachusetts, Nevada, New York	Arizona, Arkansas, California, Connecticut, Hawaii, Iowa, Kansas, Kentucky, Maine, Maryland, Minnesota, Montana, New Hampshire, New Jersey, New Mexico, Ohio, Oklahoma, Oregon, Tennessee, Utah, Vermont, West Virginia, Wisconsin

Even though a private investigator license does not ordinarily address the skills required for performing digital forensic work or providing forensic expert testimony, states are increasingly taking this route. Over the past two years – especially in 2008 -- there has been an alarming trend by state legislatures and state regulatory bodies governing private investigators to require that computer forensic professionals be licensed private investigators – all with very little justification of why this particular type of licensing was needed or appropriate.

In some states, violations of these licensing laws carry stiff monetary and criminal penalties, including jail time. States that have been particularly aggressive are Texas, Georgia, North Carolina, Rhode Island, Michigan, and New York.

Texas has extended its licensing requirement to computer repair shops, even though the state Private Security Bureau ("PSB") can provide no clarification of when computer

[2] Much of the information for this table was obtained from the following source: Doug White and Colleen Micheletti, "An Examination of State Laws Concerning the Practice of Computer Forensics and Private Investigation Licensure Requirements," International Society for Forensic Computer Examiners, Apr 21, 2008.

repair may be deemed to be investigative work.[3] Violations of the Texas Occupation Code carry criminal penalties of up to one year of jail time and a $4,000 fine plus a $10,000 civil penalty. Texas's PSB posted a warning on its Web site that, "Computer repair or support services should be aware that if they offer to perform investigative services . . . they must be licensed as investigators."[4] The law applies to all investigators, even employees of private sector companies if they are performing activities within the scope of the Texas law. The law also applies to consumers who hire unlicensed computer forensic personnel who perform services within the scope of the law, subjecting them to the same jail time and civil/criminal penalties. The Institute for Justice has filed suit against the PSB, alleging that the law, *inter alia,* is overly vague, violating the due course of law provision of the Texas Constitution.[5]

South Carolina has enacted a law that requires licenses for persons gathering digital evidence for use in court.[6] Such a requirement will sweep in many types of work performed in the course of gathering relevant electronically stored information for e-discovery and evidentiary purposes.

Georgia recently passed a new law that extends to computer forensics and computer incident response, with felony penalties for violations. The law is so broad, that according to one well respected computer security specialist, "The problem is that the statute is written so broadly as to include almost all types of computer forensics and computer incident response – at least when done by outside consultants."[7]

---

[3] Brian Boyko, "Interview with Capt. RenEarl Bowie of Texas Private Security Bureau Regarding Texas PI Licensing," July 8, 2008, http://www.networkperformancedaily.com/2008/07/interview_with_capt_renearl_bo.html. On October 18, 2007, the Texas Private Security Bureau ("PSB") sent a letter to Best Buy regarding their Geek Squad computer forensic services. The PSB advised Best Buy that any computer services that could be deemed to involve investigative services were in violation of the Texas Occupation Code and subject to criminal and civil penalties. *See also,* Katy Justice, "Computer repair technicians may be acting illegally: Group deems license law unconstitutional, sues on techs' behalf," *The Daily Texan,* June 27, 2008, http://media.www.dailytexanonline.com/media/storage/paper410/news/2008/06/27/TopStories/Computer.Repair.Technicians.May.Be.Acting.Illegally-3386027.shtml (hereinafter "Katy Justice"); "New Computer Repair Law Could Affect Both Company Owners and Consumers," CW33 Dallas/Fort Worth KDAF-TV, June 26, 2008, http://cw33.trb.com/news/kdaf-062608-computerspelpina,0,486476.story, Matt Miller and John Kramer, "Magnum, P.C.? New Texas Law Limits Computer Repair To Licensed Private Investigators," Institute for Justice, June 26, 2008, http://www.ij.org/first_amendment/tx_computer_repair/6_26_08pr.html (hereinafter "Miller and Kramer"); "When Geek Squad Becomes Geek Posse," *The Austin Chronicle,* June 25, 3008, http://www.austinchronicle.com/gyrobase/Blogs/News?oid=oid:639977.

