

# e-Discovery in the Cloud


**Speakers:**

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

**Jennifer Hoekstra,** Partner, Aylstock, Witkin, Kreis & Overholtz PLLC

**Paul Kiesel,** Partner, Kiesel Law


(c) 2020 Global Cyber Institute. All Rights Reserved.

# Speakers



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



**Jennifer Hoekstra**
Partner, Aylstock, Witkin, Kreis & Overholtz PLLC



**Paul Kiesel**
Partner, Kiesel Law

(c) 2020 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) 2020 Global Cyber Institute. All Rights Reserved.



# Overview of Cloud Computing



(c) 2020 Global Cyber Institute. All Rights Reserved.



# Cloud Computing

- "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

- NIST definition of Cloud Computing

(c) 2020 Global Cyber Institute. All Rights Reserved.

# What is Cloud Computing?

| 5 essential characteristics: | 4 deployment models: | 3 common service models: |
|---|---|---|
| • On-demand self-service<br>• Broad network service<br>• Resource pooling (a/k/a multi-tenancy)<br>• Rapid elasticity<br>• Managed service | • Public cloud<br>• Hybrid cloud<br>• Private cloud<br>• Community cloud | • Software as a Service (SaaS)<br>• Infrastructure as a Service (IaaS)<br>• Platform as a Service (PaaS) |

(c) 2020 Global Cyber Institute. All Rights Reserved.

# What are the Different Types of Cloud?

## Software as a Service (SaaS)

- Hosted single application
  - Hotmail, Gmail, Salesforce, Dynamics CRM, Quickbooks Online
- Hosted suite of programs
  - Microsoft's Office 365 - Exchange Online and SharePoint Online
  - Google Docs

## Infrastructure as a Service (IaaS)

- Users rent computing power
  - Either actual hardware or virtualized machines
  - Deploy and run your own operating systems and software applications

## Platform as a Service (PaaS)

- Users create / run their own applications
- Cloud provides:
  - Software development tools
  - Underlying infrastructure

(c) 2020 Global Cyber Institute. All Rights Reserved.



# What Are "Cloud Services"?

- Hosted, Shared, "On-demand" enterprise applications
  - Salesforce.com
  - Google docs
  - Hosted email (Exchange) services
- Cloud computing resources (roll your own)
  - Rapid provisioning of ad hoc compute environments
    - Amazon Elastic Compute Cloud (EC2)
    - VMWare vCloud Express
    - GoGrid

(c) 2020 Global Cyber Institute. All Rights Reserved.



# What Are “Cloud Services”? (cont.)

- Cloud Storage Services (like a utility)
  - Microsoft Azure
  - Amazon Simple Storage Service (S3)
  - Nirvanix
- Internet Hosted Legal Discovery, Analysis and Review (SaaS)
  - Electronic data processing, analysis and review

(c) 2020 Global Cyber Institute. All Rights Reserved.



# How are Cloud Services different?

**On Premise S/W Licensing**

- Perpetual license
- Single up-front payment
- Support separate
- Customer manages infrastructure
- Customer controls security
- Procured formally through IT

**Cloud**

- Termed Subscription
- Recurring fees
- Support bundled
- Shared responsibilities (usually)
- Shared responsibilities
- Procured more informally by LOBs/users

(c) 2020 Global Cyber Institute. All Rights Reserved.



# Why Do Companies Move to the Cloud?

- Technical Factors
  - Reduced infrastructure management
  - Rapid implementation and deployment
  - Reduced operational management, IT complexity
  - Continuous improvement

(c) 2020 Global Cyber Institute. All Rights Reserved.



# Why Do Companies Move to the Cloud?

- Business Factors
  - Lower up-front and total costs
  - Drive digital transformation
  - Capital vs. operating expenses
  - Deliver new products and services

(c) 2020 Global Cyber Institute. All Rights Reserved.

