LICENSING DIGITAL FORENSIC PRACTITIONERS AS PRIVATE INVESTIGATORS
THE RISK TO JUSTICE, THE PUBLIC, AND CONSUMERS

Executive Summary

Several state legislatures have considered licensing digital forensic practitioners as private investigators without regard to their professional credentials in the field of digital forensics. Improper licensing initiatives of this type pose a significant risk to justice, the public, and consumers.

The intention of this paper is to provide the reader with critical information about the field of digital forensics and highlight its stark contrast to the field of private investigation. The paper will also provide an overview of CDFS, its efforts to date on standardizing the profession of digital forensics and its recommendations to regulatory and legislative entities regarding any regulation of digital forensic professionals under a PI license.

Licensing Digital Forensic Practitioners as Private Investigators

In 2008, the American Academy of Forensic Sciences (AAFS) recognized digital forensics as a unique section of their organization, categorized as Digital & Multimedia Science. This was the first new category of forensic science to be added by the American Academy of Forensic Science in 28 years.[1] Per the AAFS website, "The American Academy of Forensic Sciences (AAFS) is a multi-disciplinary professional organization established to provide leadership to advance science and its application to the legal system. The AAFS aims to promote integrity, competency, education, foster research, improve practice, and encourage collaboration in the forensic sciences." Other sciences represented under the AAFS include Odontology, Pathology/Biology, Physical Anthropology and Psychiatry/Behavioral Science.

This recognition solidifies digital forensics as a science and indicates the profession should be considered unique with regard to standardization and regulation. Professionals wishing to pursue a career in the science of digital forensics must be competent, experienced and prepared to act as and substantiate opinion given as an expert, whether an expert witness or an expert hired to acquire and analyze digital information in whatever state it is encountered. Digital analysis 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. Other forensic disciplines identified by the AAFS are not held to a PI license requirement. Digital forensics should not be singled out as a scientific discipline requiring private investigator licensing.

---

[1] American Academy of Forensic Scientists <http://www.aafs.org/default.asp?section_id=resources&page_id=choosing_a_career#Kinds%20of%20FS> Accessed March 2008. Also see Erika Morphy, *Computer Forensics: Beyond the Magnifying Glass,* 29 July 2008 < http://www.technewsworld.com/story/63972.html>.

The American Bar Association (ABA) has issued a Resolution urging state legislatures to avoid improper licensing of digital forensic practitioners as private investigators, in part to protect consumers and the interests of justice. Pertinent portions of ABA Resolution 301 are below.

> "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…"[2]

The ABA believes there are remedies already in place to deal with unprofessional forensic examiners and the proper place to address such matters is the courtroom.

In addition, the Scientific Working Group on Digital Evidence (SWGDE) and the Scientific Working Group on Imaging Technology (SWGIT), both non-profit organizations sponsored by the National Institute of Justice, support the ABA resolution and together wrote a joint document opposing PI requirements for computer forensic examiners and other digital evidence practitioners.

Bruce H. Hulme, legislative director for the National Council of Investigation and Security Services, reported his impressions of presentations given at the November 2008 annual conference of the International Association of Security and Investigative Regulators (IASIR):

> "ABA representative Jody Westby, chair of the ABA Committee on Privacy and Computer Crime, along with two other presenters made a compelling argument against state licensing of such experts under state PI statutes. They were very articulate, well prepared, and quite savvy on state PI laws and seem to have the lobbying where-with-all to make their case against state licensing of "digital" forensic experts as PIs. ...My gut reaction and first impression is that the ABA will be able to prevail in their arguments against state regulation of such forensic experts should they press the issue, which I believe they will in time. I also got the impression that the state regulators present would agree by and large with the ABA's position in the end." [3]

The Practice of Digital Forensics

The science and practice of digital forensics involves the acquisition, preservation, identification and analysis of data that has been electronically processed and stored on computing media.