[4] "Licensing Geeks, Gumshoes: Private eye law poses major computer glitch," *The Dallas Morning News,* Editorial, July 7, 2008.

[5] Rife, Hayhurst, Norelid, and Rawlins, III v. Texas Private Security Board, Case No. D-1-QN-08-002236, Tex. Dist. Ct., June 26, 2008 at 14.

[6] *See* South Carolina Law Enforcement Division, ""SC Law," http://www.sled.sc.gov/PIPrivate.aspx?MenuID=PI; Deb Radcliff, "Computer Forensics Faces Private Eye Competition, *Baseline, Jan. 2, 2008 at 1,* http://www.baselinemag.com/c/a/Projects-Security/Computer-Forensics-Faces-Private-Eye-Competition/.

[7] Mark Rasch, "Forensic felonies," http://www.securityfocus.com/print/columnists/399 (hereinafter "Rasch").

301

North Carolina's Private Protective Services Board ("PPSB") recently attempted to pass a resolution that required any individual engaged in computer forensics to be licensed if they obtained and analyzed data for the purpose of making determinations and answering questions as an expert witness.[8] Numerous experts and professional organizations came out against the proposed resolution, including the head of the computer forensics department for the Raleigh Police Department[9] and the president of the Carolinas Chapter of the High Technology Crime Investigation Association.[10] The PPSB reportedly voted to create a separate license for Digital Forensics Specialists with specified training requirements. To date, there is no official announcement of the PPSB's decision.

Background on Digital Forensics and Network Testing

The work of digital forensic professionals differs significantly from the traditional work of licensed private investigators. For example, computer forensic professionals generally do not engage in traditional investigative techniques, such as surveillance and personal interviews.

Instead, digital forensic professionals perform a variety of technical services to (1) assist with internal personnel issues and other corporate matters, (2) support civil and criminal litigation and investigations, and (3) assist individuals with personal computers and systems. Services provided include:

- Creation of identical images of computer hard drives and other data storage devices.
- Keyword searches of data to identify and locate potentially relevant data.
- Analysis of system files and other artifacts to reconstruct past activities on a computer or other device.
- Production of expert reports with explanations, opinions, and conclusions regarding the analysis.
- Expert testimony at depositions or trials regarding the system and/or data examined, findings, etc.[11]

---

[8] Terry Wright Letter at 6-8.

[9] Letter to North Carolina Private Protection Services Board from Sgt. Gary Hinnant, Cyber Crimes Unit, Computer Forensics Lab, Detective Division, Raleigh Police Department.

[10] Letter to North Carolina Private Protective Services Board from Susan McMinn, High Technology Crime Investigation Association, Apr. 16, 2008.

[11] Letter to Terry Wright, Director, North Carolina Private Protective Services, State of North Carolina, Apr. 14, 2008, from Art Bowker, president, High Technology Crime Investigation Association; Michael W. Finnie, Instructor, Computer Forensics Program, University of Washington; Toby M. Finnie, Director, High Tech Crime Consortium; Steven P. Hailey, Instructor, Information Security & Digital Forensics, Chair, Digital Forensics Committee, Edmonds Community College; Gary C. Kessler, Associate Prof., Computer & Digital Forensics, Director, Champlain College Center for Digital Investigation, Champlain College; Dave Kleiman, Palm Beach Gardens, FL; Rob Lee, Forensics Faculty Fellow, The SANS Institute; Joleyn

- Penetration testing to test firewalls, intrusion detection systems, and controls.