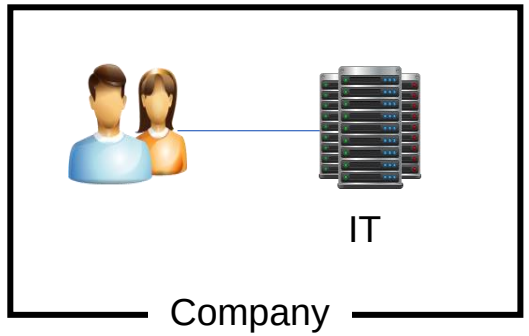


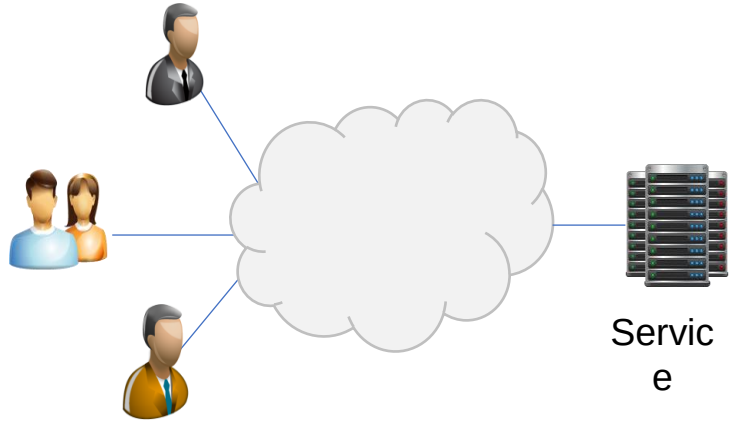

# Why Do Companies Move to the Cloud?

- Risk Factors
  - Security by default
  - Compliance

(c) 2020 Global Cyber Institute. All Rights Reserved.

# Examples of Cloud Computing Systems



























(c) 2020 Global Cyber Institute. All Rights Reserved.



# e-Discovery Overview



(c) 2020 Global Cyber Institute. All Rights Reserved.



# What is E-Discovery?

- Electronic discovery ("E-Discovery") refers to discovery of electronically stored information ("ESI").

  - Eoghan Casey, ed., *Handbook of Digital Forensics and Investigation* (Academic Press: NY, 2009), p. 567.

- Examples of types of ESI include e-mails and instant messaging chats, documents, accounting databases, CAD/CAM files, Web sites, and "metadata" of files.

(c) 2020 Global Cyber Institute. All Rights Reserved.



# Benefits of Using the Cloud in the e-Discovery Process



(c) 2020 Global Cyber Institute. All Rights Reserved.




# Anytime, Anywhere Access

- Centralized availability of data and applications allows employees to work from almost anywhere via the Internet.
- As long as you can get online, you can access, monitor and manage any part of the process.

(c) 2020 Global Cyber Institute. All Rights Reserved.



# Robust Security

- The process of creating security protocols and getting IT infrastructure appropriately certified can cost millions of dollars and countless man hours, and, at the end of the day, still might not meet requirements.
- For example, Microsoft Azure's infrastructure allows you to securely connect your resources through virtual networks (Vnets).
- The connection between Azure and your personal site does not cross the public internet.

(c) 2020 Global Cyber Institute. All Rights Reserved.

# Cost Reduction



Data volumes and IT demands have grown considerably, and maintaining in-house solutions requires capital investment; software licensing and support; premises costs; security; and proper staffing.

(c) 2020 Global Cyber Institute. All Rights Reserved.



# Potential E-Discovery Pitfalls of Storing Data in the Cloud



# Potential Issues with Cloud Computing

- Several aspects of cloud computing significantly impact electronic discovery.
  - Collection of Data
  - Format of the Data
  - Practical Risk And Security Considerations
  - Exposure of Privileged Data
  - Hidden Costs
  - No Longer Supports Data Format
  - Complying with Preservation and litigation holds
- These issues must be known and understood by both client and counsel before e-discovery commences.
- These issues ideally should be considered by the client in deciding whether cloud computing is an appropriate choice for the company.

(c) 2020 Global Cyber Institute. All Rights Reserved.

