

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

BRYAN PRINGLE, an individual,
Plaintiff,

vs.

WILLIAM ADAMS, JR.; STACY
FERGUSON; ALLAN PINEDA; and
JAIME GOMEZ, all individually and
collectively as the music group The
Black Eyed Peas, *et al.*,
Defendants

Case No. SACV 8:10-CV-01656 JST
(RZx)

DECLARATION OF ERIK LAYKIN

I, ERIK LAYKIN, declare as follows:

I. EXPERT QUALIFICATIONS

1. I am a Managing Director of the Global Electronic Discovery and Investigations practice of Duff & Phelps, LLC (“D&P”), an independent consulting firm of approximately 1,100 professionals, which is publicly listed on the New York Stock Exchange (DUF). D&P provides litigation, financial, restructuring and operational consulting services to government agencies, legal counsel and companies in a variety of industries. I have been employed by D&P since July 2008, and am based in its Los Angeles, California office.

2. I am accredited by the Electronic Commerce Council as a specialist in the field of Technology Disputes, Computer Forensics and Electronic Discovery, and have testified in state and federal courts on numerous occasions on matters

DECLARATION OF ERIK LAYKIN

1 related to the investigation, analysis and management of electronic data, computer
2 forensic preservation and analysis, and other information technology disputes. I
3 have managed over 200 matters relating to these issues during the past 10 years.

4 3. From 2004 through 2008, I was the Director of the Information
5 Technology Investigations practice group at Navigant Consulting, Inc. (NYSE:NCI)
6 and served on the Management Committee of its Discovery Services practice group.
7 In this role, I led teams of professionals that provided electronic discovery,
8 computer forensic and investigative consulting services for a wide variety of
9 national and international clients.

10 4. From 1997 to 2004, I served as President and Founder of Online
11 Security (OnlineSecurity.com) which was one of world's first providers of
12 commercial computer forensic services to the legal and business community for the
13 investigation and resolution of disputes.

14 5. As part of my work at Online Security, I managed and/or developed the
15 initial Computer Forensic service offerings and established standards on behalf of
16 investigative agencies in the United States and Asia, including The Investigative
17 Group International, Kroll & Associates and Pinkerton Consulting & Investigations.

18 6. As a result of the above training and experience, I have become very
19 familiar with a variety of software development technologies, computer systems,
20 programming languages, computer forensic and electronic discovery systems, and
21 standards of practice within the Information Technology industry.

22 7. I have provided expert training on the topics of Computer Forensics,
23 Cyber Crime and Electronic Discovery to numerous organizations including the
24 FBI, the ABA (American Bar Association), the HTCIA (High Tech Crime
25 Investigation Association), AICPA (American Institute of Certified Public
26 Investigation Association), AICPA (American Institute of Certified Public
27 Investigation Association), AICPA (American Institute of Certified Public
28 Investigation Association), AICPA (American Institute of Certified Public

1 Accountants), the Government of Malaysia, the Government of the United Arab
2 Emirates, the Government of Taiwan, the Government of Hong Kong and the
3 Government of the People’s Republic of China.

4 8. I have served as an expert witness and investigator, and have been
5 appointed as Special Master in complex cases involving information technology and
6 the disputes which arise from its usage within a business and network environment.
7 My Curriculum Vitae is attached as Exhibit A.

8
9 **II. BACKGROUND AND SCOPE OF ASSIGNMENT**

10 9. I understand that the Plaintiff, Bryan Pringle, claims that he created a
11 song in 1999 entitled “Take a Dive” (Dance Version), and that Defendants allegedly
12 copied portions of that song when they created the song “I Gotta Feeling,” which
13 was released by The Black Eyed Peas in 2009.

14 10. In asserting that he created “Take a Dive” (Dance Version) in 1999, I
15 understand that Pringle relies on an “NRG” file that contains the instrumental tracks
16 of “Take a Dive” (Dance Version). An NRG file is a proprietary file format
17 developed by the makers of the popular commercial CD Rom burning software
18 known as Nero. This software ships pre-installed on many desktop and laptop
19 computers, is downloadable from the Internet and has been available for purchase as
20 a stand-alone software title at most computer and office supply stores throughout the
21 United States. The file format itself is proprietary and encodes whatever data a user
22 wishes to copy from the hard drive of their computer onto a CD Rom or a DVD
23 Rom. The process in which a new NRG file is created and saved from the original
24 source file on the hard drive onto a CD or DVD is known as “burning” a file.

25 11. I understand that Pringle no longer possesses the computer on which he
26 originally created and saved this NRG file, as he claims that computer was stolen
27

1 from a storage locker in 2000. Instead, Pringle relies on a CD to which he allegedly
2 copied (or “burned”) the NRG file in 1999. (I refer herein to a CD containing an
3 NRG file as an “NRG disc.”)

4 12. Pringle first submitted an NRG disc allegedly containing the tracks of
5 “Take a Dive” (Dance Version) in connection with his application for a temporary
6 restraining order (“TRO”) in November 2010. That NRG disc was accompanied by
7 the Declaration of David Gallant, dated November 18, 2010, which purported to
8 authenticate the NRG file as having been last modified on June 14, 1999 and having
9 been burned to the NRG disc on May 17, 2001—after Pringle’s computer equipment
10 was allegedly stolen. Pringle also submitted his own Declaration, dated November
11 17, 2010, stating that he saved the NRG file that contained “Take a Dive” (Dance
12 Version) to his personal computer on June 14, 1999, and that he burned that NRG
13 file from his computer to a blank CD in May 2001. Pringle even identified the serial
14 number of the NRG disc which allegedly contained “Take a Dive” (Dance Version).

15 13. I was asked by counsel for Defendants to review the November 18,
16 2010 Declaration of David Gallant, and to provide my professional expert opinion
17 regarding Mr. Gallant’s methodology and conclusions. Based on that review, I
18 submitted a Declaration, dated November 23, 2010, in which I explained that the
19 process and procedures employed and described by Mr. Gallant were of
20 questionable reliability, that Mr. Gallant’s findings were incomplete, and that Mr.
21 Gallant’s declaration fell short of the standard of care expected in the practice of
22 professional computer forensics. I therefore concluded that Mr. Gallant’s
23 declaration was an insufficient basis on which to authenticate the NRG disc and its
24 contents.

