

Digital Forensics and the PI Laws: What is happening, and what you can do to help!

Dave Kleiman

CAS, CCE, CIFI, CEECS, CISM, CISSP, ISSAP, ISSMP, MCSE, MVP

www.ComputerForensicExaminer.com

Acknowledgements

- Scott Moulton - <http://www.myharddrivedied.com> – took the first hit for us – really brought some focus to this issue - <http://serenity.nicservices.com/clientaccess/PISpeech>
- Jody Westby - <http://www.globalcyberrisk.com> – ABA Resolution 301 – Author
- Toby Finnie – admin@hightechcrimecops.org - Digital Forensic Specialists Council and LemonPI group – Instrumental in formulating groups and ideas
- Doug White – doug.white@acm.org - Professor - Roger Williams University – First successful PI exemption statute for DFE (RI) <http://www.rilin.state.ri.us/PublicLaws/Law08/law08111.htm> enacted June and I “borrowed” parts of his letter
- Gary Kessler - gary.kessler@champlain.edu – Professor - Champlain College – has exemption in legislation - and I “borrowed” parts of his letter too

Reactions from IASIR

- <http://www.iasir.org/>
- Doug Rehman - <http://www.electronicdiscovery.com>
-
- Jody Westby - <http://www.globalcyberrisk.com>
- Mark Pollitt- National Center for Forensic Science – <http://www.ncfs.org>
- There were 28+ States there. NC had the largest showing, so I imagine in January we will find out what they thought, since that NC bill is back on the table when their legislation goes back on, if they are not already back in session??

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.

AMERICAN BAR ASSOCIATION

- ADOPTED BY THE HOUSE OF DELEGATES
AUGUST 11-12, 2008
- 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.

Scott Moulton

They tried to remove me from the court and allowed my testimony. That was after they passed the felony in Georgia, before I helped get it vetoed. I was told if I had not gotten in Vetoed before July 1st when it went into effect that "someone" was going to arrest me for the felony if I was still practicing forensic on July 1st. So it was allowed that I testified even though "they claimed" it was a misdemeanor.

I was arrested for Portscanning in 2000 in a different case. I was working at a 911 center and portscanned the ISP for the Sheriff's office connected to the 911 center and the ISP called the GBI and had me arrested, and it cost me \$100 grand to defend

OPINIONS?

- Opinions people have expressed:
 - ..regulation is needed.. It gets rid of the rift raft that hangs out a sign
 - ..worst computer guy working on their case over a PI and generally believe the PI is not qualified.
 - ..this is a field of science and computer science does not belong under the PI wing.
 - ..But a lot more people just think it does not apply to them; Forensic Handwriting Experts, or Question Document Examiners.

Introduction to Digital Forensics and the PI Issue

- GA
- TX
- MI
- SC

RECENT EVENTS IN MICHIGAN

- Michigan passed the “Professional Investigator Licensure Act” on May 28th 2008.
- It makes it a felony to practice computer forensics without a license going into effect:

“This act is ordered to take immediate effect.”

- Penalty for the crime of computer forensics:
 - (3) A person violating this section is guilty of a felony punishable by imprisonment for not more than 4 years or by a penal fine of not more than \$5,000.00, or both.

Introduction to Digital Forensics and the PI Issue

PI license – The Reciprocity Disadvantage

Provisions of the Reciprocity Agreements

An investigator may conduct business outside his or her home state only under the circumstances indicated below.

- The investigation must be initiated in the investigator's home state.
- The investigator may spend no more than 30 days Per Case while conducting an investigation in another state. (Note the exceptions below!)
- The investigator is prohibited from soliciting business while in another state and from establishing a business or setting up residence while conducting an investigation in that state.

Introduction to Digital Forensics and the PI Issue

PI license – The Reciprocity Disadvantage

Provisions of the Reciprocity Agreements

An investigator may conduct business outside his or her home state only under the circumstances indicated below.

- The investigation must be initiated in the investigator's home state.
- The investigator may spend no more than 30 days Per Case while conducting an investigation in another state. (Note the exceptions below!)
- The investigator is prohibited from soliciting business while in another state and from establishing a business or setting up residence while conducting an investigation in that state.

Introduction to Digital Forensics and the PI Issue

List of Reciprocity States

The following states have mutually agreed to recognize the right of private investigators to conduct interstate business:

California

Georgia

Louisiana

North Carolina

Oklahoma

Tennessee*

Virginia

<http://licgweb.doacs.state.fl.us/investigations/reciprocity.html>

What you can do to help!!

- Be Proactive – Help yourself!!
- ACT FAST!!
- ACT FIRST!!

Introduction to Digital Forensics and the PI Issue

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 and bullets) and medical evidence (e.g., blood and DNA) are well accepted in courts as well as the hearts and minds of the public through such television shows as *CSI*, *Law & Order*, and *Forensic Files*.