Computer forensic specialists are called in when a company suspects an employee of wrongdoing (such as accessing pornography or child pornography), or believes that intellectual property has been stolen or that confidential data has been accessed, used or disclosed without authorization. They are engaged when computer viruses, worms, bots, or other malware infect a system and disrupt its operation, or when digital evidence needs to be gathered from various computer hard drives and storage areas for purposes of litigation. Digital forensic experts are also used when there is a need to prove that a misplaced or recovered laptop has not been accessed or that data has not been removed from a computer. Additionally, computer forensic professionals are employed to copy data from one drive to another, find data that has been deleted, analyze logs, track and trace communications, and determine authenticity or confidentiality of data. In sum, computer forensic experts are used by clients ranging from individuals trying to keep their laptops running and by large and small businesses. Increasingly, they are called to offer expert testimony in court.

Digital Forensics is a Science

Digital forensics is a rapidly changing, complex field not readily amenable to regulation by state licensing requirements. It has been accepted as a general principle by countries around the globe that laws and regulations should be technology neutral, lest they become "hardwired" with antiquated technology requirements.

Digital forensics is a science recognized as a separate forensic discipline, but detailed definitions vary. The *Shorter Oxford English Dictionary* defines forensic science as:

> The recognition, collection, identification, individualization, and interpretation of physical evidence, and the application of science and medicine for criminal and civil law, or regulatory purposes.[12]

Forensic science is applied in law enforcement investigations, business operations, the computer and network security industries, and educational programs. Each of these areas has its own notion of what computer forensics means. An April 14, 2008, letter to North Carolina's Private Protection Services Board from a group of computer forensic organizations and respected professionals succinctly sets forth the various definitions of computer forensics:

> **Information Security Industry**: Computer forensics, also called cyberforensics, is the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it. . . . Computer

---

Smithing, International Society of Forensic Computer Examiners; Doug White, Director, FANS Laboratory, Security Assistance Studies, Roger Williams University (hereinafter "Terry Wright Letter").

[12] *Shorter Oxford English Dictionary*, Fifth Ed., 2002, Oxford Univ. Press, Inc., New York.

forensics has become its own area of scientific expertise, with accompanying coursework and certification. [*citing Information Security Magazine*, Feb. 23, 2007]

Business Technology: In order to identify attacks, "network forensics" deals with the capture and inspection of packets passing through a selected node in the network. Packets can be inspected on the fly or stored on disk for later analysis. [*citing* "ZDNet Definition for: Computer Forensics"]

Digital Forensics Service Provider: Computer Forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to analysis or explanation of technical features of data and computer usage. Computer Forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel. [*citing Cyber Forensic Group]*

Network Security Industry: The science of indentifying, collecting, preserving, documenting, examining, analyzing and presenting evidence from computers, networks and other electronic devices. [*citing Technical Working Group for Education and Training in Digital Forensics,* West Virginia University Forensic Science Initiative document #219380, Aug. 2007]

Academic Course Description: To provide a definition, computer forensics is the use of procedure-centric approaches to the study of cyber-attack prevention, planning, detection, and response with the goals of counteracting and conquering hacker attacks by logging malicious activity and gathering court-admissible chains-of-evidence using various forensic tools that reconstruct criminally liable actions at the physical and logical levels. [*citing* Gurdeep S. Hura, *CSDP 698: Computer and Network Forensics*, University of Maryland Eastern Shore: Course Description]

E-Mag Article: By definition, computer forensics is the investigation of computer hard drives and other storage media to examine and analyze current, deleted, or "hidden" information that may serve as evidence in a criminal matter. Some of today's crimes solved through the help of computer forensics are copyright infringement, industrial espionage, money laundering, piracy, sexual harassment, theft of intellectual property, unauthorized access to confidential information, blackmail, corruption, decryption, destruction of information fraud, illegal duplication of software, unauthorized use of a computer, child pornography, drug dealing, and

even murder. [*citing* Maryellen Cicione, *CSI Cyberspace: Police Turn to Computer Forensics to Solve Crimes,* ComputerEdge Online].[13]

Computer Forensics Education and Certification

This rapidly changing field is continually developing professional qualification programs that provide a neutral accreditation of an individual's skills.