25 14. I understand that, following my November 23, 2010 Declaration, on
26 January 3, 2011, Pringle filed a motion for a preliminary injunction, in which he
27

1 acknowledged that the NRG disc he had submitted in connection with his TRO
2 motion, and upon which his and Mr. Gallant's declarations were based, was, in fact,
3 the wrong disc. Pringle submitted a new "correct" NRG disc in connection with his
4 preliminary injunction motion.

5 15. In his motion for a preliminary injunction, Pringle's counsel
6 represented that Mr. Gallant had analyzed the "correct" NRG disc and assured them
7 that the NRG file on that disc had a creation date in 1999, but that Mr. Gallant was
8 unable to complete his analysis because of the 2010 winter holidays.¹

9
10 16. I have been asked by counsel for the Defendants to provide my
11 professional expert opinion as to whether or not the "correct" NRG disc on which
12 Pringle relies can be used to authenticate the date of creation of the NRG file on that
13 disc.

14 17. I also understand that Pringle has testified to having discarded two
15 computer hard drives while this litigation was pending—one in December 2010 or
16 January 2011, and another in the summer of 2011. Pringle further testified that,
17 prior to discarding these hard drives, he backed up what he considered to be relevant
18 files, but that he did not back up program files, Internet-related files or temporary
19 data files.

20 18. I have been asked by Defendants' counsel to provide my professional
21 expert opinion as to whether the process employed by Pringle meets professional
22 standards for electronic data preservation for litigation purposes. I have also been

23 _____
24 ¹ I understand that, on November 11, 2011, Pringle's counsel produced a letter from
25 Mr. Gallant dated August 6, 2011 that purports to date the "correct" NRG disc.
26 Because of substantial prior professional commitments, I have not had sufficient
27 time to analyze Mr. Gallant's letter and the technical analysis discussed therein. I
28 reserve the right to do so should Pringle rely on Mr. Gallant's letter in response to
this Declaration.

1 asked to provide my professional expert opinion as to whether examination of
2 Pringle's 2009/2010 hard drives might reveal evidence indicating (i) whether
3 Pringle back-dated the NRG disc, and (ii) whether, where and when Pringle
4 downloaded "I Gotta Feeling" music files.

5 19. In conducting my analysis, I have reviewed the following materials:

- 6 a. Declaration of Bryan Pringle, dated November 17, 2010, in Support
7 of Plaintiff's Motion for TRO;
- 8 b. Declaration of David Gallant, dated November 18, 2010, in Support
9 of Plaintiff's Motion for TRO;
- 10 c. Memorandum of Points and Authorities in Support of Plaintiff's
11 Motion for Preliminary Injunction, dated January 3, 2011;
- 12 d. Declaration of Bryan Pringle, dated January 3, 2011, in Support of
13 Plaintiff's Motion for Preliminary Injunction;
- 14 e. Copies of two CDs produced at the offices of David Gallant on
15 August 8, 2011; and
- 16 f. Transcript of the Deposition of Bryan Pringle, dated August 24,
17 2011.

18 20. I am being compensated at the rate of \$525/hour for the analysis and
19 testimony which may be provided in this matter.

20 **III. ANALYSIS**

21 **A. The Date of the NRG File Can Not be Authenticated Without Analysis**
22 **of the Computer(s) Used to Create the File and to Burn it to the NRG**
23 **Disc**

24 21. For the reasons discussed below, it is my professional expert opinion
25 that, regardless of the date on which the CD itself was manufactured, it is not
26 possible to authenticate the date on which the NRG file was saved to the NRG disc
27

1 without access to the computer on which the NRG file was saved, and the computer
2 from which the NRG file was burned to the NRG disc.

3 22. Time and date stamps on files are easily modified and cannot be relied
4 upon without corroborating evidence of their authenticity. A user may modify time
5 and date stamps in a variety of ways, the most common of which is to change the
6 system clock on the computer on which the files will be created or saved to. This
7 simple approach will allow the user to create files that are backdated to appear as
8 though they were created on any date and time they choose. A user could back-date
9 a file to 1776 as easily as they could 1976. Subsequently, the files that are created
10 with these backdated file attributes can then be saved to new locations such as other
11 computers, floppy drives, the Internet or even CD Rom or DVD Rom discs, and
12 they will still contain the same falsified time and date stamps.

13 23. The dates on which a CD or DVD has been burned can also be
14 modified or backdated using the same technique in which the computer clock is
15 rolled back to some prior point in time. This action would impact the time and date
16 stamps of the actual burning of the CD or DVD.

17 24. Validating the authenticity of backdated or falsified time and date
18 stamps requires the presence of some secondary data source to which the backdated
19 files can be compared, such as the original computer used to save the file or burn it
20 to a disc. In fraud cases where a computer is used to backdate a particular file, it is
21 not unusual that the original computer would disappear or be disposed of, so as to
22 prevent discovery of the fraud. By examining the original computer used to create
23 and save a file to CD, a computer forensic examiner would likely be able to discover
24 whether the file and CD had been backdated. That is because it would be very
25 challenging, if not impossible, for even the most adroit computer user to falsify the
26 entire record contained on a computer, where there are tens of thousands of
27

1 references to dates, many of which are maintained “behind the scenes” without the
2 knowledge or influence of the user.

3 25. There is a significant body of knowledge, freely accessible on the
4 Internet to the casual user on the topic of “Anti-Forensics” which is the process of
5 obfuscating the evidentiary trail that a computer forensic examiner would follow.
6 While there are a number of applications, software utilities and “tricks of the trade”
7 that can be deployed to cover up a falsified file date with even limited technical
8 knowledge; by far the most common method used is to simply discard the original
9 computer(s) altogether.

10 26. For a thorough analysis, it would be vital to review the original
11 computer which managed the burning of the CD in the first instance, or a forensic
12 backup of that computer.

13 27. Further complicating matters, persons engaged in the backdating of
14 computer files have also been known to use older computer equipment from the
15 back-dated time period, in order to hide the digital fingerprints often left by software
16 or hardware that was not in existence at that time. Such decommissioned computers
17 can be purchased at second-hand stores, garage sales, flea markets, EBay.com and
18 other sources for as little as \$50.00. Similarly, older digital storage media such as
19 CDs, which are also readily available for purchase, have been known to be used to
20 make it more difficult to determine the true date of back-dated files. This is
21 particularly true where, as here, the computer(s) on which the files were created and
22 burned to CD are not available for forensic examination.

