Legal Ethics for Digital Technology

Speakers:

Daniel B. Garrie, Esq., Co-Founder, Law and Forensics; Mediator, Arbitrator, and e-Discovery Special **David Farkas,** Associate, DLA Piper

David Farkas, Associate, DLA Piper

Douglas Smith, Associate, Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates

Gail Gottehrer, Founder, Law Office of Gail Gottehrer LLC

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

Speakers



Daniel B. Garrie, Esq.
Co-Founder, Law and Forensics; Mediator, Arbitrator, and e-Discovery Special Master, JAMS; Partner, Zeichner, Ellman & Krause LLP



David Farkas
Associate, DLA Piper



Douglas Smith
Associate, Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates



Gail Gottehrer
Founder, Law Office of Gail Gottehrer LLC

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

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) 2019. Global Cyber Institute. All Rights Reserved.

Agenda

1. Cyber Attacks on Law Firms
2. Ethics Rules
3. Bar Associations' Ethics Opinions
4. Real World Examples
5. Where are we now? What comes next?

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



Cyber Attacks on Law Firm

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

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



Why is it critical that firms follow ethical guidelines?

- Law Firms are specific targets for cyber security hacks
- Failure to respond properly to a cyber incident can open a firm to serious ethical issues.

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



Law firms are major targets.

- Law firms have money, house valuable, confidential client information, and are usually not prepared for a cyber security attack.
- “A firm in Toronto saw a six-figure sum stolen from its trust account when a Trojan swiped the firm’s banking passwords.”
- “In one 2016 incident, attackers hit several well-known M&A firms with more than 100,000 attacks over just three months, earning more than $4 million by selling the stolen information.”
- “According to the Logicforce Q4 2017 Law Firm Cyber Security Scorecard, 62% of law firms do not have a dedicated information security professional, less than a third have formal cyber security training programs, and only 41% have formally documented cyber security policies.”

The Barkly Team, *Law Firm Cybersecurity in 2018: Attacks and Audits Add Up* (2018) (last visited Feb. 20, 2019, https://blog.barkly.com/law-firm-cybersecurity-2018-attack).

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



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

What security measures should firms adopt?

- As technology continues to evolve, firms must implement robust security measures, as not doing so means easier access to sensitive information for adversaries.
- Law Firms tend to implement weaker security measures, which provides hackers increased accessibility to sensitive information.
- As a result, law firms are increasingly targeted by hackers seeking client information.

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


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

Who commits these attacks?

- There is a wide variety of hackers with their own skill-sets and motivations

Examples of distinct groups include:

- (1) nation-states
- (2) non-state organizations, including criminal enterprises, terrorist groups, and sophisticated hacker communities
- (3) “lone-wolf” hackers and insiders.

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



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

Firm Liability

- Law Firms may be increasingly liable for client's damages resulting from a cyber attack.
- Statutes can vary widely from state to state on issues such as notification to law enforcement, and Congress has yet to pass a national data breach notification law.
- This means law firms and other businesses that possess private client information on firm networks must be prepared to meet the data breach notification requirements of any jurisdiction in which they do business, including internationally.

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



Ethics Rules

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



Model Rule 1.1- Duty of Competence

- Model Rule 1.1
  - " A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."
- Comment [8]:
  - "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

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



Example

- A lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document.

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



Model Rule 1.4 - Communications

- Model Rule 1.4(a)(3)
  - “A lawyer shall keep the client reasonably informed about the status of the matter”
- Model Rule 1.4(a)(4)
  - "A lawyer shall promptly comply with reasonable requests for information"
- Model Rule 1.4(b)
  - “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.”

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



Model Rule 1.4 - Communications

- Comments:
  - [1]: Reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation.
  - [4]: When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with the request.
  - [5]: The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so.
  - [7]: In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication…A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person.

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



Model Rule 1.6 – Confidentiality of Information

- Model Rule 1.6(a)
  - "A lawyer shall not reveal information relating to the representation of a client unless certain circumstances arise."
- Model Rule 1.6(c)
  - "Lawyers must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."
    - Comment [18]: The unauthorized access to, or the inadvertent disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

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



"Reasonable Efforts" Definition

- Comment [18] includes nonexclusive factors as a guide for lawyers in making a "reasonable effort"
  - The sensitivity of the information,
  - The likelihood of disclosure if additional safeguards are not employed,
  - The cost of employing additional safeguards,
  - The difficulty of implementing the safeguards, and
  - The extent to which the safeguards adversely affect the lawyer's ability to represent clients.
- Comment [19]
  - When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.
  - This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy.