---

[2] American Bar Association (2008) *Resolution 301.* Section of Science & Technology Law Report to The House Of Delegates. Page 1. Retrieved on August 15, 2008 from http://www.abanet.org/leadership/2008/annual/recommendations/ThreeHundredOne.doc

[3] Hulme, Bruce H. (2008) *The American Bar Association's Resolution 301: The ABA Opposes Regulation of Computer or Digital Forensics Experts by PI Licensing Authorities.* The National Voice of the Private Investigation and Security Professions Report. Winter 2008-2009. (National Council of Investigation and Security Services) Retrieved April 18, 2009 from <http://www.nciss.org/Newsletter/NCISS_Report/TheReport.Winter2008-2009.Web.pdf>

Significant numbers of digital forensic practitioners are retained by attorneys, or appointed by the courts to serve as technical consultants who opine on analytical findings. Courts structure the actions of digital forensic professionals in a way that affords protection of the rights of all parties with respect to privacy, chain of custody, disclosure, prevention of spoliation of digital data, etc. Professional digital forensic practitioners do not gain involuntary access to computers or other digital devices.

Digital forensic specialists typically:

- Create identical or "mirror images" of data stored on digital media.
- Conduct keyword searches of the data in attempt to identify files with potentially relevant content.
- Analyze low level system files and other digital artifacts to reconstruct and substantiate past activities on computers or other devices.
- Produce reports to explain and validate the findings of the analysis.
- Testify as a Digital & Multimedia Science expert at deposition or trial concerning the forensic examination, findings and validation.

The science of digital forensics is applied in myriad disciplines and settings. Police may examine digital evidence to confirm criminal activity. Businesses may examine digital evidence to identify instances of network intrusion, theft of intellectual property, or trademark violation. Scientific or academic institutions might examine digital evidence to authenticate research data and findings or to determine abuse of computing systems.

Distinguishing Digital Forensics from Private Investigation

An opinion published in *Wisconsin Regulatory Digest*: *A Publication of the Department of Regulation and Licensing for Private Detectives and Private Detective Agencies (*and excerpted below in its entirety) distinguishes the activities of a private investigator from those of a digital forensic specialist:

> **"<u>Computer Forensic Companies</u>**
>
> The following letter was prepared by Legal Counsel, William Black, in response to an inquiry:
>
> You have asked whether a computer forensic company of the type described below falls within the regulatory scheme of s. 440.26 Stats. It is my opinion that it does not. Its activities either fall outside of the traditional definition of private detective work, or would qualify as exempt under RL 30.02(12)(b)10.
>
> <u>FACT SCENARIO</u> The following five factor background is presented:

Turnkey Network Security Solutions Assist third parties recovering hidden, deleted, encrypted, and/or damaged data; litigation support; expert witness testimony.

Electronic Discovery Civil litigation forensic services - restore or recover from a wide variety of systems. Consultants help to preserve and collect evidence.

Forensic Analysis Gather data. Employ techniques to find deleted, hidden or forgotten evidence. Work performed on site or at lab. Consultants piece together an event or chain of events by restoring deleted or password-protected files. Tracking patterns of individuals or groups through evidence left on electronic calendars, e-mail, and data files, pull together a detailed picture of fraud, sabotage, theft, espionage and other destructive acts.

Electronic Search & Seizure Assistance in pre-search warrant preparations and post-seizure handling of the computer equipment. Maintaining control over the proper seizure and subsequent evidence gathered. Assistance in drafting interrogatories. What devices should be requested in a subpoena. Procedures in maintaining a verifiable chain of evidence. Maintenance and proper protection of electronic evidence. Evaluate electronic evidence.

Consultants Be able to account for the complete chain of evidence. Know the legal requirements for admissible expert witness testimony.

OPINION What constitutes private detective work can be elusive to define given that the statute and rules contemplate a private detective calling himself or herself as such, thus falling within the statute, or doing specific acts generally considered within the scope of private detective work. Often, an expert will perform an investigation and analysis of evidence. From this expert's work product an opinion regarding a factual or legal issue will often be formed and presented at trial. However, this expert will not be deemed a private detective for purposes of the statute.