23 28. In my experience, it is not uncommon for individuals who use CD Rom
24 discs on a regular basis, such as those in the electronic music industry, to retain a
25 number of unused CDs, and to burn data to those old CDs years later. CD Rom
26
27

1 discs are often purchased in bulk, for instance in packages of 25, 50, 100 or even
2 250 discs. Indeed, Mr. Pringle testified to having repeatedly sent out demo CDs in
3 batches as large as 200 at a time, over a period of many years. Pringle thus likely
4 had access to old CDs from the late 1990s which he could have used to burn the
5 NRG discs in 2009 or 2010.

6 29. In my experience as a computer forensic investigator, I find it highly
7 circumspect that an individual such as Pringle, who claims to rely upon computer
8 technology for his craft of creating digital music, has failed to maintain any of his
9 computers which would have a digital relationship of some sort to the files in
10 question. Not only are backups and archives unavailable, which alone is highly
11 unusual, but even his more recent computers used in 2009 and 2010 are unavailable
12 for examination. Through Pringle's reluctance or inability to provide any of these
13 original computers, he has prevented the files residing on the NRG discs from ever
14 being authenticated or disproved as genuine.

15 **B. Pringle's 2009/2010 Hard Drives Would Likely Contain Evidence of**
16 **Any Backdating of the NRG File**

17 30. Pringle has not produced the computer hard drives that he used in 2009
18 and 2010 because he disposed of them while the lawsuit was pending. Examination
19 of those drives could yield evidence that Pringle backdated the creation and last
20 accessed dates of the NRG files. This would be found by examining a combination
21 of resources on the hard drive including but not limited to the system registry which
22 logs the connection of all devices to the computer, the file system which maintains
23 last accessed dates and creation dates for every file on the computer, and finally the
24 unallocated space which maintains a variety of data points which are inaccessible by
25 the user and often include best evidence of the creation or deletion of files, and clues
26 to modifications which have taken place on the system.

1 31. In this instance, the computer forensic examiner would most certainly
2 review the unallocated space of Pringle’s hard drives for fragments of files which
3 indicate the actual time and date on which the computer was operating at the time
4 the NRG files were burned. In addition, the computer forensic examiner would
5 review artifacts in the operating system contained on the hard drive for markers that
6 would indicate that the operating system had been impacted by the ‘rolling back’ of
7 the date on the machine. These and other techniques, including analysis of whether
8 or not software was rolled back to earlier versions, could prove or disprove the
9 authenticity of the dates of the NRG file in question. Without employing these and
10 other related techniques, I am not aware of a reasonably reliable way to authenticate
11 the date of files saved to Pringle’s NRG disc.

12 32. Pringle’s disposal of his 2009 and 2010 hard drives also prevented us
13 from examining his recent user activity, which could not only include a review of
14 unallocated space, but also of temporary Internet files and other artifacts, which
15 would provide insight into his activities at that time. This activity could show that
16 the music files in question were actually downloaded from the Internet in 2009 or
17 2010, after the release of “I Gotta Feeling,” and subsequently backdated and/or
18 modified to appear as though they had been created in 1999.

19 33. At present I cannot see any rationale for the failure to preserve the
20 electronic evidence which is central to Pringle’s claims, whether the hard drives or
21 computers were operational or not. In fact, even if the drives were not functioning
22 properly in Pringle’s personal computer, computer forensic techniques could still
23 reliably retrieve the data contained on them for analysis and reporting to this Court.
24 Indeed, a simple search on the Internet for terms such as “Failed Hard Drive”,
25 “Crashed Computer”, “Broken Hard Disc” or “Data Restoration”, will yield dozens
26 upon dozens of companies that will gladly receive your hard drive and restore the
27

1 data. Instead, it appears that Pringle disposed of his hard drives such that the
2 information on them could never be recovered.

3 **C. Pringle’s 2009/2010 Hard Drives Would Likely Contain Evidence As**
4 **to When and Where Pringle Downloaded “I Gotta Feeling” Music**
5 **Files**

6 34. While Pringle claims to have saved certain computer files from the hard
7 drives that he used in 2009 and 2010 and discarded during this lawsuit, he has
8 acknowledged that he did not conduct a forensic backup of those hard drives, and, in
9 particular, did not preserve the temporary Internet files, program data or system data
10 from those hard drives. Had these sources been preserved and provided, they would
11 have the capacity to show whether or not, and when, Pringle obtained The Black
12 Eyed Peas’ music from the Internet.

13 35. Had Pringle downloaded these music files from the Internet, the hard
14 drive would likely have a record of this activity stored within the temporary Internet
15 history files, the cookie history files and the download repository. Even if Pringle
16 had downloaded the music files, copied or burned them to another location, and then
17 deleted the files and the Internet history and cookie repositories, there is a strong
18 likelihood that a forensic examination would have found evidence of this activity in
19 the unallocated space of the computer hard drive. It is here that we could have
20 found entire files, fragments of files and logs of computer usage which would have
21 been nearly impossible for the user to manually erase.

22 36. It is therefore my opinion that Pringle’s act of discarding his computer
23 hard drives due to their claimed mechanical failures, falls far below the accepted
24 standard of preservation of electronic evidence in litigation, not to mention the
25 common-sense pursuit of his claims in this action. Indeed, it appears that Pringle
26 has used the simplest “anti-forensics” technique available to him to prevent the
27

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Defendants and this Court from learning the true nature of the activity that took place on Pringle's computers, and thus whether or not his claims have any merit.

37. I reserve the right to supplement this report and to revise my opinion to account for any new information that may be made available by Plaintiff, Defendants, their counsel or any other source.

I declare under penalty of perjury that the foregoing is true and correct.



November 14th, 2011

Erik Laykin

Date

Exhibit A to
Declaration of Erik Laykin

Erik Laykin

Erik Laykin, CHFI

Managing Director

Duff and Phelps, Inc.