Less well known -- and less well understood -- is the role of digital or computer forensic examinations in criminal and civil litigation. *Digital (or computer) forensics* is the acquisition, examination, and reporting of information found on computers, networks, and other digital devices (e.g., cell phones and PDAs) that pertain to a criminal, civil, corporate, other private sector incidents. Nearly everything that someone does on a computer or a network leaves traces - from deleted files and registry entries to the Internet history cache and automatic Microsoft Word backup files. E-mail headers and instant messaging logs give information as to the intermediate servers through which information has traversed. Server logs provide information about every computer system accessing a Web site.

Digital forensics is increasing in importance in both public and private sector investigations 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/or record-keeper of everyday activities, including those of a criminal nature and/or of interest to a civil investigation.

This importance can be noted in three distinct recent events in the Forensic Science community:

1. The recent release of American Bar Association resolution 301 on Computer Forensics adopted by the house of delegates August 11-12, 2008. (which can be downloaded and viewed at:
<http://www.abanet.org/leadership/2008/annual/adopted/ThreeHundredOne.doc>)
 - A. 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.

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>

B. 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.

2. The formation of the Digital Forensic Certification Board (DFCB) by the National Center for Forensic Science, a program of the U.S. Department of Justice, Office of Justice Programs National Institute of Justice hosted by the University of Central Florida (<http://www.ncfs.org/dfcb/> and <http://www.ojp.usdoj.gov/>).
3. The formation of the Digital and Multimedia Sciences (DMS) Section of the American Academy of Forensic Sciences (AAFS) on February 20, 2008. It has been 28 years since the last AAFS section was formed (https://www.aafs.org/content/aafs/sections/digital_multimedia.asp)

Additionally, it should be noted in 1980, George Firestone, Florida Secretary of State, issued a Declaratory Statement (DS 80-04) on the subject of private investigator licensing for scientific and technical investigations. The statement includes:

"The Department of State concurs that *Kennard v. Rosenberg*, is persuasive, and that when taken together with the previously cited Attorney General's Opinion (1967 Op. Att'y. Gen. Fla., 067-1) and Florida Supreme Court case (*Segal v. Simpson*, 121 So. 2d 790 (Fla. 1960), demonstrates that the intent of the Legislature in writing Chapter 493 was not to require every person conducting technical and scientific investigations into the causes of physical phenomena or events to first obtain a private investigator's license."

Competent digital forensics examinations must be conducted by a *Digital Forensics Specialist (DFS)*. A DFS means a person who holds a professional certification or degree, or who has training, education, and experience as a digital or computer forensic examiner in the seizure, preservation, examination, and analysis of media containing digital data. A digital forensic specialist may interpret, evaluate, test, or analyze pre-existing data from computers, computer systems, networks, or other digital media provided to them by another person who owns, controls, or possesses said computer, computer system, network, or other electronic media.

Private Investigators and Digital Forensics Specialists

Investigation is defined as "to observe or study by close examination and systematic inquiry; to make a systematic examination; especially: to conduct an official inquiry." Inquiry is defined as an "examination into facts or principles: a request for information. Private Investigator is defined as a person not a member of a police force who is licensed to do detective work (as investigation of suspected wrongdoing or searching for missing persons)"²

² Investigation and Inquiry, Merriam-Webster's Collegiate® Dictionary, Eleventh Edition and Webster's Third New International Dictionary, Unabridged. (MERIAM-WEBSTER ONLINE) Retrieved November 22, 2008, from <http://www.merriam-webster.com/dictionary/investigation>, <http://www.merriam-webster.com/dictionary/inquiry>, and <http://www.merriam-webster.com/dictionary/private%20investigator>

Digital Forensic Specialists provide these, as defined above, facts retrieved during the examination that an investigator, Law Enforcement (LE) or PI, may inquire into further. DFS examinations require examining media and reporting the findings. Similar to a Medical Examiner (ME), that may find a poison in the examination of deceased person. The ME does not go and investigate suspect's dwellings looking for the poison; they merely pass on the information found in their scientific process to LE. A DFS may assist a "Missing Persons" investigation through the forensic process, by finding recently deleted emails that when turned over to an investigator, may provide clues to help that investigator find the missing person. However, it is beyond the scope of examination to act on the found emails and go looking for the missing person.

A strict reading of the Florida Private Investigative Services (PI) statutes could be construed so as to include digital forensics specialists that work outside of the public sector.

