How to Depose a Chief Information Security Officer

Today's Speakers:

Daniel B. Garrie, Esq., Co-Founder, Law & Forensics, Mediator, Arbitrator, and e-Discovery Special Master, JAMS

Michael Yellin, Member, Cole Schotz P.C.

Una Dean, Partner, Fried Frank

(c) Global Cyber Institute 2019. All Rights Reserved.

This Photo by Unknown Author is licensed under CC BY-NC-ND

Disclaimer

- This is not legal advice nor should it be considered legal advice.
- This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.
- This presentation is offered for educational and informational uses only.



(c) Global Cyber Institute 2019. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Co-Founder, Law and Forensics;
Mediator, Arbitrator, and e-Discovery Special Master, JAMS



Michael Yellin
Member, Cole Schotz P.C.



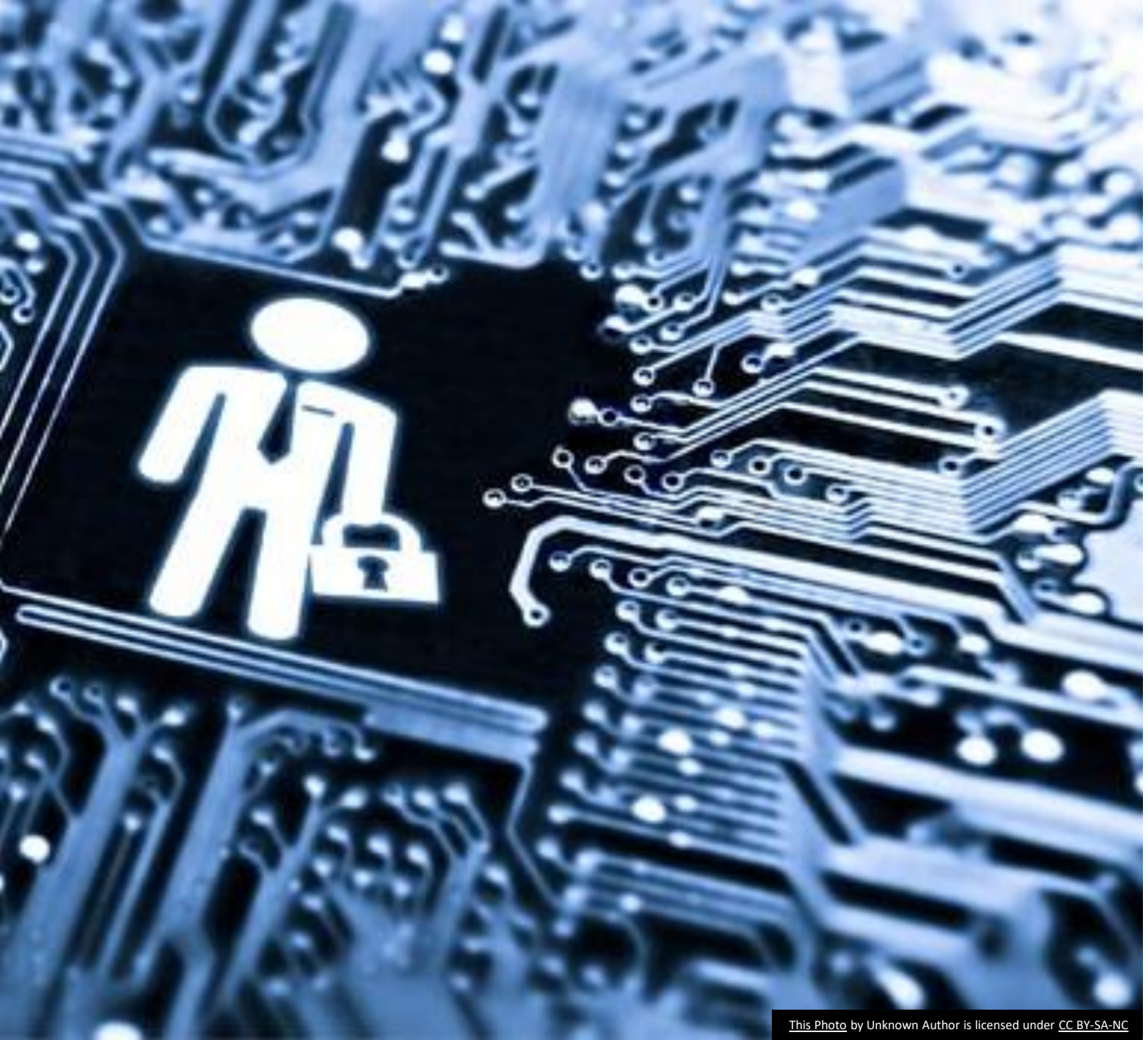
Una Dean
Partner, Fried Frank

(c) Global Cyber Institute 2019. All Rights Reserved.

Agenda

1. What is a Chief Information Security Officer?
2. What is a deposition?
3. Performing Technical Depositions
4. Apex Doctrine
5. Techniques for Using Expert Consultants
6. CISO Liability Case Law

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA-NC

What is a Chief Information Security Officer?

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC-ND

What is a chief information security officer (CISO)?

- A CISO is a senior-level executive responsible for operational security, infrastructure security and employee access management for information technology resources.
  - Stated differently, the CISO is responsible for ensuring that the firm's electronic data is adequately protected.
- The CISO may also be referred to as the chief security architect, the security manager, the corporate security officer or the information security manager, depending on the company's structure and existing titles.

(c) Global Cyber Institute 2019. All Rights Reserved.

CISO Roles and Responsibilities



- Instead of waiting for a data breach or security incident the CISO is tasked with anticipating new threats and actively working to prevent them from occurring. The CISO must work with other executives across different departments to ensure that security systems are working smoothly to reduce the organization's operational risks in the face of a security attack.

This Photo by Unknown Author is licensed under CC BY-NC-ND

(c) Global Cyber Institute 2019. All Rights Reserved.

Responsibilities: Broadly Defined

Protect, Shield, Defend, Prevent	Monitor, Hunt, Detect	Respond, Recover, Sustain
		