# Traditional Data Governance

Many organizations transfer data to a third party hosted archiving service which has challenges

| Exchange Data | Outsourced Data Journaling | Challenges |
|---|---|---|



Third party outsourced journaling

**Increased costs**
Having a separate copy of the data being stored significantly increases costs

**Increased risks**
Content may be compromised moving from one environment to another

**Point in time data**
Captures data at a point in time which miss any edits in place or from transport agents in flight

**Increased time**
Waiting for indexing increases time required to find relevant data

**No service wide insights**
Unable to leverage service wide machine learning to draw correlations between the data

(c) 2020 Global Cyber Institute. All Rights Reserved.




# Collection of Data

- There is a growing legal concern about the collection of information from cloud providers that store data outside the home jurisdiction.
- For example, cloud providers that elect to store information in the EU may trigger data-protection laws that otherwise would not apply, and some providers store data across multiple jurisdictions for cost, security or other reasons that take no account of U.S. e-discovery obligations.

(c) 2020 Global Cyber Institute. All Rights Reserved.



# The Data May Be Stored in a Different Format

- The information that sits in the cloud is not all necessarily searchable. It is possible that data sits in the cloud, but that the cloud lacks the necessary search component required to search and retrieve that data.
  - For example, the information may be stored in a unique format proprietary to the client that is not recognized by the cloud.
- It is imperative that counsel understand the formats in which data is stored in the cloud and ensure that all the data can be searched and produced, before committing to a cloud-based system.

(c) 2020 Global Cyber Institute. All Rights Reserved.



# No Longer Supports Data Format

- Litigations may continue for a long enough time period that the cloud no longer actively supports the data format in which your information is stored in the cloud.
  - The issue then arises as to how you deal with the upgrade, and the impact of any such upgrade on the required preservation of that data.
- For instance, many upgrades limit or eliminate the types of metadata that can be extracted during production, leading to potential spoliation claims by your adversary.

(c) 2020 Global Cyber Institute. All Rights Reserved.



# Practical Risk And Security Considerations

- Security is a critical component of information governance, and sending data outside a company's infrastructure may increase security risks, with implications for e-discovery and business in general.
- There are some obvious technical steps to take, such as data encryption, and risk assessments should consider the number of attacks and the tools and skills available to would-be attackers.
- Organizations must identify who is responsible for what aspects of security, and they must understand the difference between compliance and security. Achieving a minimum level of compliance does not necessarily imply an adequate level of security.

(c) 2020 Global Cyber Institute. All Rights Reserved.





# Exposure of Privileged Data

- Cloud computing necessarily involves migrating data outside the company and to a third-party host. Quite apart from any catastrophic breach in the cloud, it is likely that the specific elements of privilege, and the importance of maintaining that privilege, will not be as understood or appreciated by those that manage the cloud infrastructure on your behalf.
- Extra care must be taken to ensure that the data managed is not accidentally accessed by a third-party or by a system administrator accessing privileged data in the context of resolving a technology issue.