There are a number of reasons that digital forensic specialists seek to be exempt from the PI statutes, but the overriding one is that a DFS and a PI have different roles, responsibilities, education, and training:

1. A DFS is a forensic scientist who, by his/her knowledge, skill, experience, training, and/or education, assists courts in understanding digital evidence and/or in determining facts based on digital evidence. If a DFS is required to obtain a private investigator license, then all forensic scientists should be licensed.
2. A DFS also serves in other capacities such as litigation support, electronic-discovery services, information security, computer network security and video data analysis. These professionals are also monitored by courts (as expert witnesses) or by businesses (as owners of the data) and their attorneys.
3. Requiring a DFS to be licensed as a private investigator may:
 - a. Provide false assurance to consumers that a PI is qualified to offer digital forensics services.
 - b. Provide false assurance to consumers that a DFS is qualified to conduct private investigations.
 - c. Reduce the effectiveness of law enforcement investigators who might seek and rely on assistance from a private sector DFS, especially one that may be located outside of the state of Florida.
 - d. Create conflict and confusion with respect to the roles and responsibilities of a DFS versus a PI.
 - e. Diminish citizens' access to justice through the diminishment of the available pool of qualified DFS persons who are not licensed PIs and have no desire to obtain a PI license and/or conduct the typical work of a PI.
4. Unequal regulation by states requiring a DFS to obtain a private investigator license will be costly and burdensome to litigants and may conflict with the Federal Rules of Evidence.

- a. U.S. Vs. Ganier 6th Circuit Nov. 15, 2006: An IRS Special Agent who was a qualified computer forensic specialist was offered by the government prosecutor as a fact (lay) witness. In her opinion, Judge Moore recognized that while many computer applications are common knowledge, the ability to interpret the output of forensic software required qualification as an expert witness under FRE 702. It is therefore the responsibility of the court to determine if the witness is qualified, if appropriate scientific principles were utilized and applied to the matter at bar.
5. The cross-border nature of computing and telecommunications demands flexibility in digital evidence collection. State PI licensing statutes, on the whole, do not address problems with jurisdiction and reciprocity, and may impede the collection of digital evidence.

Respectfully,

Dave Kleiman - <http://www.ComputerForensicExaminer.com>
4371 Northlake Blvd #314
Palm Beach Gardens, FL 33410
561.310.8801

Proposed Changes to Florida PI Statutes

Florida Private Investigative and Security Services are defined in F.S.S. CHAPTER 493, PRIVATE INVESTIGATIVE, PRIVATE SECURITY, AND REPOSSESSION SERVICES, PART II, PRIVATE INVESTIGATIVE SERVICES (ss. 493.6201-493.6203).

These statutes can be found in the appendix to this memo or online at:

http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&URL=Ch0493/ch0493.htm.

F.S.S. 493.6101 Definitions.-- includes the following language:

- (1) "Department" means the Department of Agriculture and Consumer Services.
- (2) "Person" means any individual, firm, company, agency, organization, partnership, or corporation.
- (3) "Licensee" means any person licensed under this chapter.
- (4) The personal pronoun "he" or the personal pronoun "she" implies the impersonal pronoun "it."

Proposed new language to § 493.6101:

(24) "Digital Forensic Specialist" means a person who has training, education, experience, and/or certification in the seizure, preservation, examination, and analysis of media containing digital data. A digital forensic specialist may interpret, evaluate, test, or analyze pre-existing data from computers, computer systems, networks, or other digital media provided to them by another person who owns, controls, or possesses said computer, computer system, network, or other electronic media.

Or this????

Digital Forensic Specialist" means a person who holds a professional certification or who has training, education, and experience as a digital or computer forensic examiner and who interprets, evaluates, tests, or analyzes pre-existing data from computers, computer systems, networks or other electronic media, provided to them by another person who owns, controls or possesses said computer, computer system, network or other electronic media

F.S.S. 493.6102 Inapplicability of this chapter.--This chapter shall not apply to: (Exemptions) includes the following language:

- (1) Any individual who is an "officer" as defined in s. 943.10(14) or is a law enforcement officer of the United States Government, while such local, state, or federal officer is engaged in her or his official duties or when performing off-duty security activities approved by her or his superiors.
- (2) Any insurance investigator or adjuster licensed by a state or federal licensing authority when such person is providing services or expert advice within the scope of her or his license.
- (3) Any individual solely, exclusively, and regularly employed as an unarmed investigator in connection with the business of her or his employer, when there exists an employer-employee relationship.
- (4) Any unarmed individual engaged in security services who is employed exclusively to work on the premises of her or his employer, or in connection with the business of her or his employer, when there exists an employer-employee relationship.

(15) Any licensed Florida-certified public accountant who is acting within the scope of the practice of public accounting as defined in chapter 473.

Proposed new language to §493.6102 :

(16) An individual employed as a Digital Forensic Specialist, as defined in 493.6101 clause 24.

Or this??

An individual employed as a Digital Forensic Specialist who holds professional certification or degree as a Digital or Computer Forensic Examiner.

Thank you for your attention!

Questions??

****NOT LEGAL ADVICE****