More than 50 universities, colleges, and professional organizations offer excellent training and education in the areas of computer forensics that can serve as qualifications of forensic expertise.[14] The National Security Agency ("NSA") has 85 National Centers of Academic Excellence in Information Assurance Education ("CAEIAE") and CAE-Research ("CAE-R"). Under the CAEIAE program, 4-year colleges and graduate-level universities are eligible to apply for designation as a CAEIAE. Institutions meeting the Carnegie Foundation's classifications of Research University/Very High, Research University/High, and Doctoral Research University are eligible to apply for CAE-R standing. Each application undergoes a lengthy and rigorous review process and must reapply every five years to retain its CAEIAE designation. Graduates from CAEIAEs and CAE-Rs are eligible to apply for grants and scholarships from the U.S. Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. The Information Assurance Directorate of the NSA also sponsors the Colloquium for Information Systems Security Education and the Senior Executive Liaison programs to help promote and increase the availability of information assurance education.[15]

Law enforcement organizations also sponsor or provide courses in many areas of computer forensics. For example, the National White Collar Crime Center, a congressionally-funded non-profit corporation, offers a full array of courses, including identifying and seizing electronic evidence, basic and intermediate data recovery and acquisition courses, introduction to automated forensic tools, securing law enforcement networks, and financial records examination and analysis.[16] The National Consortium for Justice Information and Statistics offers courses on the investigation of computer and Internet crime, the seizure and examination of computers, the investigation of online child exploitation, advanced response to the search and seizure of networks, and the investigation of cellular phones.[17] Other organizations offering specialized training include the Law Enforcement and Emergency Services Video Association[18] and the National Technical Investigators' Association.[19]

---

[13] Terry Wright Letter.
[14] Terry Wright Letter, Appendices at 6-10.
[15] "Centers of Academic Excellence," National Security Agency, Central Security Service, http://www.nsa.gov/ia/academia/caeiae.cfm?MenuID=10.1.1.2.
[16] See National White Collar Crime Center, http://www.nw3c.org/ocr/courses_desc.cfm.
[17] National Consortium for Justice Information and Statistics, http://www.search.org/programs/hightech/courses.asp.
[18] Law Enforcement and Emergency Services Video Assoc., http://www.leva.org/.
[19] National Technical Investigators' Association, http://www.natia.org/.

301

In addition to educational programs, several professional certifications are offered in the field of computer forensics that are widely recognized as indicators of competence, knowledge, and skill. These include[20]:

ACE™	Certification	Offered by Access Data
CAP	Certification	Certification and Accreditation Professional; certification offered by (ISC)2 for individuals who are involved in the process of certifying and accrediting the security of information systems
CCCI-Basic and Advanced	Certification	Certified Computer Crime Investigator; offered by HTCN; based on number years experience, number hours of training and narratives from specified number of cases.
CCE	Certification	Certified Computer Examiner; offered by ISFC
CCFT – Basic and Advanced	Certification	Certified Computer Forensic Technician, Basic and Advanced; offered by HTCN; based on number of years experience, number of hours training, narratives; (for Advanced) number of cases as lead investigator, total cases.
CFE	Certification	Certified Fraud Examiner, offered by Association of Certified Fraud Examiners (not computer-specific); see www.ACFE.org.
CHFI	Certification	Computer Hacking Forensic Investigator; Offered by EC-Council; 5-day class; examination. CEH suggested as prerequisite.
CIFI	Certification	Certified International Information Systems Forensic Investigator; offered by IIFSA.
CISA	Certification	Certified Information Systems Auditor; offered by ISACA; for information systems audit, control and security professionals.
CISM	Certification	Certified Information Security Manger; offered by ISACA
CISSP	Certification	Certified Information Systems Security Professional certification. Offered by $(ISC)^2$.
CSFA	Certification	Cybersecurity Forensic Analyst http://www.cybersecurityforensicanalyst.com/
CSICI	Certification	CyberSecurity Institute Certified Instructor; offered by CyberSecurity Institute.
CWSP	Certification	Certified Wireless Security Professional; offered by CWNP
EnCE	Certification	Encase Certified Examiner. Offered by Guidance Software. Requires 60 hours of courses or 1 year experience, plus passing written and practical examinations.
GCFA	Certification	Certified Forensic Analyst; for individuals responsible for forensic investigation, analysis, advanced incident handing or formal incident investigation; offered by GIAC; 4-year renewals.