Govern, Manage, Comply, Educate, Manage Risk



(c) Global Cyber Institute 2019. All Rights Reserved.



What is a deposition?

This Photo by Unknown Author is licensed under CC BY-SA

(c) Global Cyber Institute 2019. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY-SA-NC

What is a deposition?

- A deposition is a valuable discovery tool that a party nay use for many reasons, including to learn the facts of a case and to elicit testimony for use in settlement discussions, in dispositive motions, or at trial.

(c) Global Cyber Institute 2019. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY-SA

Who can be deposed?

- Any person: Fed. R.Civ.P. 30(a)
- Witnesses and non-witnesses:
  Fed. R.Civ.P. 26(b)(1)
- Organizations through designee(s):
  Fed. R.Civ.P. 30(b)(6)
- Testifying experts: Fed. R.Civ.P. 26(b)(4)

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Why take a deposition?

- Find out what you don't know
  - Allows you to fill in any holes
- Confirm what you think you know
  - Lock in testimony
  - Discover and deal with discrepancies
- Test out legal/factual theories
  - Do you have facts to support your theories?
  - Are there other, better theories?
  - Are there problems with any theories that need to be addressed
- Figure out and address what the other side knows and their theories/supporting facts

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

What are some reasons for taking a deposition?

- To preserve testimony
  - Lock in testimony in case of deviations at trial
  - Substitute for live testimony if witness will be unavailable at trial
- To facilitate settlement
  - Chance to evaluate witness and attorney
  - Open lines of communication with opposing counsel
  - Establish favorable testimony

(c) Global Cyber Institute 2019. All Rights Reserved.



Questions Asked at Most Depositions

- Background on the witness (education, employment, prior litigation history)
- A detailed review of the facts at issue, including the:
  - Who?
  - What?
  - Where?
  - When?
  - Why?

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Performing Technical Depositions

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Prepare Thoroughly

- Before the deposition, learn as much as you can about the company's information security protocols, the CISO's role and responsibilities, prior roles the CISO has held (at the company and elsewhere), and prior incidents at the company
- Sources of the information can often include public records, in addition to discovery already obtained

(c) Global Cyber Institute 2019. All Rights Reserved.