Two California Plaza
350 South Grand Avenue
31st Floor
Los Angeles, CA 90071

Tel: 213.270.2370

Fax: 213.985.2500

Cell: 310.245.2902

erik.laykin@duffandphelps.com

Current Position

Erik Laykin is the Managing Director and Practice Co-Chair of the Duff and Phelps, Inc. (NYSE: DUF) Global Electronic Discovery and Investigations Practice. Mr. Laykin manages complex investigations and disputes in a wide variety of industries and geographies on behalf of litigants, corporations and government agencies.

Previously Mr. Laykin was the Director of Information Technology Investigations at Navigant Consulting, Inc. (NYSE: NCI) and in the mid 1990's was the Founder and President of Online Security, Inc., a pioneer in the emerging discipline of high technology investigations, computer forensics and electronic discovery.

Today Mr. Laykin is an accredited specialist in the reactive investigation and analysis of domestic and international digital theft, cyber-terrorism, trademark infringement, online piracy, cyber squatting, information technology disputes, electronic discovery protocols and corporate espionage. He has frequently appeared on CNN, FOX, ABC, NBC, and CBS and has participated on several advisory boards including the California Judicial Council's Subcommittee on Digital Evidence, The Electronic Commerce Council, The State of California's Insurance Fraud Task Force and he is the past Pacific Rim Director of the FBI's INFRAGARD program.

Mr. Laykin has also served as an expert witness, Investigator and Special Master to the court in complex cases involving information technology and the disputes which arise from its usage within a business and network environment. Through his ability to distill and simplify a broad range of technology concepts and issues, many of his clients have successfully resolved their disputes.

Selection of Noteworthy Cases

Largest Bankruptcy in US History

On behalf of Anton R. Valukas, Chairman of Jenner & Block

On behalf of the court appointed examiner, Mr. Laykin led the team responsible for managing the data request, collection and analysis effort for the financial investigation of the largest bankruptcy in US history. In providing support to the financial analysis teams, Mr. Laykin directed the collection, analysis and distribution of over 40 million pages of documents culled from 7 petabytes of data in over 2,600 global systems. The effort resulted in a comprehensive 2,200 page report on the causes of the September 2008 failure of Lehman Brothers which was delivered to several branches of the US government.

Global Intellectual Property and Patent Dispute

On behalf of Kelley Dye and Warren

Appointed expert witness on behalf of defendant, a European based global Fortune 50 Company engaged in an intellectual property dispute with an American Fortune 100 company. The action, which was filed in 2003 rested on transactions and systems dating back to the mid 1990's. As an expert in the matter Mr. Laykin directed the management and retrieval of archival data from multiple global systems and successfully testified as to the impact of the plaintiff's actions and access to databases operated by the defendant.

Global Cyber Crime Conspiracy

On behalf of Baker Hostetler

As expert witness and Special Master to the Federal Court, Mr. Laykin managed the strategic direction of the plaintiff's global electronic evidence preservation, analysis and discovery requirements. Directing both local teams and subcontracted teams from "Big 4" consulting firms on several continents, Mr. Laykin successfully acquired digital evidence which thwarted a major global cyber crime conspiracy which included both intellectual property theft and trade secret misappropriation in which the plaintiff had already suffered considerable loss. As a result of Mr. Laykin's testimony, the defendants elected for settlement.

Global Trademark Infringement and Trade Secret Theft Matter

On behalf of Kelley Dye and Warren

On behalf of defendant and counter claimant: one of India's largest online businesses, Mr. Laykin was appointed expert witness in a trademark infringement matter, valued at over 60 million dollars, which had lingered for several years. Through extensive discovery and pretrial investigations, Mr. Laykin and the electronic evidence team was able to establish substantial evidence favorable to the position of the defendant, thereby helping to induce positive early settlement.

California Insurance Fraud Matter

On behalf of Ford, Walker, Haggerty and Behar

On behalf of several co-defendant insurance carriers, Mr. Laykin was appointed expert for the purpose of testifying as to the market value of an online business which had suffered a catastrophic fire several years earlier and had filed a claim for exorbitant losses based on inflated internet valuations. As a result of Mr. Laykin's testimony, plaintiff settled with the insurance carriers for an amount equal to a small fraction of their original claim.

National Intellectual Property Theft and Unfair Competition Dispute

On behalf of Goodwin Procter

Plaintiff's counsel appointed Mr. Laykin to establish a basis for intellectual property violations based on the unfair usage of computer code. Mr. Laykin and his team examined thousands of pages of database and programming code from both plaintiff and defendant and provided a basis for the argument that the defendant had both infringed on plaintiff's intellectual property and was engaging in unfair competitive practices. As a result of Mr. Laykin's testimony defendant settled on terms favorable to the plaintiff.

Selection of Recent and Upcoming Presentations

Conference

- BIT's 2nd Annual World Congress of Forensics – Chongqing, China – Oct 2011
- International Association of Privacy Professionals Privacy Academy 2011 – Dallas, TX – September 2011
- IQPC 11th eDiscovery Summit – San Francisco, CA – April 2011
- RSA 2011 / 8th Annual Executive Security Action Forum – San Francisco, CA – February 2011
- BIT's 1st Annual World Congress of Forensics Conference – Dalian, China – October 2010
- Hacker Halted USA Conference – Miami, FL – October 2010
- Asia Anti Fraud Conference – Jakarta, Indonesia – August 2010
- Association of Information Technology Professionals Panel Discussion – Los Angeles, CA – July 2010
- Annual National IASA Conference: Insurance Accounting and Systems Association – Dallas, TX – June 2010
- Greenberg Traurig Litigation Skills Academy – Chicago, IL – May 2010

Topic

- Speaker – “Managing Computer Forensic Investigations in the Cloud”
- Speaker – “Monitoring and Preserving Data on Social Media Sites”
- Speaker – "How an eDiscovery Special Master can Reduce your Risks and Costs in the Courtroom"
- eDiscovery Strategies in a World with Clouds, Social Media and User-owned Devices
- Chair – Cyber Crimes, Computer Forensics and IP toward Business Law
- Speaker – “The National Cyber Corps: A Call to Action”
- Faculty – International Seminar on Information Technology, Cyber Crimes and Computer Forensic series
- Panelist / Moderator – “Protecting Client Data in the Enterprise”
- Investigative Computer Forensics: A hands on primer for leveraging computer forensics to preserve evidence and prevent fraud.
- Faculty – Computer Forensics