[20] This table is inserted with permission from signatories of the Terry Wright Letter, Terry Wright Letter at 4-5.

CEIC	Conference	Computer and Enterprise Investigations Conference; see http://www.ceicconference.com; offered for Corporate IT, Legal, Government and Enforcement professionals.
CEECS	Course & Certification	Certified Electronic Evidence Collection Specialist. One day course or offered as part of two-week CFCE course by IACIS. For law enforcement only.
CFCE	Course & Certification	Certified Forensic Computer Examiner Certification. Granted by IACIS for applicants who either complete a two-week course followed by successful completion of correspondence proficiency problems or by passing examination. For law enforcement only. Requires recertification every three years and payment of dues.
CEH	Course and Certification	Certified Ethical Hacker. Course material offered by Specialized Solutions (see ceh.SpecializedSolutions.com); exam offered by EC-Council.
CFIA	Course and Certification	Certified Forensic Investigation Analyst, offered by 7Safe.
CSA	Course and Certification	Certified Security Analyst. 2-day workshop provides both ECSA and LPT
CSFA	Course and Certification	CyberSecurity Forensic Analyst; offered by CyberSecurity Institute; requires FBI background check, experience and testing.
CSTA	Course and Certification	Certified Security Testing Associate; offered by 7safe.
CSTP	Course and Certification	Certified Security Testing Professional; offered by 7safe.
ECSA	Course and Certification	EC-Council Certified Security Analyst; offered by EC-Council; 5-day course followed by exam.
LEVA	Course and Certification	LEVA Forensic Video Analyst Certification. LEVA Forensic Video Analysis Certification requires applicants to have completed 120 hours core courses "Basic, Intermediate & Advanced Forensic Video Analysis & the Law," 88 hours of approved imaging training, 40 hours of courtroom training, 32 hours in specific elective specialized training (total: 280 hours). At the time of application, candidates must have at least two years of experience as a Forensic Video Analyst. Candidates must also have either: a Bachelor's Degree or higher, or an Associate Degree with a minimum of 60 semester hours and at least three years of experience as a Forensic Video Analyst; or four years of experience as a Forensic Video Analyst. Applicants must also provide endorsement letters from a law enforcement agency and from a current LEVA member. Applicants must also successfully complete a "boarding interview" in front of the LEVA Certification Committee during which they must defend a written examination report on an actual case. (see http://www.leva.org/pdf/CertificationReq-v3.pdf).
LPT	Course and	Licensed Penetration Tester. Offered by EC-Council. Usually

301

	Certification	taken after CEH and CHFI.
SEC	Course and Certification	SubRosaSoft Examiner Certificate. http://www.macforensicslab.com/ Offered by SubRosaSoft.com Inc. http://www.subrosasoft.com/
SCERS	Training	Seized Computer Evidence Recovery Specialist, offered by FLETC.

Educational and certification courses in the area of computer forensics are continually evolving to keep pace with new threats, innovations in technology, and vulnerabilities in hardware and software. The marketplace is very competitive in this area and the security community is small enough that market forces work effectively to drive cyber security students and professionals to the courses with accurate and current content and certifications with industry recognition.

State licensing requirements for private investigators are not appropriate for digital forensics.

The U.S. Department of Labor (DOL) Bureau of Labor Statistics reports that most private investigators have some college education and previous experience in investigative work.[21] Most states require private investigators to be licensed by a state regulatory body, but the DOL notes that, "There are no formal education requirements for most private investigator jobs."[22] At least one state, California, requires private investigators to have a combination of an education in political science, criminal law, or justice and experience equaling three years (6,000 hours),[23] but there are no requirements for forensic education or experience.