Do Your Homework

- Discovery is the most time-consuming and expensive way to learn anything. Don't make the deposition the start of your education about the company, the witness, or information security protocols in general.
- It is critical to work with your own experts to determine the nature and scope of the questions to ask.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC-ND

Ask Why

- The question lawyers fear to ask on cross-examination is often the best one you can ask in a discovery deposition: “Why?” If you want to learn your opponent’s theory of the case, and get a sense of how well the expert can present it, ask “why” questions. The answers also will help tell you what to stay away from at trial.
- For example, during a deposition, ask the CISO to help counsel understand difficult concepts. It gets the witness to open up and gives her a better idea of the witness’s real approach to the case.

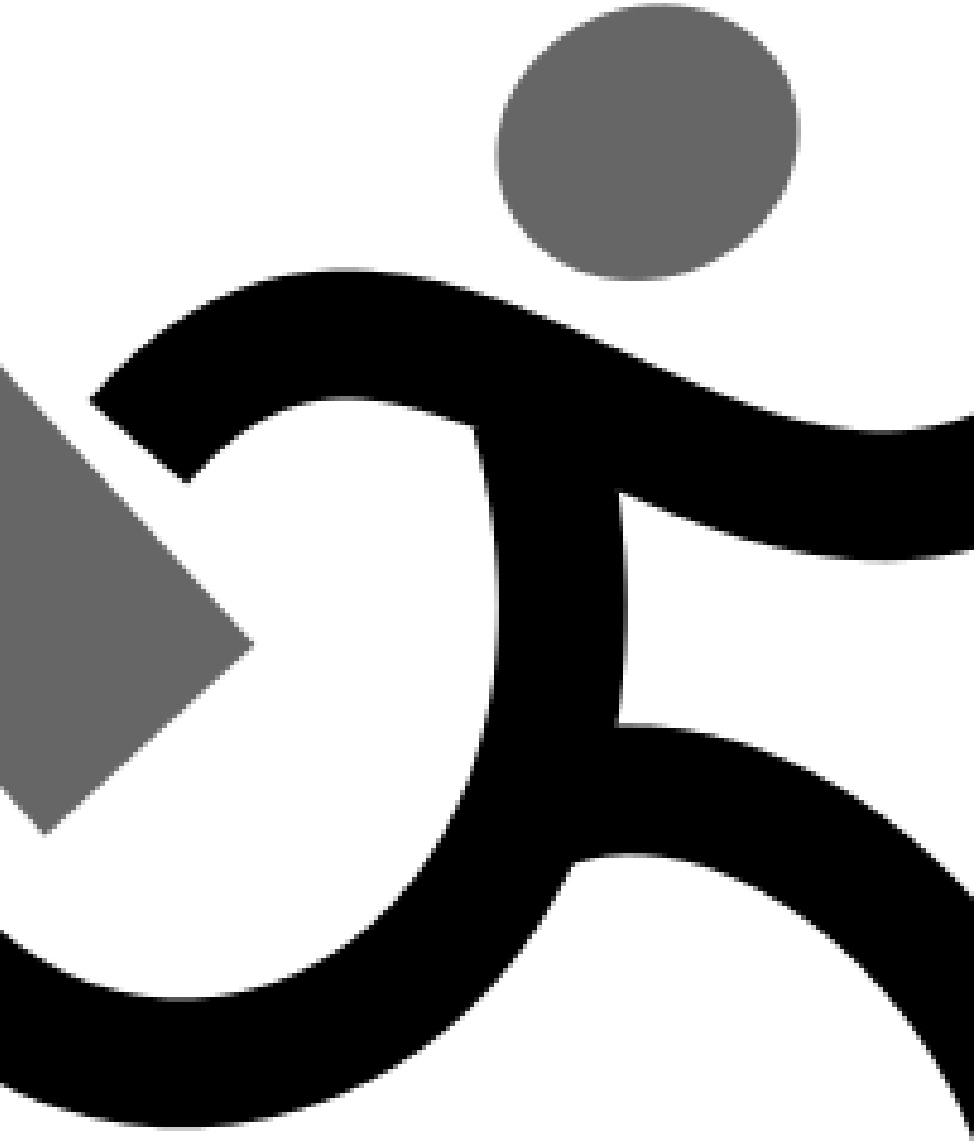
(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

Apex Doctrine

(c) Global Cyber Institute 2019. All Rights Reserved.