The extent and scope of an investigation and the license requirements necessary to undertake such an investigation arises in different contexts often involving expert witnesses and consultants. Rule RL30.02(12)(b)10 contemplates that certain scientific researchers, laboratory personnel and expert consultants are not included under the definition of private detective. Although case law is sparse concerning the definition of the term "private detective", rule RL30.02(12)(b)10 codifies certain principles regarding a workable definition by exception. A definition is also proposed to outline the characteristics of private detective work in 76 Op. Att'y Gen. 35 (1987) (Opining that fire investigators may be hired and conduct their specialty without regard to licensure under the private detective law.)

Private detectives have three principal characteristics:

1. They are an unofficial person, not an employee of a governmental agency.
2. They are engaged in obtaining information in secret, in that it is without the knowledge of the person being observed.

3. The information is obtained and transmitted to a third party. 37 OAG 469, 470 (1948). 53 OAG 183, 185 (1964)

The openness of observation of a person removes the element of secrecy and thus no private detective license is necessary. 37 OAG 542 (1948) (persons being observed are told of the observation, and it is done in their presence.) Observations of persons in secret naturally also include gathering information about a person from information sources in secret. This extra dimension of the definition appears to be impliedly assumed as it plays such a major part in any detective work. Therefore, within the context of this discussion it is assumed that the term "observations of a person in secret" includes visual observation and informational data gathering, as these are the two major facets of private detective work.

Using the reasoning either that no person is being observed in secret, or that the exception of RL 30.02(12)(b)10 applies, the activities described in the FACT SCENARIO do not constitute work for which a private detective license is needed. Indeed, RL 30.02(12)(b)10 impliedly codifies nothing more than the acknowledgement that the types of activities listed therein do not involve "observations of persons in secret" and thus don't qualify as private detective activities needing licensure.

In the area of a specialty or expertise the concept of "observations of persons in secret" loses meaning since the expert is consulting in or observing or testing a tangible physical object to discover facts about the object itself.

The distinction is critical because once a fact is discovered pertaining to an object, that fact may or may not be connected to a person. The nature and quality of the fact observed relating to the tangible physical object may directly connect to a person or may need additional facts or inferences to do so. However, it was the fact pertaining to the tangible physical object itself that was observed, not the person.

This special role of the expert, or forensic specialist is noted thusly, "…no expert witnesses, whether they be arson experts or any of hundreds of other types of experts, are required to be licensed as private detectives under section [440.26], merely because they may investigate matters relating to their fields of expertise". 76 OAG 35 (1987) In approving fire investigator investigations without licensure, the Attorney General drew from the similar analogies of pathologists (investigating a cause of death) or an accountant (investigating a corporate takeover or white-collar crime). Id. Because these are individualized fields of expertise such work is excluded from the requirement for licensure. Such work is also excluded because it does not fit the three-part definition provided consistently by the Attorney General in its opinions on this subject.

In a like manner, the computer forensic specialist is an area of expertise and technical practice not requiring licensure if practiced within the restraints of the FACT SCENARIO. The reason lies in recognizing what computer forensics is not. Computer forensics is not using a computer to merely perform investigations traditionally done with binoculars, or cameras, or to access information contained in other data banks or computer systems as part of an investigation. Computer forensics instead focuses on the computer itself as a tangible physical object to be observed. (Note- Tangible in this sense means anything capable of being observed, whether encoded electronically as with a computer, or genetically, chemically, or otherwise by a physical process.)

This is a critical distinction, that for the forensic computer expert the computer itself is the object of the investigation versus being used merely as an additional tool to obtain information in an investigation. In the former instance the computer forensic specialist is similar to a fire investigator who examines tangible physical objects to determine the cause of a fire, or the accountant who examines corporate books to determine evidence of white-collar crime. Similar to a DNA or fingerprint investigator, a computer forensic specialist employs laboratory research techniques and specialized analytical equipment to determine characteristics of a tangible physical object, i.e. a computer (and any processes that encode information) that may or may not lead to the discovery of evidence.

