CHAMPLAIN COLLEGE

Computer Forensics Examiners as Private Investigators: The Role of Academia in the Debate

CDFSL 2008
Oklahoma City, OK
April 23, 2008

Gary C. Kessler
Champlain College
Burlington, VT

DISCLAIMER

- I teach in an undergraduate digital forensics (DF) academic program
- I am a Certified Computer Examiner (CCE)
- I do the bulk of my DF practice in support of law enforcement, and some civil work

Overview

- Introduction
- Status
- Does it make sense for DFEs to be licensed as PIs?
- Does it make sense for DFEs to be licensed?
- What is the role of certification?
- What is the role of academia?

Purpose of P.I. Licensure

- 42 states plus D.C. license P.I.s
  - *http://www.crimetime.com/licensing.htm*
- Rules vary nation-wide
  - Some states only require valid business license; others require specialized P.I. license by city or county
  - Licensure may be managed by state agency, licensing board, or police department
  - Reciprocity across jurisdictions is not guaranteed

P.I. Laws & Computer Examiners

- The language of most states' P.I. regulations would suggest that private-sector digital forensics examiners (DFEs) need to be licensed Private Investigators (P.I.)*
- Most P.I. laws pre-date personal computers and private-sector computer forensics practice

*** E.g., see: Radcliff, D. (2008, January 2). Computer forensics faces private eye competition [Electronic version]. *Baseline*. Retrieved April 20, 2008, from http://www.baselinemag.com/c/a/Projects-Security/Computer-Forensics-Faces-Private-Eye-Competition/**

Example: Vermont

- Vermont statutes covering P.I.s says, in part:

V.S.A. Title 26 (Professions and Occupations), Chapter 59 (PRIVATE INVESTIGATIVE AND SECURITY SERVICES), section 3151 defines:

:

(3) "Private detective" or "private investigator" means any person who, for a consideration engages in or solicits business or accepts employment to furnish, or agrees to make or makes any investigation to obtain, information with reference to any of the following or provides, or offers to provide, security of persons incident to any of the following:

:

(B) The identity, habits, conduct, honesty, loyalty, movements, whereabouts, affiliations, associations, transactions, reputation or character of any living person.

:

(E) Evidence to be used before any court, board, officer or investigative committee.

http://www.leg.state.vt.us/statutes/fullchapter.cfm?Title=26&Chapter=059

Example: Texas

- Texas statutes are the most stringent
- Occupation Codes, Title 10 -- Occupations Related to Law Enforcement and Security
- Only licensed P.I.s can secure evidence

§ 1702.101. INVESTIGATIONS COMPANY LICENSE REQUIRED. Unless the person holds a license as an investigations company, a person may not: (1) act as an investigations company; (2) offer to perform the services of an investigations company; or (3) engage in business activity for which a license is required under this chapter.

§ 1702.104. INVESTIGATIONS COMPANY. (a) A person acts as an investigations company for the purposes of this chapter if the person: (1) engages in the business of obtaining or furnishing, or accepts employment to obtain or furnish, information related to: ... (B) the identity, habits, business, occupation, knowledge, efficiency, loyalty, movement, location, affiliations, associations, transactions, acts, reputation, or character of a person; ... (2) engages in the business of securing, or accepts employment to secure, evidence for use before a court, board, officer, or investigating committee; ... For purposes of Subsection (a)(1), obtaining or furnishing information includes information obtained or furnished through the review and analysis of, and the investigation into the content of, computer-based data not available to the public.

Example: Texas (cont.)

- It is also a crime to hire a non-licensed person to secure evidence

§ 1702.386. UNAUTHORIZED EMPLOYMENT; OFFENSE. (a) A person commits an offense if the person contracts with or employs a person who is required to hold a license, registration, certificate, or commission under this chapter knowing that the person does not hold the required license, registration, certificate, or commission or who otherwise, at the time of contract or employment, is in violation of this chapter. (b) An offense under Subsection (a) is a Class A misdemeanor.

- Yet a non-licensed DFE could still be accepted as an expert in a Texas court

http://tlo2.tlc.state.tx.us/statutes/oc.toc.htm

Status in the U.S.

- States that do not license P.I.s: 8
  - AL, AK, CO, ID, MS, MO, SD, WY
- States that exclude DFEs from licensure as P.I.s: 5
  - DE, LA, ND, VA, WA
- States with no clear guidelines but appear to exclude DFEs from P.I. licensure: 3
  - FL, IN, NE
- States that require P.I. licensure for DFEs: 2
  - IL, TX

Status in the U.S. (cont.)

- States with no clear guidelines but could include DFEs in the P.I. requirement: 27
  - AZ, AR, CA, CT, GA, HI, IA, KS, KY, ME, MD, MI, MN, MO, NH, NJ, NM, NY, OH, OK, OR, RI, TN, UT, VT, WV, WI
- States that require P.I. license based on opinion: 4
  - MA, NV, NC, SC
- Unknown status: 2
  - PA, D.C.

White, D., & Micheletti, C. (2008, April 21). An examination of state laws concerning the practice of computer forensics and private investigation licensure requirements. Warren, RI: Secure Technology.