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



Model Rule 1.9(c) – Duties to Former Clients

- Model Rule 1.9 (c)
  - "A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter. . . Reveal information relating to the representation except as these Rules would permit or required with respect to a client."
- The rule fails to provide what steps, if any should be taken if such information is revealed.

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



Model Rule 4.4 – Respect for Rights of Third Person

- Model Rule 4.4(b)
  - "A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender."
    - Comment [2]: Paragraph (b) recognizes that lawyers sometimes receive a document or electronically stored information that was mistakenly sent or produced by opposing parties or their lawyers… If a lawyer knows or reasonably should know that such a document or electronically stored information was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures."
    - Comment [3]: Some lawyers may choose to return a document or delete electronically stored information unread, for example, when the lawyer learns before receiving it that it was inadvertently sent.

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



Bar Associations' Ethics Opinions

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

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



“Cloud computing” while keeping client information confidential.

- “Cloud computing” is where remote servers are networked so data storage can be shared within large groups. Lawyers need to take reasonable precautions and must ensure that there is “adequate access” to the client’s information where it is stored remotely, the service provider has “adequate security,” and the confidentiality of the client’s information is maintained.

Florida Bar Ethics Opinion 12-3 (2013).

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



Using the internet as a means to transmit information relating to the representation of a client.

- Under Model Rule 1.1, a lawyer has a duty to understand the "benefits and risks associated with relevant technology." Model Rule 1.6(c) states that a lawyer must make "reasonable efforts" to prevent unauthorized access or disclosure of a client's information. Under Model Rule 1.4, a lawyer may be required to inform the client of security safeguards. A lawyer can use the internet to transmit client information as long as reasonable efforts where made to prevent unauthorized access to said information.

American Bar Association Formal Opinion 477R (2017).

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



Using social media in providing legal services.

- Social media can be used to a client's benefit or detriment so it is important for lawyers to recognize and understand how social media can work with the zealous representation of a client. Client confidentiality and communications go hand and hand for social media because the communications made by the client on social media could jeopardize the confidentiality of the information. A lawyer should discuss with the client the potential risks for communicating through social media.

Washington D.C. Ethics Opinion 371 (2016).

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



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

Securing Communication of Protected Client Information

- "The term 'cybersecurity' has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a … world where law enforcement discusses hacking and data loss in terms of 'when,' and not 'if.' Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client."

ABA Formal Opinion 477, "Securing Communication of Protected Client Information" (May 11, 2017)

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



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

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

- "Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes. Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be."

ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018)

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



Real World Examples

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



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

Targeted attacks are increasing.

- Last year, 80% of law firms reported phishing attempts. (InfoSecurity North America)
- The FBI has reported that law firms are often viewed as “one-stop shops” for attackers (with information on multiple clients) and it has seen hundreds of law firms being increasingly targeted by hackers. (American Bar Association)
  - Law firm breaches have ranged from simple (like those resulting from a lost or stolen laptop or mobile device) to highly sophisticated (like the deep penetration of a law firm network, with access to everything, for a year or more).

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



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

Unnamed law firm targeted by state-sponsored Chinese hackers.

- A U.S. law firm with strong experience in intellectual property law with clients in the pharmaceutical, technology, electronics, biomedical, and automotive sectors, among others was targeted from November 2017 to September 2018.
- The group, known as APT10 that is backed by a unit of the Chinese Ministry of State Security, used stolen user credentials to access third-party software used by the companies and leveraged that access to further encroach upon internal systems.