What is the Apex Doctrine?

- Apex depositions occur when a party seeks to depose an individual at the top of a corporate hierarchy.
- A distinct line of authority has emerged under Federal Rules of Civil Procedure 26(c)(1).
- Apex depositions often provoke disputes as corporations almost uniformly object to their occurrence.
- Some argue apex depositions are an abusive discovery tactic used to leverage settlement, while others allege they are a legitimate means to reveal discoverable information.

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-NC-ND

What is the Basis of the Doctrine?

- Under this doctrine, a court may protect a high-level executive from the burdens of a deposition under any of the following circumstances:
  - The executive has no unique personal knowledge of the disputed issues (Unique Personal Knowledge).
  - The information sought from the executive can be obtained from:
  - another witness; or
  - an alternative discovery method (Alternate Means of Discovery).
  - Sitting for the deposition is a severe hardship in light of the executive's obligations to the company (Undue Hardship).

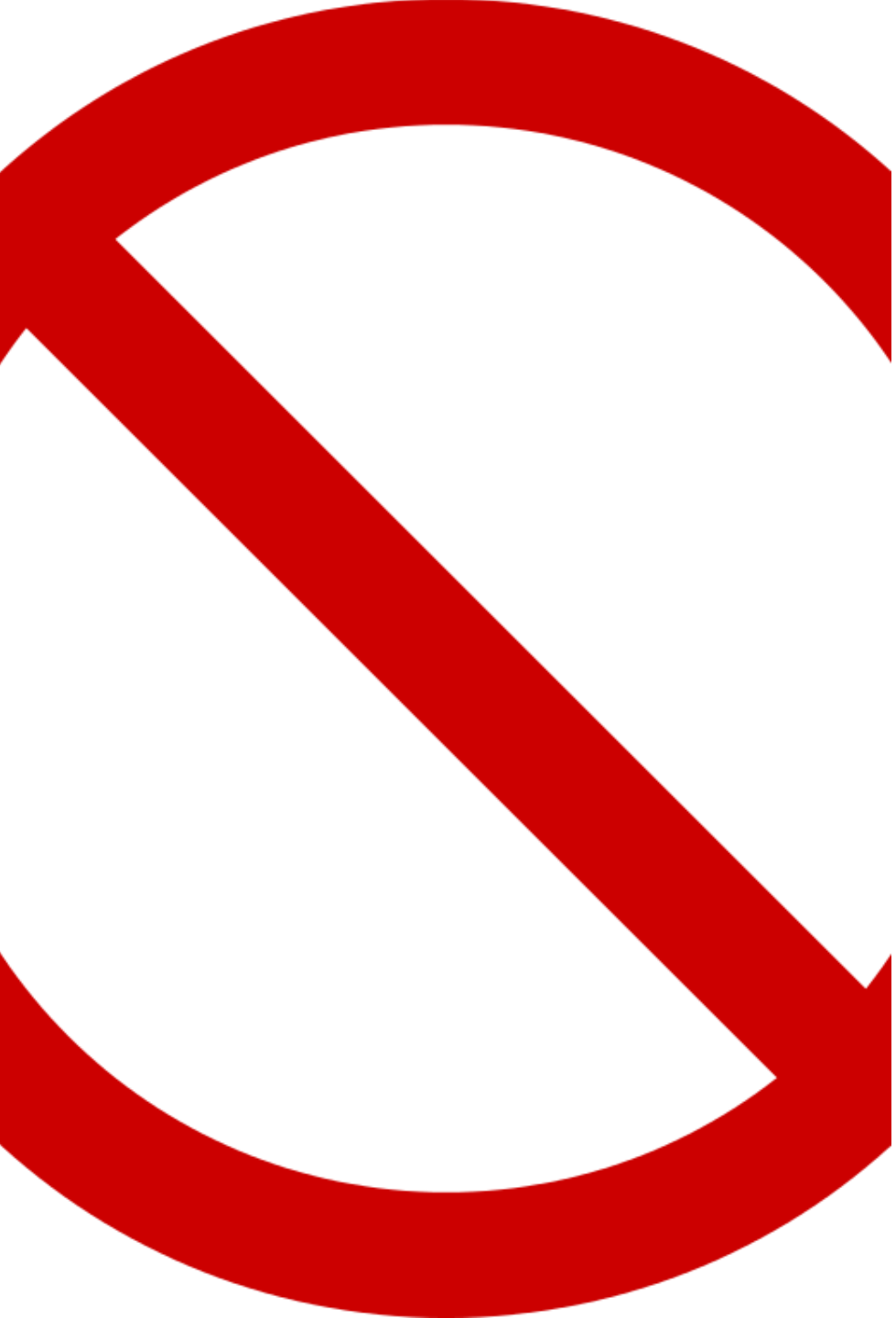
(c) Global Cyber Institute 2019. All Rights Reserved.