Rhode Island

- Rhode Island's response -- add an exclusion clause into the P.I. legislation
  - Current proposal to RI legislature
  - Also known to be under consideration in NV and VT
- Add definition of *computer forensic specialist*

"Computer forensic specialist" means a person 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 and holds a professional certification as a computer examiner.

Why License P.I.s

- Consumer protection
- Regulate the industry
- Generate revenue
  - This is one reason that many states are enlarging the scope of the P.I. board!
- Many PI firms are in favor of d.f. licensure because it allows them to expand their business but prevents DFEs from business (at least temporarily)

Why License DFEs as P.I.s

- Same reasons to license DFEs as for P.I.s...
  - ... but does it make sense to license DFEs as P.I.s?
- E.g., VT P.I. requirement is that an individual
  - Knows VT P.I. statutes
  - Knows the VT Fair Credit Reporting Act
  - Has 2,000 hours working under a licensed P.I.
  - D.f. knowledge and experience requirement: **ø**

Should DFEs be Licensed?

- Would provide same oversight as P.I. licensure
- Could suggest that DFE license holder has at least minimal qualifications
- But what are those *minimal qualifications*?
  - Certification/training
  - Education

Industry Certification Efforts

- CyberSecurity Institute
  - CyberSecurity Forensic Analyst (CSFA)
- EC-Council
  - Computer Hacking Forensic Investigator (CHFI)
- International Association of Computer Investigative Specialists (IACIS)
  - Certified Forensic Computer Examiner (CFCE)
  - Certified Electronic Evidence Collection Specialist (CEECS)
- International Society of Forensic Computer Examiners (ISFCE)
  - Certified Computer Examiner (CCE)
- SANS Institute
  - GIAC Certified Forensics Analyst (GCFA)

Vendor Certification

- AccessData Corp.
  - AccessData Certified Examiner (ACE)
- Guidance Software
  - EnCase Certified Examiner (EnCE)
- Wetstone Technologies
  - Certified Malicious Software Investigator
  - Certified Steganography Investigator
- X-Ways Software
  - X-Ways Investigator
- ...

National Certification (U.S.)

- Digital Forensics Certification Board (DFCB)
  - Attempt to create standards for DF practitioners
    - Focus and history is very LE focused (e.g., IACIS, HTCIA, FBI CART, USSS ECTF)
  - Project ran from 2004-2007
    - Web site shows reports, competencies, and certification levels... but no criteria or testing methodologies
    - Current status...
    - http://www.ncfs.org/dfcb/

DFCB Competencies & Certifications

Core Competencies		*Certification Map*
Foundation Skills	**Examination**	**DFCB Acquisition Certification**
Quality Assurance	Networking and Communications	Foundation Knowledge
Legal and Ethics	Computer/Data Concepts	Acquisition Knowledge
Techniques	Hardware	Examination Knowledge
Process	Exam Process	Analytical Knowledge
Concepts		
	Analysis	**DFCB Examiner Certification**
Acquisition (Remote/Live/Field/Lab)	Law and Procedures	Foundation Knowledge
Process	Processes	Acquisition Knowledge
Evidence Identification	Analytical Techniques	
Legal Authority	Technology	**DFCB Forensic Foundations Certificate**
Acquisition Techniques		Foundation Knowledge

Education

- There are a growing number of undergraduate DF programs in the U.S.
  - Is a B.S. in DF sufficient for licensure?
  - Is an A.S. in DF sufficient for licensure?
  - Who vets the curricula?
    - I.e., how many DF courses does a curricula need to have in order to "qualify"?
- Is a graduate of a DF program ready to start a practice?

What is the Role of Academia

- How do we keep *any* curriculum relevant, correct, and practical?
- How do we remain responsive to new technologies, laws, and requirements
- How do we enforce our own standards?
- How can we be *properly* inclusive?
- Should academic programs teach to industry training certifications?

Can Academics Add to the Debate?

- Work with industry groups
  - ISFCE and HTCC are leading the effort
  - May also include HTCIA, SANS, and others
- Proposals, discussion, training -- and testimony -- to state legislatures

Conclusion

- Most sources agree that some sort of certification or professional vetting is a Good Thing
  - It appears unclear as to what neutral agency exists to prepare and monitor this endeavor
  - The profit motive will drive the pool of players
- Do we need more than one certification suite?
  - Different set of certifications for different sectors

Speaker Contact Information

Gary C. Kessler, Ed.S., CCE, CISSP
Computer & Digital Forensics program
Center for Digital Investigation
Champlain College
163 South Willard Street
Burlington, VT 05401

office: +1 802-865-6460
cell: +1 802-238-8913
fax: +1 802-865-6446
e-mail: gary.*kessler@champlain.edu*
Skype: *gary.c.kessler*

http://digitalforensics.champlain.edu
http://c3di.champlain.edu
http://www.garykessler.net

The speaker preparing his presentations...

This work was partially supported by Grant No. 2006-DD-BX-0282 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United State Department of Justice.