Conference

- Annual Symposium on Risk Management – Hong Kong – March 2010
- Information Systems Security Association (ISSA) – New York, NY – February 2010
- Legal Technology CEO Summit – New York, NY – January 2010
- HTCIA – Asia Pacific Annual Conference – Hong Kong – December 2009
- Greenberg Traurig Shareholders Mock Trial – Houston TX – October 2009
- AICPA National Conference – Orlando, FL – September 2009
- Hacker Halted USA Conference – Miami, FL – September 2009
- Greenberg Traurig Litigation Skills Academy – Tampa, FL – May 2009
- US Trustees Annual Conference – Los Angeles, CA – May 2009
- US Department of Defense – CyberCrime Summit – January 2009
- Practicing Law Institute – National CLE – December 2008
- Annual Risk Symposium – Hong Kong – 2008
- Hacker Halted USA – Myrtle Beach, SC – 2008
- IASA – Seattle, WA – 2008
- Microsoft Asian Partners Symposium – Taiwan – 2008
- Integrated Security Conference – Hong Kong – 2008
- Greenberg Traurig Litigation Skills Academy – Washington, DC – 2007
- Malaysian Prime Minister's Symposium on Cyber Terrorism and Cyber Crime – Kuala Lumpur – 2007
- Taiwan Privacy Association – Taipei – 2007
- ABA Employment Section National Conference – New Orleans, LA – 2007
- Hacker Halted 2007 – Dubai
- IAPP Privacy Summit 2007 – Washington, DC
- Hacker Halted – Peoples Republic of China – 2006
- Symposium on Risk Management 2006 – Hong Kong

Topic

- Keynote Speaker – Computer Forensics
- Panelist – "Shifts in the CISO's Domain – Authenticity, Admissibility and the Future of Forensics."
- Speaker – Intersection of Law, Technology and Capital
Investigating Accounting and Financial Fraud in Asia
- Faculty – Computer Forensics
Computer Forensics in Accounting Investigations
- The Intersection of Technology and Crime
- Faculty & Keynote – Computer Forensics
Complex Data Management in Bankruptcy Matters
- The Chinese Cyber War Machine
Electronic Discovery in the Financial Sector
- Forensic Data Collection in Foreign Jurisdictions
- The Chinese Cyber War Machine
Forensics for the Insurance Industry
The Global Cyber Security Footprint
- Keynote Speech – Hackers and CyberCrime Comes of Age
Faculty and Keynote – Computer Forensics and Electronic Discovery
- Guest Faculty and Conference Chairman
- Keynote Speech on Digital Privacy for Launch of Association
Investigating Mass Personal Identity Theft
- Keynote: Penetration Testing Methodologies
Investigations and Litigation in the European Union
- Keynote – CyberCrime: A Global Outlook
Digital Disaster: How Digital Data can Destroy your Business

Conference

- 3rd Annual Integrated Security Conference and Storage World 2006
- International Technology Law Association 35th Annual Congress – San Francisco – 2006
- Middle East Security Conference – Abu Dhabi
- Hacker Halted 2005 – Dubai
- Hacker Halted 2005 – Singapore
- Direct Selling Association 2005 – Baltimore, MD
- HTCIA (High Tech Crime Investigators Association) – Los Angeles
- IASA 2005 – Anaheim, CA
- Lex Mundi European Annual Conference – Prague
- Hacker Halted 2005 – Mexico City
- Symposium on Risk Management 2005 – Hong Kong
- American Conference Institute – New York, NY
- Techno-Security 2005 – Myrtle Beach, SC
- InfoSecurity 2004 – New York, NY
- Hacker Halted / Asian Computer Forensic Conference – Kuala, Lumpur
- CA World 2004 – Las Vegas, NV
- Software Council of Southern California – Los Angeles, CA
- IDG Integrated Security Asian Expo 2004 - Singapore
- Informatics Symposium on Computer Forensics and Cyber Crime – Hong Kong
- Security Industry Roundtable 2004 – Miami, FL
- Computer Security Institute's 30th Annual Industry Conference – Washington, DC
- USC Marshall School of Business – Roundtable – 2003 – Los Angeles, CA
- CA World 2003 – Las Vegas, NV
- Los Angeles Venture Association – Los Angeles, CA
- California CPA Educational Foundation Conference 2003 – San Francisco, CA
- Association of Internet Professionals – Los Angeles, CA
- Asian Development Bank : 36th Annual World – Shanghai, China

Topic

- Privacy Risks in the Enterprise
- Navigating the new threat landscape: Exploring methods and protecting critical business infrastructures
- Global Internet Money Laundering
- Global Internet Money Laundering
- The State of Personal Data Privacy
- Best Practices in Security and Disaster Recovery
- Ethical Considerations in Electronic Discovery
- Insurance Industry Investigations
- Challenges in Electronic Evidence Collection
- Cyber Crime
- Technology Risk Management Best Practices
- Responding to Insurance Industry Investigations
- Hardware Based Computer Forensic Acquisitions with the Logicube
- Electronic Evidence Fundamentals
- Keynote – Information Espionage
- Risks of OutSourcing
- Risks of OutSourcing
- Keynote – Cyber Terrorism
- Keynote – Information Espionage
- Computers and Terrorists
- Computer Forensics: Incident Response and Best Practices
- Pan-Pacific Strategies to Secure the M-Commerce Marketplace
- Convergence of Physical and I.T. Security: A New Dynamic
- Economic Espionage, Fraud and Embezzlement
- Digital Evidence and Monitoring for Electronic Fraud
- Security in the Connected World
- Global Security Risks in the Energy Industry

Conference

- Information Systems Audit and Control Association : 30th Annual
- United Kingdom National Crime Squad Conference – London, UK
- Association of Certified Fraud Examiners – Irvine, CA
- ComTech – Santa Barbara, CA
- Association of Trial Lawyers of America – Atlanta, GA
- Federal Bureau of Investigations – Los Angeles, CA
- International Security Conference and Exposition
- LinuxWorld – New York, NY
- Comdex – Las Vegas, NV
- 1st Annual China Banking Security Forum – Hong Kong
- Computer Law Association – Sidney, Australia
- Asia Law Society
- Information Systems Security Association