The Texas licensing law is very broad and specifically applies to computer forensics. All investigation companies must have a license in Texas. The company must be managed by an individual who (1) holds a criminal justice degree or has completed a three-year apprenticeship under a licensed private investigator, *and* (2) has had two consecutive years of "legally acceptable" experience "in the guard company business."[24] The DOL, however, has determined that a computer science or accounting degree is more helpful in computer forensic work than a criminal justice degree.[25] *Thus, even one of the strictest state government's educational requirements for private investigator licensing does not include the training that helps ensure computer forensic investigators are competent.*

To obtain a private security consultant license in Texas as an employee (sole proprietors are still considered a company and must obtain a company license), there

---

[21] "Private Detectives and Investigators," "Training, Other Qualifications, and Advancement," U.S. Dept. of Labor, Bureau of Labor Statistics at 3, http://www.bls.gov/oco/ocos157.htm (hereinafter "DOL").
[22] *Id.*
[23] *Id.* at 4.
[24] "Company License Application Instructions and General Requirements for Licensing," Texas Dept. of Public Safety, Private Security Bureau, PSB-27, Rev. 11/07 at 2.
[25] *Id.*

are no educational requirements other than passing the general examination set by the PSB.[26] Computer forensic employees need a Private Security Consultant license. It is doubtful that the examination materials cover this area in any substantive manner, as there are only 200-some questions on the exam. The study questions offered on the PSB website are quite pedestrian and do not delve into computer forensics.[27]

Thus, a company offering forensic services or other services within the broad reach of the law can hire a manager with a criminal justice degree who has two years experience as a guard and has passed the state examination. The company can then hire any individual who passes the general test and assign them to perform computer forensic services. Texas state licensing requirements are not based upon a demonstration of qualifications, experience, skill, or education. Rather, the licensing process just screens individuals to ensure that they do not have addictions, arrest records, dishonorable discharges, are mentally incompetent, or criminals. Thus, licensing laws like the one enacted in Texas do not protect consumers, companies, or the computer forensic profession. In fact, such laws may do a disservice because they may give consumers, corporations, and other members of the public and business community a false assurance that a licensed private investigator is qualified to do computer forensic work.

Tying computer forensic qualifications to a private investigator license is thus inappropriate. Private investigator licenses can be renewed upon payment of fees, whereas forensic education never stops, as noted in the discussion above of certification and education programs. . The Department Labor has a more realistic perspective on computer forensic qualifications:

> "Either of these two degrees [computer science or accounting] provides a good starting point after which investigative techniques can be learned on the job. Alternatively, many colleges and universities now offer bachelor's or master's degrees in computer forensics, and others are planning to begin offering such degrees. . . . Because they work with changing technologies, computer forensic investigators never stop training. They learn the latest methods of fraud detection and new software programs and operating systems by attending conferences and courses offered by software vendors and professional associations.[28]

Resolution Protects Discretion of Trial Judge

State PI licensing is not necessary to ensure the quality of courtroom evidence; in fact, it interferes with the discretion afforded trial judges through the rules of evidence to determine if expert testimony is useful, relevant, and reliable.

---

[26] 35.75 Private Security Consultant, Texas Dept. of Public Safety, http://www.txdps.state.tx.us/psb/consultant.aspx.

[27] See, e.g., "Testing / Training Information, Texas Dept. of Public Safety, Private Security Bureau, http://www.txdps.state.tx.us/psb/testing/default.aspx.

[28] Id.