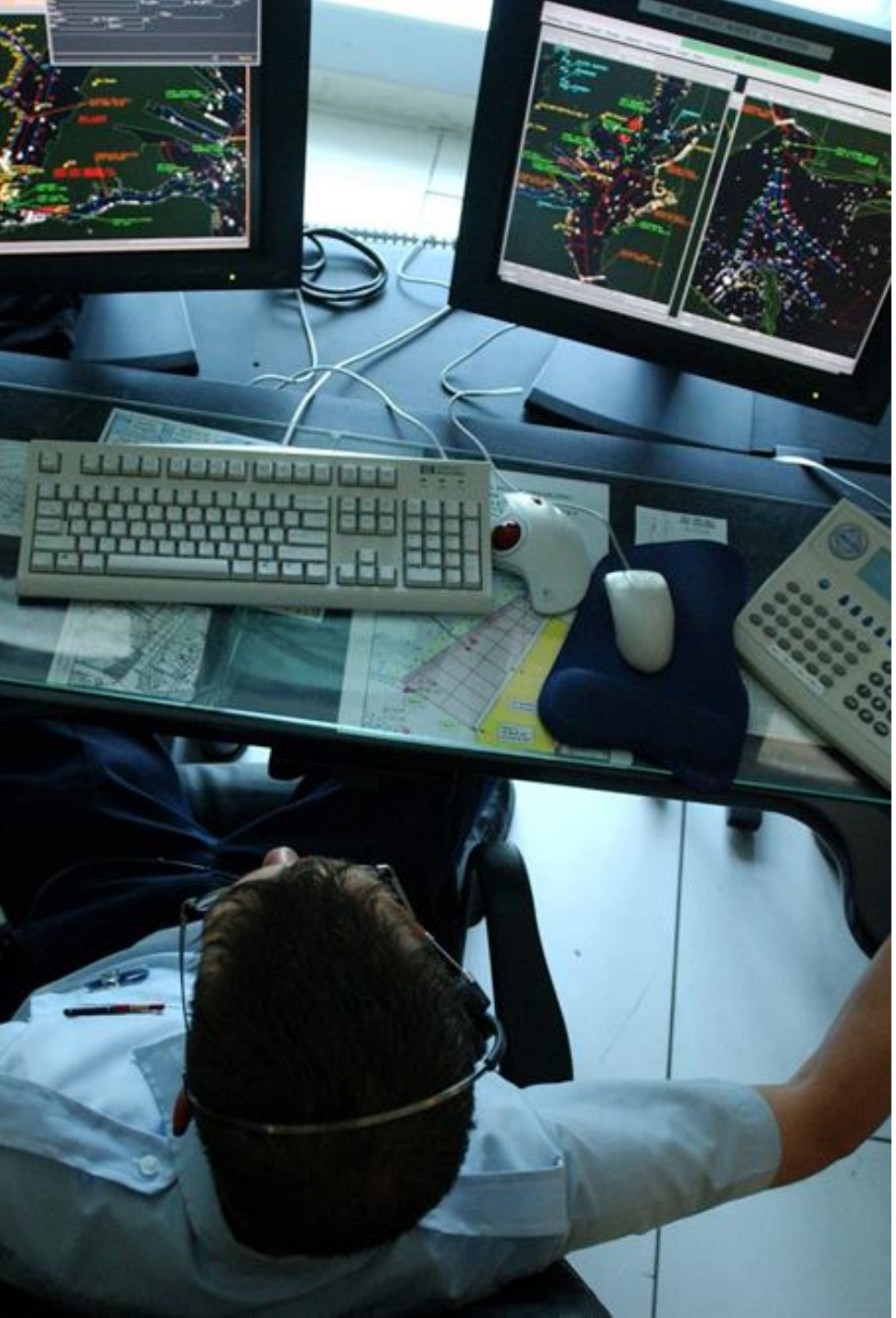
(c) 2020 Global Cyber Institute. All Rights Reserved.



# Hidden Costs

- Hidden costs might arise as a result of the size of the data set, the difficulty of retrieval, or the need to repeatedly access and manipulate the data hosted on the cloud.
- It may make sense to migrate only a portion of a company's data to a cloud-based computing system, while retaining in-house control over other areas of information.

(c) 2020 Global Cyber Institute. All Rights Reserved.



# Complying with Preservation and Litigation Holds

- Organizational policies must be established that cover the lifecycle of data, regardless of its location or of the circumstances – whether ordinary or discovery-related – that may require access to it. IT departments have specific technical concerns, and cloud providers may have their own policies for the periodic deletion of data.
- It is critical to settle these matters in a negotiated contract, stipulating records management and retention protocols.

(c) 2020 Global Cyber Institute. All Rights Reserved.



# Questions

(c) 2020 Global Cyber Institute. All Rights Reserved.

# Contact Us



**Daniel B. Garrie**
Email: daniel@lawandforensics.com
Phone: (855) 529 – 2466
URL: www.lawandforensics.com



**Jennifer Hoekstra**
Email: jhoekstra@awkolaw.com
URL: https://www.awkolaw.com



**Paul Kiesel**
Email: Kiesel@Kiesel.law
Phone: (310) 854-4444
URL: Kiesel.law

(c) 2020 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
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) 2020 Global Cyber Institute. All Rights Reserved.