Topic

- Compliance Tools: The Changing Landscape of American Business
- Fraud in the Enterprise: Economic Espionage in the Connected World
- Information Technology Fraud: Emerging Threats and Responses
- Cyber Attack: Security and Recovery Solutions
- Discovery of Insurance Industry Computer Systems
- Computer Forensics and International Cyber Crime
- Economic Espionage and Protecting Intellectual Property
- Information Espionage and Global Corporate Risk
- Computer Forensics and Digital Evidence Preservation
- Electronic Evidence and Contemporary Banking Fraud
- Wireless Security
- Emerging Trends in Cyber Terrorism and Global Information Security
- Internet Security and Investigations

Selection of Recent Publications**Publications**

- Metropolitan Corporate Counsel – August 2011
- Metropolitan Corporate Counsel – March 2011
- Featured Computer Forensic Expert for a 6 part television series on Forensic Sciences produced by A&E /The History Channel 2010
- Investigative Computer Forensics – Wiley, Due 2012
- Government Information Security News – May 24, 2010
- Product Liability Litigation: Current Law, Strategies and Best Practice, Published 2009 by Practising Law Institute Press.
- American Bar Association – National Institute on White Collar Crime 2008
- Cybex Europe – 2007
- eSecurity Magazine
- Certified Forensic Hacking Investigator
- Informatics Computer Education Centers
- Government Security News

Title

- “Man And Machine: A Look Forward Into The Future Of eDiscovery”*
- “Machines Versus Humans In E-Discovery – Strengths And Weaknesses”*
- “Control – Alt – Delete”*
- Investigative Computer Forensics*
- “National Cyber Corps: Recruiting the Best”*
- “Fact Finding in the Digital Age”*
- “Avoiding the Disclosure of Intermingled Data”*
- “Managing European Data Collections”*
- “Computer Forensics in Asia”*
- Editor of Official Courseware*
- Computer Forensic Courseware*
- “Computers and Terrorists”*

- OnlineSecurity.com *“California Law SB 1386 Impacts Global Business”*
- Association of Trial Lawyers of America *“Discovery of Insurance Industry Computer Systems”*
- Asia Law & Practice *“Computer Forensics: A Primer for Recovering Electronic Evidence”*
- Corporate Secretary Magazine *“Overview of Online Security and Privacy Issues: Preparing and Responding to Intrusions”*
- OnlineSecurity White Paper *“Network Security: Intrusion Detection Response for Enterprise Networks”*
- The Life and Death of a Dotcom in China *“Cyber Crime Reads Its Ugly Head”*

Professional Associations and Affiliations

- Consortium of Digital Forensic Specialists *Member – Ethics Committee*
- RSA / ESAF (Executive Security Action Forum) *Member*
- The Sedona Conference Working Group 1: Electronic Document Retention and Production *Member*
- The Sedona Conference Working Group 6: International Electronic Information Management, Discovery and Disclosure *Member*
- Boy Scouts of America *Member*
- 2011 LA Leadership Event Blue Ribbon Committee
- Association of Information Technology Professionals *Member*
- Academy of Court-Appointed Masters *Fellow*
- High Tech Crime Consortium *Member*
- Association for Enterprise Information *Member*
- Forensic Expert Witness Association *Member*
- Practicing Law Institute *Faculty*
- Presidential Task Force on CyberCrime *Member*
- State of California – Insurance Fraud Task Force *Past Director – Technology Committee*
- FBI / Infragard – National *Past Pacific Rim Director*
- FBI / Infragard – Los Angeles Chapter *Past President*
- Secret Service Electronic Crimes Task Force *Member*
- WestLaw / Thompson Publishing *Writing Faculty*
- California Judicial Council’s Sub-Committee on Electronic Evidence *Member*
- American Bar Association *Member*
- 2011 Planning Committee
- Pretrial Practice and Discovery Committee
- China Law Committee
- Anti Corruption Committee
- Committee on CyberSpace Law
- Open Security Exchange *Founding Member*
- USC School of Information Technology Industry Advisory Board *Founding Member*
- Electronic Commerce Council *Past Chairman of the Advisory Board*
- Rotary International (LA5) *Member*
- Independent Power Producers Forum *Delegate*
- Pacific Water Council *Past Member*

- Association of Internet Professionals *Past Corporate Member*
- Information Security Systems Association *Member*
- Association of Certified Fraud Examiners *Member*
- High Tech Crime Investigators Association *Member – Asia Pacific Chapter*
- Strategic Alliance for Enforcement (SAFE) *Past Member*
- Culver City Police Department
- Taiwan Privacy Association *Founding Member*

Education

Santa Monica College, Santa Monica, CA
Major: Political Science

Gemological Institute of America, Santa Monica CA
Degree: JMG (Jewelry Management Graduate)

Certifications and Commendations

Commendation from the Government of the Peoples Republic of China, Bank of China
CHFI: Certified Hacking Forensic Investigator
Commendation from the Government of Abu Dhabi, United Arab Emirates
Commendation from the Government of Malaysia, Judicial Training Academy

Advisory and Boards of Directors

Dapict, Inc. (Los Angeles) *
EC Council, Inc. (New York) *
Kornerstone, Ltd. (Hong Kong) *
Leadership for Life Academy (Shanghai)
Odessa Philharmonic Orchestra (Odessa)
American Music Ensemble of Vienna (Vienna)
U.N World Peace Bell Foundation (Hiroshima)
Los Angeles Master Chorale / Los Angeles Music Center (Los Angeles)
* Current

Prior Work Experience

2004 – 2008

Director

Navigant Consulting, Inc. (NYSE: NCI) – Los Angeles and New York

Director of the firms Information Technology Investigations Practice and member of the Discovery Services management committee. Provided electronic discovery, computer forensics and investigative consulting for multinational corporations involved in disputes, internal investigations or governmental inquiries. Responsibilities included Directing the firm's European Union Data Privacy Monitoring, Developing and Managing Computer Forensic Laboratories throughout the United States and in foreign jurisdictions. Directed complex electronic discovery matters in the domestic market as well as throughout Asia and Europe. Managed significant matters related to issues such as: Stock Options Backdating, Theft of Trade Secrets, Software Failures, CyberCrime, Insurance Industry Bid Rigging, SEC and DOJ Investigations, International Due Diligence and numerous expert witness engagements.