CAVEAT - The traditional use of the computer as an investigation tool to discover evidence and access data not germane to the computer itself is still certainly an activity for which a private detective license is necessary. The use of the computer as an investigative tool in this way does not qualitatively differ from traditional investigative techniques that observe a person (or information relating to them) in secret without their knowledge. Therefore if a computer forensic company were to offer services whereby they would access other data banks or computer systems to search for evidence or information as and for its own sake, this would satisfy the traditional definition of observing of a person in secret and licensure would be necessary. However, it must be strongly reinforced that this type of activity does not appear to be within the scope of the FACT SCENARIO.

Finally, any work performed in the context of litigation discovery using statutory authorized discovery mechanisms is certainly not information gathering or observation in secret and any consulting services related thereto would not need licensure.[4]

Critical Thoughts for Improper Licensing Initiatives

1. Digital Forensic Specialists are practitioners who, by their knowledge, skill, experience, training, or education, assist courts to understand digital evidence or to determine facts. Regulators should not single out digital forensic specialists to obtain private investigator licenses or instead should require that *all* forensic scientists be licensed.

2. Digital forensic specialists also serve in other professional capacities, for example: in litigation support, discovery services, information security, computer network security and video data analysis. These professionals are monitored by courts (as expert witnesses) or by businesses (as owners of the data).

3. Requiring digital forensic specialists to be licensed as private investigators may:

- Provide false assurance to courts, consumers, and those involved with the justice system that private investigators are qualified to do digital forensics based upon the license alone;

[4] Black, William. (1999). Computer Forensics. In *Wisconsin Regulatory Digest*: *A Publication of the Department of Regulation and Licensing for Private Detectives and Private Detective Agencies.* Volume 11, No. 2. (pages 3-5) Retrieved August 8, 2008 from <http://drl.wi.gov/boards/rfr/digest/19991100.pdf>

- Reduce effectiveness of law enforcement investigators who seek and rely on assistance from private sector digital forensic specialists;
- Create conflict and confusion with respect to the roles and responsibilities of digital forensic specialists and private investigators;
- Diminish citizens' access to justice;
- And unduly burden companies trying to protect their own assets and networks.

4. Unequal regulation by states requiring digital forensic specialists to obtain private investigator licenses will be costly and burdensome to litigants and may conflict with state and federal rules of evidence, including interfering with broad discretionary powers vested in the courts when vetting expert witnesses.

5. The cross-border nature of computing and telecommunications demands flexibility in digital evidence collection. State private investigator licensing statutes, on a whole, do not address problems with jurisdiction and reciprocity, and may impede the collection of digital evidence.

Other Concerns for Licensing Implementation

Good regulations should produce benefits that outweigh the costs of implementation. If a regulatory authority intends to regulate digital forensic specialists, it should establish qualifications for such individuals, and a licensing scheme that meets the needs of the profession.

The undertaking to regulate the work of a digital forensic professional is not insignificant. Digital forensic specialists are no longer tasked with simply recovering information from a standalone desktop hard drive seized from a crime scene. The profession has grown, and will continue to grow, concomitant with technological advancements in contemporary and emerging digital media such as desktop and laptop computers, tablets, net books, mobile phones, smart phones, mp3 players, gaming systems, cameras, closed-circuit television digital video recorders and other devices.

The task of writing standards to test and certify and therefore regulate professionals in any field is costly and does not guarantee the quality of work performed by those professionals. To plan for and coordinate a method to train, test and regulate scientific practitioners in a profession such as digital forensics would require Subject Matter Experts (SMEs) to write the testing methods and a psychometrician to ensure any testing methodology is sound. The requirements of a digital forensic professional have changed so rapidly over the past 5 years that it is not unreasonable to assume that any test crafted or standards set to certify these professionals would require at least annual revisions to stay valid and current. This projection is based on the work load that has been thoroughly assessed by the CDFS board members of whom include highly experienced professional practitioners in the digital forensic profession.

More important than cost is the effort and necessary expertise needed to define competencies. The challenge is to accurately identify requirements for a forensic science profession that advances so rapidly.