It's Not Universally Applied in Jurisdictions

- Some courts have not recognized the apex doctrine as a distinct rule and have instead reached similar conclusions on the basis of Rule 26(c) alone.
- These courts reason that because the language of Rule 26 allows a court to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, there is no need to apply a special doctrine. Regardless of whether a court expressly adopts the terminology "apex doctrine," the inquiry is the same.

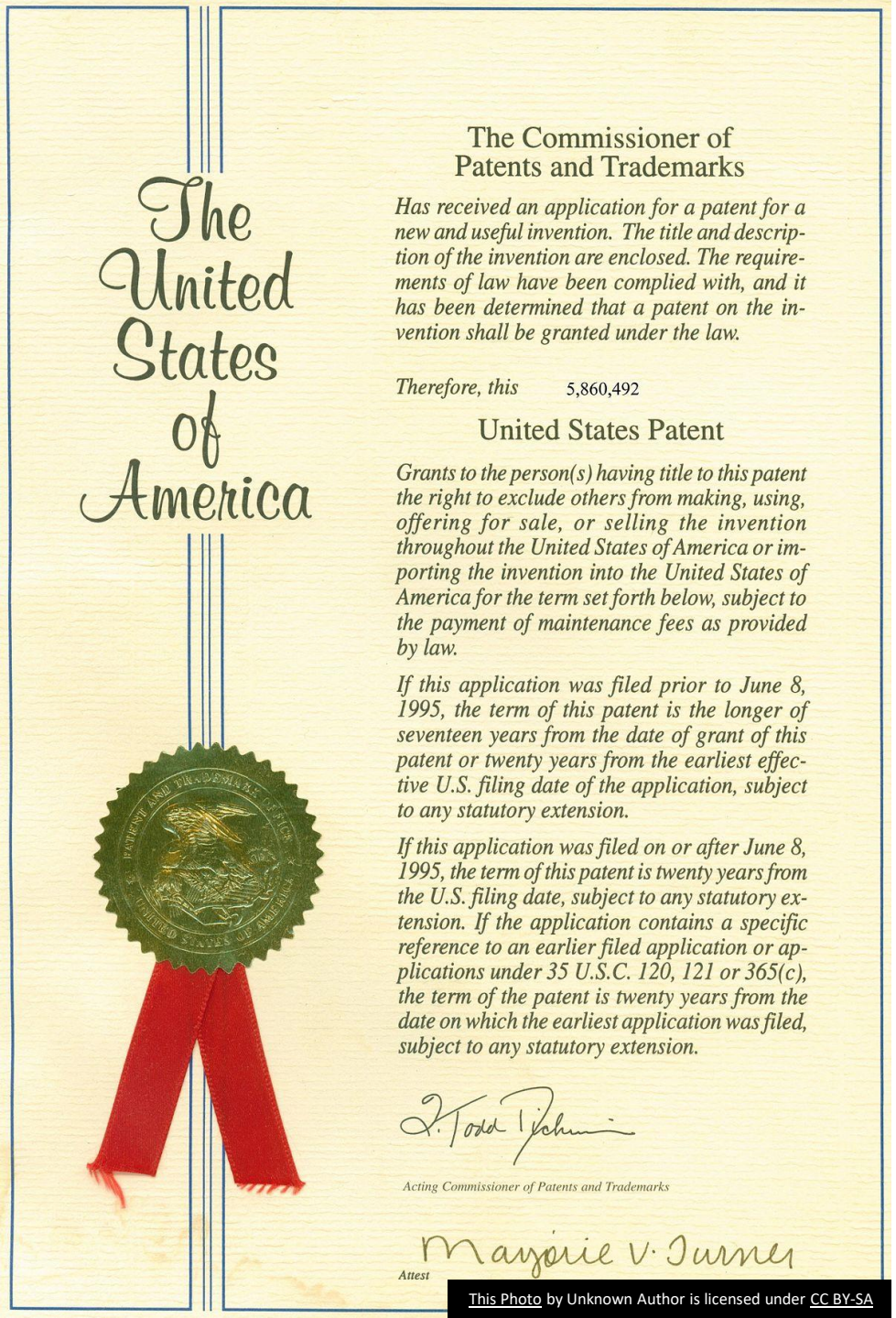
(c) Global Cyber Institute 2019. All Rights Reserved.