1997 - 2004

President

Online Labs, Inc. – Los Angeles

Software integration, Email hosting, Web application development and hosting, online marketing and developer of custom database driven technology solutions for online and traditional applications and businesses. Developed, managed and hosted large scale secure web enabled projects for clients including; The State of California, The Government of Hong Kong, Warner Brothers, Disney Studios, Toyota, Porsche, Veterinarian Centers of America, Latham and Watkins, Kroll and Associates, California Manufacturing Technology Center, The Government of Alsace France, ICN Pharmaceuticals and The Richemont Group.

1998 - 2004

President and Founder

Online Security, Inc. – Los Angeles

Information Technology Investigations and Computer Security firm specializing in the protection of digital assets, computer forensics and the analysis of online fraud. Pioneered numerous groundbreaking investigative techniques which resulted in the successful conclusion of investigations and litigation valued in the hundreds of millions of dollars.

1995 - 1997

Publisher and Editor in Chief

PhotoRents Magazine – Los Angeles

PhotoRents at America Online

Natural Living at America Online

1992 - 1994

Director of Sales and Marketing

American Product Development, LTD - Peoples Republic of China

1991- 1992

Director of Sales and Marketing

Oleg Cassini Products, LTD – Japan

1990 – 1991

Director of Sales and Marketing

Les Quad Products, Inc. – France

1986 – 1990

Vice President

Laykin et Cie at I.Magnin & Co. – Beverly Hills

1984 - 1986

Director of Marketing and Advertising

Laykin et Cie at I.Magnin & Co. – Beverly Hills

1982 - 1984

Sales Person

Laykin et Cie at I. Magnin & Co. – Beverly Hills

Expert Witness and Special Master Case List

CASE NUMBER	CASE NAME
United States District Court, Northern District of California Case No. CV-09-5749-BZ	Cataphora, Inc. vs. Jerrold Seth Parker, Dawn M. Barrios, Victor Manuel Diaz, Ben Gordon, Daniel E. Becnel, Jr., Ervin Amanda Gonzalez, Hugh P. Lambert, Arnold Levin, Christopher Seeger, Scott Weinstein, Gerald E. Meunier, James Robert Reeves, Bruce William Steckler, Russ M. Herman, Leonard Davis, and Does 1 - 50, inclusive.
United States District Court, Central District of California, Southern Division Case No. SACV10-1656 JST (RZx)	Bryan Pringle v. William Adams, Jr.; Stacy Ferguson; Allan Pineda; and Jaime Gomez, all individually and collectively as the music group The Black Eyed Peas, et al.
United States District Court, Western District of Washington, Seattle Case No. C10-268 TSZ	*Straitshot Communications, Inc. v. Telekenex, Inc., Mark Prudell and Joy Prudell, Mark Radford and Nikki Radford, Joshua Summers and Julia Summers, Anthony Zabit and Jane Zabit, Brandon Chaney and Jane Doe Chaney, Mammoth Networks, LLC, and Brian Worthen and Jane Doe Worthen
Superior Court of the State of California, County of San Bernardino, Central District Case No. CIVSS-814598	Tracy A Yarbough-Moore v. Addus Healthcare, Inc.
Superior Court of the State of California, County of San Diego Case No. 37-2009-00086022-CU-PO-CTL	Jeff Fratilla v. So Relax California, Inc., et al.
Superior Court of the State of California, County of Los Angeles, Central District Case No. BC385368	The Estate of Joseph Omar Cosina et al v. Crash Mansion LA.
United States District Court, Southern District of California Case No. 09'CV0723	** Ann Capozza, Anthony Capozza, Capstone Investments, Capstone Group LLC, and Capstone Partners v. Steven Martinez, Kenneth Goertz, Goertz & Martinez, CPA, EFTPS-2007, Inc., EFTPS-2008, Inc., Goertz & Martinez, CTA, Inc., and DOES 1-10
United States District Court, Central District of Florida, Orlando Division Case No. 6:08-cv-1872-ORL-31GJK	Federal Trade Commission vs. CyberSpy LLC and Tracer Spence.
United States District Court for the Southern District of Texas, Houston Division Case No. 4:2008cv00338	*Control Components, Inc. vs. Juan Ricardo Simeoni, David Minoofar, Vinay Nagpal, Sanjay Sherikar, Koso America Inc., Nihon Koso (Japan) Ltd. and Baro Control Valve, Inc.
United States District Court, District of Connecticut Case No. 3:07CV171	*Sedona Corporation vs. Open Solutions Inc.
United States Securities and Exchange Commission	SEC vs. (Confidential)

CASE NUMBER	CASE NAME
Superior Court of the State of California, County of Los Angeles Case No. VC 047347	Chi Ming Fan vs. Horizon Grocers LLC, A California Limited Liability Corporation and Carmanita Corporation, A California Corporation
Superior Court of the State of California, County of San Diego Case No. GIC 853833	*Baja Bound Insurance Services Inc., a California Corporation vs. Richard Allen Crews Individually dba Mexbound.com, Brian Archambo Individually and dba Mexbound aka Mexbound.com; Baja-Mex Insurance Services Inc., a Corporation
United States District Court, District of Minnesota Case No. 06-2446 JRT/FLN	*NAU Holding Company LLC, a Minnesota Limited Liability Company vs. Crop 1 Insurance Direct Inc., a Wyoming Corporation, Farm Bureau Mutual Insurance Company, an Iowa Corporation and Ecliptic Technologies Inc., a North Dakota Corporation
Superior Court of the State of California, County of Los Angeles Case No. BC 336916	Burnie Allen, an individual, as an individual and as Co-Trustee and Beneficiary of the Burnie Allen Trust v. Gary Allen, an individual and as Co-Trustee and Beneficiary of the Gary and Robin Allen Family Trust; Robin Allen, as Co-Trustee and Beneficiary of the Gary and Robin Allen Family Trust; Ampac Insurance Marketing, Inc., and Does 1 – 5 inclusive
CA Dept of Justice before the Division of Medical Quality Medical Board of CA, Dept of Consumer Affairs State of CA Case No 11-04-162836	Gloria L. Castro, Deputy Atty General of the State of CA, CA Dept of Justice Attorney for Complainant v. Lawrence Koplin, M.D.
CA Dept of Justice before the Division of Medical Quality Medical Board of CA, Dept of Consumer Affairs State of CA Case No 05-2001-124743	Bill Lockyer, Atty General of the State of CA, John DeCure, Deputy Attorney General, CA Dept of Justice Attorneys for Complainant v Gary J. Ordog, M.D., Newhall CA
US District Court for the Southern District of California Case No. 04 CV 1479 H (BLM)	TrekEight, LLC, a California Company limited liability company v. Symantec Corporation, a Delaware Corporation
Supreme Court of the State of New York County of New York	*Genserve, Inc. v. Unity International Inc., Joseph Belmonte Sr., Joseph Belmonte Jr., James Guida, & William Randel
US District Court for the Northern District of Illinois, Eastern Division Civil Action No. 03 CV 07882	Evelyn Clark, on behalf of herself and all other others similarly situated v Experian Information Services d/b/a Consumerinfo.com, Inc.
US Western District of Oklahoma Case No. CIV-04-1013-W	Robert H.Braver, an individual v Ameriquest Mortgage Company, a Delaware corporation; Innovative Marketing, Inc., d/b/a Lead Extreme, a Washington corporation; The Loan Page, Inc. a Delaware corporation; Go Aplly, Inc., d/b/a Eleadz, a Nevada corporation, John Does 1 -50