301

Judges already have adequate authority to monitor the quality of technical evidence admitted in court. The Resolution is consistent with Rule 702 of the Federal Rules of Evidence that expert testimony may be substantiated through a variety of means, including knowledge, skill, experience, training or education:

> If scientific, technical, or other specialized knowledge will assist the trier of fact . . . a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise.[29]

The Resolution is also aligned with the Supreme Court's holding In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), that the trial judge must determine whether expert testimony offered in federal courts is relevant and reliable. The Court rejected the view that scientific evidence could be admissible only if the scientific principle upon which it is based is "generally accepted" as reliable in the relevant scientific community. The Court noted that, "The subject of an expert's testimony must be 'scientific knowledge:'"

> The adjective 'scientific' implies a grounding in the methods and procedures of science. Similarly the word "knowledge" connotes more than subjective belief or unsupported speculation. The term "applies to any body of known facts or to any body of ideas inferred from such facts or accepted as truths on good grounds" . . . . But in order to qualify as "scientific knowledge," an inference or assertion must be derived by the scientific method. Proposed testimony must be supported by appropriate validation – i.e., "good grounds," based on what is known. In short, the requirement that an expert's testimony pertain to "scientific knowledge" establishes a standard of evidentiary reliability.[30]

The Court noted that "an expert is permitted wide latitude to offer opinions, including those that are not based on first hand knowledge or observation," but concluded that the trial court must determine if the offered expert testimony is scientific knowledge that will assist the trier of fact. Factors that may help guide a court in assessing expert testimony are (1) whether the theory or method can be or has been tested, (2) whether it has undergone peer review or publication, (3) the known or potential rate of error associated with the technique or theory, (4) the existence and maintenance of standards and controls, and (5) whether the theory or technique has been generally accepted by the scientific community.[31]

In *Kumho Tire Co. Ltd. v. Carmichael,* 526 U.S. 137 (1999), the Court clarified that its holding in *Daubert* applied to all expert testimony, not just scientific testimony.

---

[29] *Federal Rules of Evidence,* Rule 702, http://www.law.cornell.edu/rules/fre/.
[30] *Id.*
[31] *Id.; see also* "Notes to Rule 702," *Federal Rules of Evidence,* p. 3, http://www.law.cornell.edu/rules/fre/ACRule702.htm.

Many state evidentiary rules regarding expert testimony track the federal rules. Therefore, the Resolution, by opposing an additional layer of state licensing requirements, may help protect the discretion of the trial court to determine if expert testimony is relevant, useful, and reliable. In a recent Arizona opinion, the appellate court held that Arizona statute section 12-2604(A) governing qualifications for expert witnesses providing expert testimony was unconstitutional because it violated the doctrine of separation of powers since it was in direct conflict with Rule 702 of the Arizona Rules of Evidence. Section 12-2604(A) set stricter limits on the medical experts than Rule 702.[32] State license laws for expert testimony also may be vulnerable under this doctrine.

State Licensing Requirements Create Jurisdictional Issues

Computer forensic assignments often require handling data in multiple jurisdictions. For example, data may need to imaged from hard drives in New York, Texas, and Michigan. Does the person performing that work need to have licenses in all three states? Will expert testimony potentially be barred if the person performing the work is not licensed where the work was performed or where the testimony is given? What if the forensic expert who performed the work is called to testify in trial in South Carolina but is not licensed there? In 1991, Arizona's attorney general was asked by a society of professional engineers if they had to be licensed as private investigators because they were offering forensic engineering testimony in court. The attorney general responded that they did not, citing *Kennard v. Rosenberg,* 127 Cal. App. 2d 340, 273 P.2d 839 (1954).[33]

Summary

This Resolution will accomplish five major objectives.

First, it clearly states that computer forensics is a complex science whose role in the legal system requires careful deliberation, especially with respect to qualifications, expert testimony, and the need to involve forensic personnel in e-discovery.

Second, it will help ensure that litigants, the courts, and the public benefit from the science of computer forensics through qualified experts whose credentials are based on knowledge, experience, skills, education, and training.

Third, it will help protect consumers and businesses from misperceptions that licensed private investigators are automatically qualified computer forensic experts.

Fourth, it discourages an unnecessary level of regulation regarding expert testimony beyond the existing discretion of the trial judge, and it is in alignment with rules of evidence on expert testimony.

---

[32] *Seisinger v. Siebel*, 1 CA-CV 07-0266, (Ariz. App. 6/17/08) at 1-2.
[33] Rasch at 3-4.