It's Not Universally Allowed in All Types of Depositions

- The apex doctrine does not apply to Rule 30(b)(6) depositions.
- Under Rule 30(b)(6), the responding party is entitled to choose which witnesses will appear to answer questions regarding the subject matters identified in the notice. Accordingly, the responding party simply needs to produce a witness of its choosing—not necessarily an apex witness—to answer the questions.

(c) Global Cyber Institute 2019. All Rights Reserved.



Example

- In a patent-licensing dispute pending in the Southern District of California, Magistrate Judge Nita L. Stormes applied this doctrine to prevent the deposition of one of the defendant's former corporate executives. *Rembrandt Diagnostics, LP v. Innovacon, Inc.*, No. 16-cv-0698 CAB, 2018 WL 692259, at *6–7 (S.D. Cal. Feb. 2, 2018). In fact, it wasn't a particularly close call.
- The witness had been employed as only one of only three global presidents for an international, publicly traded company. Moreover, the plaintiffs had yet to depose lower-ranking employees within the company. The only real wrinkle was that the corporate executive had since left the company. Judge Stormes, however, gave that argument short shrift and relied on a number of cases extending the apex-deposition doctrine to former executives.

This Photo by Unknown Author is licensed under CC BY-SA

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY

Techniques for Using Expert Consultants

(c) Global Cyber Institute 2019. All Rights Reserved.



Non-testifying Experts - Consultants

- In some cases, it is strategically beneficial for a party to retain experts that will not testify. Federal Rule 26(b)(4)(D) outlines the rules for non-testifying experts.
- Attorneys should retain non-testifying consultants early because they can assist in the identifying of testifying experts.
- Consultants can also help with preparation of interrogatories and document requests as well as preparing for the opposing experts' depositions.
- While consultant's materials are not typically discoverable, a consultant's work cannot be protected from disclosure if it is the complete basis of a testifying expert's opinion.

See The Sedona® Conference, *Best Practices for the Selection of Electronic Discovery Vendors: Navigating the Vendor Proposal Process*

(c) Global Cyber Institute 2019. All Rights Reserved.



Plan Ahead

- Forensic and technical experts can assist in drafting accurate, specific, effective interrogatories, deposition questions, and requests for production.
- Venturing in the world of electronically stored information without a sufficient background or training can result in discovery requests which generate squabbles over technical terminology, miss or request information from obscure data sources, cause dumping of meaningless data, and create unintended over-breadth.
- Thoughtful and forward-thinking requests lead to faster, targeted, and more effective discovery requests. The forensic or technical expert can help plan and even attend depositions.

(c) Global Cyber Institute 2019. All Rights Reserved.



Verifying, Developing, and Advising Production

- Technical expert can also assist in verifying the completeness, authenticity, and responsiveness to the production requests.
- Experts can also assist in developing search and examination strategies for the produced data, and help develop protocols for examining or sampling data bases or examining computer hard drives and other devices holding electronically stored formation.
- Experts can provide advice on the production format and the production specifications that will accompany load files. A serious but common mistake in electronic discovery is the failure to negotiate the specifics of the document production and load file.

(c) Global Cyber Institute 2019. All Rights Reserved.



CISO Liability
Case Law

(c) Global Cyber Institute 2019. All Rights Reserved.