CASE NUMBER	CASE NAME
Circuit Court of the First Judicial District of Hinds County, Mississippi Civil Action No. 251-04-642CIV	*Eaton Corporation; Aeroquip-Vickers, Inc.; Eaton Hydraulics, Inc. f/k/a Vickers, Inc.; & Eaton Aerospace, LLC v Jeffery D. Frisby, Individually; Kevin E. Clark, Individually; James N. Ward, Individually; Douglas E. Murphy, Individually; Rodney L. Case, Individually; Billy D. Grayson, Individually; Frisby Aerospace LLC, Frisby Aerospace Inc n/k/a Four Seventeen Aerospace, Inc; Triumph Group, Inc.; The Triumph Group Single Business Enterprise; and certain Doe Defendants numbers 1 – 150
US District Court Southern District of New York Case No. 05 CV 5597 (GEL) (DFE)	*Solar Tours Inc, v Luis Macias d/b/a Tournet Systems v Rafeal A. Chieca & Rudy Tan a/k/a Rudy Fnu
US District Court Eastern District of Michigan, Southern Division Case No. 05-72031	*Easton Sports, Inc., a California corporation v Warrior Lacrosse, Inc., a Michigan corporation and New Balance Athletic Shoe, Inc., a Massachusetts corporation
US District Court Southern District of New York Case No. 04-CV-00604 (CSH) (DFE)	Logicom Inclusive Inc.d/b/a Logicom Inc.; Stephen Boriotti and Richard Rosen v W.P. Stewart & Co., William P. Stewart; John C. Russell; Edward Butler; & Rocco Macri
American Arbitration Association Case No. 7311700207 03 ARC	Laguna Coast Publishing, Inc. dba Performance Racing Industry v. Gomembers, Inc.
US District Court of Eastern Michigan Case No. 02-70906	*Compuware Corporation, a Michigan corporation vs International Business Machines Corporation, a Delaware corporation
Orange County Superior Court Case No. 02CC00003	Peggie Jo Brown, Rick Hornbeck, and Laurel Nevans v. Erie Insurance Exchange Company, The Chubb Group, Federal Insurance Company, Salor & Hill Company
Los Angeles Superior Court Case No. BC 280222	*McFarlin Graphic Systems, Inc. dba McFarlin Group vs. Shell Oil Company, et al
US District Court of Maryland Northern Division Civil No. AMD 03 CV 3108	Federal Trade Commission v. D Squared Solutions, LLC, a California limited liability company; Anish Dhingra, individually and as an officer of D Squared Solutions, LLC; Jeffrey Davis, individually and as an officer of D Squared Solutions, LLC
Orange County Superior Court OCDA Case No. 01F11792	People of the State of California vs. Timothy Chavez
US District Court for the Eastern District of California Case No. CR-F-03-5142 OWW	United States of America vs. Terry L. Walton and Everett Rabbon, Jr.
US District Court of California Case No. CA-1193-A (Lee)	*Physicians Interactive (a division of Allscripts, LLC v. Lathian Systems, Inc. Stephan Martinez and John Does 1-10

CASE NUMBER	CASE NAME
U.S. District Court – Eastern District of New York Case No. 02-CIV-04195 (DGT) (RLM)	Elizabeth De Chanval Pellier against British Airways, Plc., Irving Rudowitz, Rosemary Rogers, Dan Driscoll, and Doug Hutchenson, individually, and as employers, agents, and as abiders and abettors
U.S. District Court – Southern District of California Case No. 00CV1199 BTM (JFS)	*India World Communications Private Limited, v. ASAP Solutions, Inc., Hassan Jacob and Victor George
U.S. District Court – Central District of California Western Division Case No. 02-04299 DT (Cox)	*/**Software Center, Ltd., trading as Gambling.com v. Unified Productions, Inc., a California corporation; Jason Yard, an individual; James Taylor, an individual; Internet Traffic Solutions Management Pty Limited, trading s ITS Management, an Australian corporation; Ryan McFadden, an individual; and John Does 1-100, inclusive
U.S. District Court Central District of California Case No. 03-1504 FMC (Ex)	*Honeywell International Inc. and Honeywell Intellectual Properties, Inc. v. ABB Inc., ABB Inc. – BU Turbocharger and ABB Turbocharger Company
Superior Court of the State of California For the County of Orange Case No. 01CC08414	B.J.M.V., Inc., dab Southern Pacific Coatings; Arbor Media, Inc., and Pueblo Computers, Inc. vs. Paul J. Tolbert; Joyce K. Tolbert; Tolbert Living Trust Dated March 27, 1990; Propone Satitpunwaycha; 3-Star T-Shirts; Mario Guerra; Scalon, Guerra and Jacobson, and Does 1 through 20, et al.

* Cases involving the theft of Trade Secrets and / or Intellectual Property theft

** Special Master in Case