Digital forensic professionals must stay current with trends and developments in order to remain successful and competitive in their profession. Practitioners must continuously update their skill sets to assess, acquire and analyze digital evidence from dynamically changing media while staying current with software and hardware tools also undergoing frequent upgrades. As a consequence, standards developed to regulate digital forensic specialists must also stay apace with emerging technologies and developments that will shape any requirements or standards developed to regulate digital forensic professionals.

Standards Must be Driven by the Industry

Any regulation must come from an organization intimately familiar with the requirements of this profession and well prepared to revise and update these requirements as the digital forensics profession continues to grow and technology continues to advance. To date, efforts made have originated from individual states and have made it more difficult for digital forensic professionals to provide the public it serves the best service possible.

Many states have recently attempted to regulate digital forensic professionals through their PI licensing arm. Some states, when faced with the task of quantifying the training, education, and experience requirements for digital forensic professionals necessary to properly regulate these professionals have stalled their efforts and contacted digital forensic representatives to assist them in defining these requirements (NC) or enacted legislation specifically exempting digital forensic professions from the PI requirements (VA, RI).

In another case (MI), SMEs were contracted and tasked with researching and defining the training, education, and experience requirements necessary for individuals to hold in order to practice digital forensics in addition to a PI license. Subject matter experts concluded, however, that the newly codified requirements resulted in a very limited market of digital forensic professionals authorized to serve the state of Michigan, instead excluding many highly qualified, experienced practitioners who did not meet the PI side of the requirements.

The varied actions and results of individual states illustrate a severe lack of understanding of the requirements necessary to properly regulate digital forensic professionals. Additionally, action taken by individual states compounds the difficulty faced by these professionals by restricting their ability to follow their work across state lines without first addressing that state's specific licensing requirements. This highly compromises the service the public receives from the digital forensic professionals, since digital data is not confined within state borders and more often than not must be followed not only across state lines, but also across international boundaries. Regulation of digital forensic specialists must include local and international reciprocal agreements with other regulatory entities.

Only recently have leaders in the digital forensics profession become united to form the Consortium of Digital Forensic Specialists, an international, not-for-profit organization to lead the way in standardization and regulation of digital forensics. Formation of CDFS arose as a result of discussions with regulatory entities and legislators. Officially launched in August 2011, CDFS is lead by a board of directors comprised of industry leaders representing well-recognized training, certification and professional digital forensics associations. The primary objective of CDFS is to generate and maintain professional standards and guidelines for digital forensic professionals. To date the organization appears to be a

welcome addition to the digital forensic profession, as membership has flourished since its recent launch, attracting individual, academic, corporate, government and professional association memberships.

Until now there has not been a group or organization that represents the digital forensics profession as a whole. CDFS stands to unite the profession and draft and maintain standards up to date with the practice requirements, needs, technology and rapid pace of the digital forensics profession today. Standardization or regulation attempts from groups outside of the qualifications and experience of that of CDFS have been unsuccessful and in some cases detrimental to the level of service provided by digital forensic professionals and the public they serve.

Conclusion

As demonstrated above, the professions of private investigation and digital forensics are so dissimilar that it is illogical and counter-productive to contemplate cross-regulation. It is no more appropriate to comingle regulation of digital forensics with private investigation than to comingle the regulation of accountants and physicians.

Despite recent acceptance as a forensic science, digital forensic specialists are constantly working to define and improve standards, and to raise the level of professionalism within its ranks. Locking out qualified practitioners with requirements drafted without complete knowledge and experience of the science of digital forensics while granting tacit endorsement to private investigators with limited to no expertise in digital forensics, may have a chilling effect on the development of this needed profession.

States and regulatory authorities should not attempt to regulate digital forensics with the PI license. Proper digital forensic practices are a matter for courts, counsel, and practitioners.

For More Information

CDFS is always willing to discuss and research those issues impacting the practice of digital forensics. It is through proper research and debate that informed decisions on licensing and regulatory issues may be made. To learn more or reach CDFS, visit our website at www.cdfs.org.