This Photo by Unknown Author is licensed under CC BY-SA

U.S. Office of Personnel Management (OPM)

- **Facts:** The CIO of the U.S. Office of Personnel Management (OPM), Donna Seymour, was named in a lawsuit for failing to protect the personal data files of millions of government employees and federal contractors. As part of a massive breach of governmental computer systems, the highly personal data of at least 21.5 million people – including addresses, legal, health, mental and financial history – was exposed and taken. Essentially, every person given a government background check for the last 15 years, as well as their spouses and friends, are now at risk of having their private and personal information misused. An earlier breach at the OPM had compromised the "sensitive" personnel data of another 4.2 million federal employees. Ms. Seymour has already been subject to intense grilling by Congress, but it is her legal exposure that should concern her and every CIO and CISO.
    - The lawsuit against Ms. Seymour seeks to hold her personally liable for these OPM breaches, advancing claims for negligence, privacy violations, and other causes of action.
- **Holding:** U.S. District Judge Amy Jackson granted the government's motion to dismiss the case citing the federal government's immunity from lawsuits and the difficulty of legally proving harm as the result of having personally identifiable information (PII) stolen.

(c) Global Cyber Institute 2019. All Rights Reserved.



Questions?

(c) Global Cyber Institute 2019. All Rights Reserved.

Contact Us



Daniel B. Garrie
Email: daniel@lawandforensics.com
dgarrie@jamsadr.com
Phone: 855-529-2466
URL: www.lawandforensics.com



Michael Yellin
Email: myellin@coleschotz.com
Phone: 201-525-6258
URL: http://www.coleschotz.com/



Una Dean
Email: Una.Dean@friedfrank.com
Phone: 212-859-8851
URL: https://www.friedfrank.com/

(c) Global Cyber Institute 2019. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics – Executive Managing Partner
JAMS – Special Master, Neutral, Arbitrator
Contact:
W: (855) 529-2466
M: (206) 228-5457
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

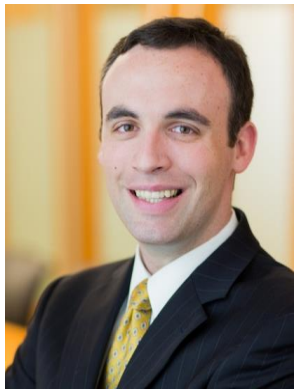
LAW & FORENSICS
Computer Forensics, E-Discovery, Cyber Security

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, he successfully built and sold several technology start-up companies. Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States. In particular, Daniel recently located and recovered deleted files in both private and public cloud computing environments using his patented software, Forensic Scan. This investigation took less than forty-eight hours to clean and recover the data from the servers of a cloud-hosting provider that was compromised by a malicious cyber-attack. Thanks to the Forensic Scan technology, that Daniel co-invented and patented (US9990498B2 and US9990497B2), and his own expertise, Daniel and his team was able to identify the source of the breach and remediate the problem in record time.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases, including one involving the embezzlement of millions of dollars from a large non-profit. Daniel was able to perform a thorough analysis of the alleged embezzlers' phone and computer, despite the embezzlers' attempts to wipe them, and identify concrete evidence of the embezzlement to a jury. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cyrptocurrency, and complex software and technology related disputes. Some of the major cases for which he has served as an e-discovery special master, or forensic neutral include: *Hougan vs. City of Newport Beach, No. 30-2012-00582855* (Super. Ct. Cal. 2014)*; Small v. University Medical Center of Southern Nevada, 2014 WL 4079507*(D. Nev. 2014)*; C.D.S. Inc. v. Zelter and Amazon Web Services, Inc.*, (S.D.N.Y. 2016); *Jawbone, Inc. v. Fitbit Inc.* et al (Super. Cal., S.F. County 2018). In addition to his vast litigious experience, Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) Global Cyber Institute 2019. All Rights Reserved.



Michael Yellin
Cole Schotz P.C. – Member
Contact:
W: 201-525-6258
E: myellin@coleschotz.com
URL: http://www.coleschotz.com/

Cole Schotz P.C.