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



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

O'Neill, Bragg & Staffin

- In late 2017, three-lawyer real estate and corporate transactional law firm O'Neill, Bragg & Staffin, based in Pennsylvania, fell prey when a hacker posed as a partner of the firm, Gary Bragg, and emailed another partner about a loan transaction of which the hacker seemed to have intimate knowledge.
- In the correspondence, the hacker addressed partner Alvin Staffin by his nickname, Mel, making the ruse even more convincing, and asked for a $580,000 transfer from the firm's IOLTA sub-account to the Bank of China on behalf of a client.
- Bank of America made the transfer at Staffin's request. After the transfer was made, Staffin called Bragg to discuss it, finding out only then that Bragg had no knowledge of the $580,000 request.
- The firm's client's account had insufficient funds to cover the transfer, only $1,900, according to the complaint. However, Bank of America drew from the firm's sub-accounts belonging to other clients to cover the fraudulent transfer, the plaintiffs claimed.
- The firm sued Bank of America for failing to stop the transfer once it had been notified of the breach, but in November, a federal judge for the Eastern District of Pennsylvania dismissed the action, finding that the firm failed to show that the bank breached any agreement, violated federal regulations or breached the Pennsylvania Commercial Code.
- At the time it filed its complaint, the firm had recovered only $58,000.

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



Where are we now? What comes next?

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

Will there be a national data breach law?



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


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

National Data Breach Law

- Congress has not yet passed a national data breach notification law.
- A new bill, the Data Security and Breach Notification Act, was introduced in the wake of reports that Uber paid $100,000 to cover up a 2016 data breach that affected 57 million users.
- The bill has currently not made it out of Senate Committee.

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

What is going to happen on the data security regulatory front?



SECURITIES AND EXCHANGE COMMISSION, UNITED STATES



HONG KONG MONETARY AUTHORITY, CHINA



FINANCIAL CONDUCT AUTHORITY , UNITED KINGDOM



BAR ASSOCIATIONS/ COURTS



NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

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



Will cyber threats create a tighter relationship between the state, individuals, businesses, and the legal community?

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



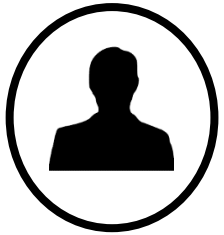
Questions?

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

Contact Us



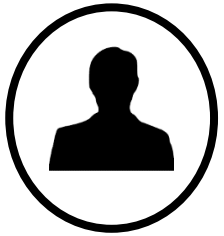
Daniel Garrie
Email: daniel@lawandforensics.com
Phone: 855-529-2466
URL: www.lawandforensics.com



David Farkas
Email: david.farkas@dlapiper.com
Phone: (310) 500-3412
URL: www.dlapiper.com



Gail Gottehrer
Email: ggottehrer@outlook.com
Phone: (860) 416-4520



Douglas Smith
Email: douglas.smith@skadden.com
Phone: (213) 687-5029
URL: www.skadden.com

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



David Farkas
DLA Piper – Associate
Contact:
E: david.farkas@dlapiper.com
W: (310) 500-3412
URL: www.dlapiper.com

David B. Farkas focuses on complex commercial litigation at the trial and appellate levels, with a particular emphasis on consumer class actions.

David has appeared and argued before state and federal courts and has extensive experience in all phases of litigation, including initiating complaints, briefing extensive successful pre-and post-trial motions, managing discovery teams, working with expert witnesses, deposing and defending witnesses, preparing key fact witnesses for trial and assisting in direct and cross examinations at trial and appeals.

Experience:

- Represented several major American corporations in defending against putative class actions brought under California's Invasion of Privacy Act (CIPA)
- Represented several major American corporations against putative classwide Telephone Consumer Protection Act (TCP) claims involving autodialed telemarketing calls, pre-recorded calls and texts, and provided compliance advice and instructions
- Obtained denial of class certification in a nationwide putative class action alleging violation of the TCPA for an international hospitality company
- Member of a trial team that obtained a jury verdict of non-infringement for the second-largest Internet content delivery service provider in a lawsuit alleging infringement of more than 100 claims in three patents
- Member of a team that represented an Alabama death row inmate and succeeded in having the trial court invalidate the underlying trial on Constitutional grounds of ineffective assistance of counsel

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



Douglas Smith
Skadden, Arps, Slate, Meagher & Flom LLP - Associate
Contact:
W: 213.687.5029
E: douglas.smith@skadden.com
URL: www.skadden.com

Skadden
Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates

Doug Smith litigates complex matters before trial and appellate courts. His diverse practice has concentrated on tax-related class actions, securities, civil and criminal insider trading, and antitrust. Representative matters in which Mr. Smith has been involved include:

- Credit Acceptance Corporation in obtaining summary judgment on antitrust claims seeking approximately $1 billion in damages arising from the allegedly fraudulent acquisition and enforcement of a patent in the indirect auto lending market. The *Daily Journal* named the decision one of the Top Verdicts of 2017;
- JP Morgan Chase in an antitrust class action involving alleged price fixing and other anti-competitive restraints by Visa and MasterCard members;
- Bank of America in federal class actions regarding alleged underreporting of home mortgage interest payments on Internal Revenue Service Form 1098;
- American Apparel in shareholder derivative and proxy solicitation fraud lawsuits and in various corporate takeover matters;
- Anheuser Busch in a putative federal class action alleging misleading advertising of Bud Light Lime, Lime-a-Rita and related products;
- Jawbone in a trade secret misappropriation and breach of contract lawsuit against Fitbit in state court;

Mr. Smith has a strong commitment to *pro bono* work and civic engagement. In 2017, Mr. Smith was the recipient of the State Bar of California's Jack Berman Award of Achievement, which recognizes exemplary *pro bono* service provided by young lawyers. He serves on the nonprofit boards of Reframe Labs, Inc., an incubator that helps launch innovative public schools in Los Angeles, and The Samburu Project, which provides clean water to the Samburu region of Kenya by drilling water wells. Previously, he co-founded and served as a board member for Global Playground, a nonprofit focused on improving education in developing countries. He also spends hundreds of hours each year on *pro bono* cases, which have involved torts, nonprofit incorporation and tax-exempt status, immigration, false advertising, contract disputes and the death penalty.

(c) Global Cyber Institute 2018. All Rights Reserved



Gail Gottehrer
Law Office of Gail Gottehrer LLC – Founder
Contact:
E: ggottehrer@outlook.com
W: (860) 416-4520

Gail Gottehrer is the Founder of the Law Office of Gail Gottehrer LLC in Stamford, CT. Her practice focuses on emerging technologies, including autonomous vehicles, AI, biometrics, robots and facial recognition technology, and the privacy and security laws and ethical issues associated with the data collected and used by these technologies. She is one of the few defense lawyers to have been involved in the trial of a class action to verdict before a jury.

Gail teaches Law for Knowledge Innovation at Columbia University, and is a member of the Advisory Board for Rutgers University's Leading Disruptive Innovation Program, and a Fellow at the Center for Legal Innovation at Vermont Law School.

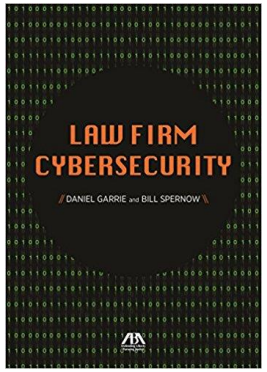
Gail is a member of the New York State Bar Association's Task Force on Autonomous Vehicles and the Law and the State of Connecticut's Task Force to Study Fully Autonomous Vehicles. Gail also serves as Co-Chair of the New York State Bar Association's Technology and the Legal Profession Committee, a member of the New York State Bar Association's Transportation Law Committee, and as Chair-Elect of the ABA TIPS Automobile Litigation Committee. She is the New York Regional Co-Chair for the ABA's Judicial Intern Opportunity Program, Co-Chair of the Programming Committee of the ABA's Woman Advocate Committee, Co-Chair of the National Association of Women Lawyers' IP & Technology Affinity Group, Editor of the ABA's Pretrial Practice and Discovery Newsletter, and a member of the Sedona Conference Working Group 1.

Gail was selected as one the Profiles in Diversity Journal's 2017 Women Worth Watching in STEM and one of the Connecticut Technology Council's 2016 Women of Innovation. She is a graduate of the University of Pennsylvania Law School and served as a law clerk to the Honorable Murray C. Goldman, in the Philadelphia County Court of Common Pleas. Gail is admitted to practice in New York, New Jersey, Connecticut, and Pennsylvania.

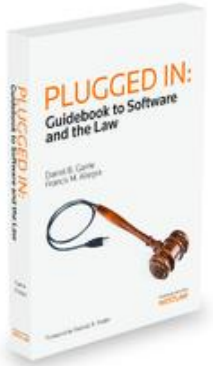
(c) 2019. Global Cyber Institute. All Rights Reserved.

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



The Wider Implications of the California Consumer Privacy Act



'Act Of War' Questions In Cyberattack Insurance Case



Arbitrating Cyber Coverage Disputes

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