301

Fifth, it help prevent unnecessary jurisdictional issues that could occur as a result of a patchwork of state licensing requirements, especially with respect to for computer forensic expert testimony.

Swift action by the ABA on this matter will make a significant contribution to this debate and will most certainly cause legislators and regulators to pause and carefully consider actions in this area. It is much easier to pass good laws than to remove or change enacted ones.

Respectfully submitted,

Gilbert Whittemore, Esq.
Chair, Section of Science & Technology Law

GENERAL INFORMATION FORM

Submitting Entity: Section of Science & Technology Law

Submitted By: Gilbert F. Whittemore, Chair
Section of Science & Technology Law

1. Summary of Recommendation(s).

The Recommendation urges that State, local, and territorial legislatures and regulatory bodies refrain from requiring private investigator licenses for persons engaged in computer or digital forensic work, including expert testimony; and supports the development of certification and competency requirements for such forensic activities.

2. Approval by Submitting Entity.

Approved by the Council of the Section of Science & Technology Law on July 16, 2008.

3. Has this or a similar recommendation been submitted to the House or Board previously?

Not to our knowledge.

4. What existing Association policies are relevant to this recommendation and how would they be affected by its adoption?

None specifically that we are aware of. Generally, the ABA has adopted resolutions supporting legal standards to assure the authenticity and integrity of information in electronic form, principles relating to science and technology in judicial decision making, and Uniform Rules of Evidence including expert testimony.

301

5. What urgency exists which requires action at this meeting of the House?

Several states have taken action in the past year to require private investigator licenses for computer forensic work or expert testimony with little or no justification. As discussed in the report, this approach does not assure that qualified persons are performing the work, with potential adverse impact on the reliability of the evidence, quality of the forensic investigations and network testing, and e-discovery. Legislative sessions upcoming in the fall, prior to the ABA Midyear Meeting, could result in additional such legislative actions, and the ABA should be ready to comment on proposals for private investigator licenses and the preferred alternatives of certification or competency requirements.

6. Status of Legislation. (If applicable.)

Legislative efforts are underway at the state level, as discussed in the report.

7. Cost to the Association. (Both direct and indirect costs.)

None

8. Disclosure of Interest. (If applicable.)

Some members of the sponsoring Section work in the computer forensic field, provide expert testimony, and hire forensic experts. All attorneys that litigate or are involved with e-discovery potentially have the need to use computer forensic experts. To our knowledge, no member of the sponsoring Section has been involved in any of the legislative efforts in the various States.

9. Referrals.

This report is being referred to all ABA Sections, Divisions, and Forum Committees as well state and local bar associations for co-sponsorship.

10. Contact Person. (Prior to the meeting.)

Ellen J. Flannery
Covington & Burling LLP
1201 Pennsylvania Avenue, NW
Washington DC 20004
Phone: 202-662-5484
eflannery@cov.com

11. Contact Person. (Who will present the report to the House.)

Ellen J. Flannery
Covington & Burling LLP
1201 Pennsylvania Avenue, NW
Washington DC 20004
Phone: 202-662-5484
eflannery@cov.com

Bonnie E. Fought
Emerquest
Ste 112
1155 Chess Dr
Foster City, CA 94404-1118
Phone: 650- 218-6248
Cell: 650- 218-6248
aba@garber-fought.net

301

EXECUTIVE SUMMARY

1. Summary of the Recommendation

The Recommendation urges that State, local, and territorial legislatures and regulatory bodies refrain from requiring private investigator licenses for persons engaged in computer or digital forensic work, including expert testimony.

2. Summary of the Issue Which the Recommendation Addresses

The subject of the recommendation is state statutory and/or regulatory requirements that computer forensic professionals must be licensed private investigators.

3. How the Proposed Policy Will Address this Issue

The proposed policy will discourage State, local, and territorial legislatures and regulatory entities from enacting such licensing requirements and the proposed policy supports efforts to establish professional certification or competency requirements based upon the current state of technology or science.

4. Summary of Minority Views or Opposition

None that we are aware of.