A litigator by trade, Michael Yellin values the role of trusted friend and advisor – someone who can be relied on to assist no matter the issue. Mike views a strong relationship with his clients as essential to anticipating and addressing their needs, whether legal, business, or otherwise. As a result, Mike's clients turn to him as a counselor and problem solver both inside and outside of the courtroom. Oftentimes, complex matters require a range of resources. In such cases, Mike seamlessly assembles the best team by drawing on the firm's diverse group of attorneys – never stepping away but remaining the client's point of contact, accessible at any time.

Mike has served as lead counsel in a myriad of matters, from creative transactions to expand a client's business to emergent "stop the bleeding" situations and critical litigations. His clients appreciate his broad experience and the way in which he applies that experience to guide them in maximizing opportunities while minimizing expense and exposure.

Examples of Mike's recent successes include:

- Obtaining an emergency court order directing a major hospital's former employee, her spouse, and her new employer to provide the hospital's forensic expert with immediate access to personal computers, phones, and e-mail accounts for timely sanitizing a potential HIPAA breach.
- After two years of litigation and several days of trial, securing dismissal of 12 fraud-based claims asserted against a general contractor by a large subcontractor.
- Assisting a client with the acquisition of a $19 million building in Queens, New York, which is to be converted into a mixed-use medical office facility constituting approximately 98,000 square feet.
- Representing a New Jersey private equity fund in recovering its entire investment following the Chapter 11 filing by a New York borrower.
- After a 5-day hearing before a FINRA arbitration panel, obtaining a unanimous ruling in favor of our client as to all issues, including a denial of the adversary's $21 million claims.

(c) Global Cyber Institute 2019. All Rights Reserved.



Una Dean
Fried Frank – Partner
Contact:
E: Una.Dean@friedfrank.com
URL: http://www.friedfrank.com/

FRIED FRANK

Una A. Dean is a partner in Fried Frank's White Collar Defense and Government Investigations Practice, resident in the New York office.

Ms. Dean concentrates her practice on white collar criminal defense, internal investigations, cybersecurity and related civil litigations. She represents public, multinational corporations and financial institutions in conducting internal investigations involving allegations of fraud and other misconduct. She also routinely advises corporate clients on issues relating to cybersecurity corporate governance, cyber preparedness and incident response.

Prior to joining Fried Frank, Ms. Dean served as an Assistant United States Attorney (AUSA) for the Eastern District of New York (EDNY) from 2010-2017 where she investigated, prosecuted and tried some of the EDNY's most important and high-profile cases across a wide spectrum of practice areas, including money laundering, securities fraud, trade sanctions, and cybercrime. Notably, she secured convictions in seven jury trials and successfully argued numerous cases for the United States Court of Appeals for the Second Circuit.

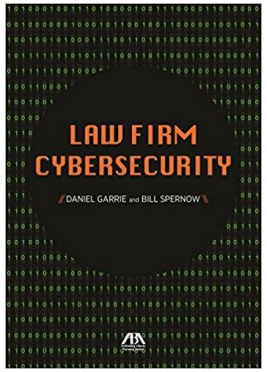
During her time as a federal prosecutor, Ms. Dean served in a number of leadership positions. Most recently, as the Office's Cyber Specialist, she developed the EDNY's current cross-border cybercrime practice and supervised all of the Office's cyber-related investigations and prosecutions. Simultaneously, she served as a Computer Hacking and Intellectual Property Coordinator (CHIP), where she served as counsel in all matters related to technology and evidence collection, including electronic surveillance, encryption and data privacy.

Ms. Dean also worked as an associate at an international law firm from 2004-2005 and 2007-2009, where she advised Fortune 500 corporations and individuals in connection with high profile litigation and global investigations.

(c) Global Cyber Institute 2019. All Rights Reserved.

Additional Reading

Books



Law Firm Cybersecurity



Plugged In: Guidebook to Software and the Law



Software and the Law: Digital Forensic Investigations and E-Discovery



Dispute Resolution and e-Discovery

Articles



Arbitration, Mediation Can Resolve Cyber Coverage Disputes



Spearfishing Can Be Stopped Once You Remove the Bait



Mediators Need to Become 'Bilingual' to Resolve Smart Contracts

(c) Global Cyber Institute 2019. All Rights Reserved.