**Jennifer Hoekstra**
Alystock, Witkin, Kreis & Overholtz PLLC – Partner
**Contact:**
E: jhoekstra@awkolaw.com
URL: https://www.awkolaw.com

**Jennifer M. Hoekstra** is a partner with Aylstock, Witkin, Kreis & Overholtz, PLLC. A native of Saint Paul, Minnesota, Ms. Hoekstra boasts an impressive academic and professional record, including graduation from two of the nation's top schools. She earned her earned Bachelor of Arts in Environmental Science from Columbia College, Columbia University in the City of New York. She relocated to Louisiana to attend Tulane Law School, where she earned her J.D. while also completing a certificate in Environmental Law. During her law school career, she spent a semester studying at the University of Wisconsin School of Law and visited on their International Law Journal as a Junior Member during her Hurricane Katrina evacuation semester. While in law school, Ms. Hoekstra served as Executive Treasurer of the Student Bar Association and as a Graduate Student Association delegate.

Ms. Hoekstra has been involved in complex litigation cases of all forms since 2007. Jennifer was inspired to pursue her law degree while working as a Litigation Assistant at Cravath Swaine and Moore LLP in New York. Ms. Hoekstra has earned a solid reputation as a skilled writer and researcher, and plays an integral role in several complex litigation cases, practicing in the areas of Pharmaceutical Mass Torts, Defective Device Mass Torts, and other complex litigation. Ms. Hoekstra has been involved in all aspects of MDL litigation involving Actos, Genetically Modified Rice, DePuy ASR, DePuy Pinnacle, Biomet, Plavix, NuvaRing, the BP Oil Spill, and other defective drugs or devices. She is currently a member of the DePuy Pinnacle Law and Briefing Committee as well as a member of the Biomet II PSC. Jennifer was central to the successful outcome in bellwether trials in the Genetically Modified Rice, Actos and DePuy Pinnacle Hip MDLs with more than $11 Billion in trial verdicts resulting from those cases.

She is licensed to practice before all Louisiana state and federal courts and the U.S. District Courts for the Northern District of Texas and Eastern District of Missouri as well as the 5th and 8th Circuit Courts. She is a member of the American Bar Association, the Louisiana Bar Association, the Acadiana Federal Bar Association, the Alexandria Louisiana Bar Association and the American Association for Justice. She is a member of Women En Mass and was also a member of the inaugural 2018 Board of Directors for Emerge Louisiana.

(c) 2020 Global Cyber Institute. All Rights Reserved.



**Paul Kiesel**
Kiesel Law LLP – Partner
**Contact:**
W: 310.854.4444
E: Kiesel@Kiesel.law
URL: Kiesel.law

KIESEL LAW LLP

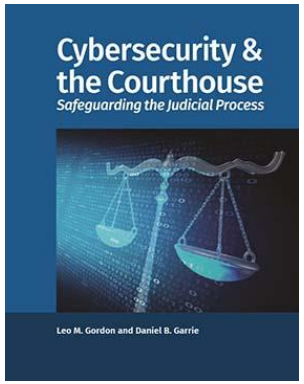
Paul Kiesel is very active in the legal community. He was the president of the Los Angeles County Bar Association for 2015-2016 and was the past Chair of the Litigation Section. He was appointed by former Chief Justice Ronald George to the State of California Judicial Council Civil and Small Claims Advisory Committee. He served on the Board of Governors for the Consumer Attorneys of California and the Consumer Attorneys Association of Los Angeles for over 25 years. In recognition of his service, Mr. Kiesel was elected an emeritus (lifetime) board member of both organizations. From 2001-2005, Mr. Kiesel sat on the Board of Governors of the Association of Business Trial Lawyers. Mr. Kiesel is currently the Co-Chair of the Open Courts Coalition, a bipartisan committee of attorneys from throughout California advocating full-funding of the civil justice system. Members of the Open Courts Coalition include Niall McCarthy, president of the Consumer Attorneys of California, the Honorable Carlos Moreno, former Governors Gray Davis and George Deukmejian, Los Angeles Mayor Antonio Villaragosa, and former California Attorney General John VanDekamp. Recently, Mr. Kiesel was named a Senior Fellow of the Litigation Counsel of America, a trial lawyer honorary society composed of less than one-half of one percent of American lawyers, dedicated to promoting superior advocacy, professionalism and ethical standards in the legal profession.

Currently, Paul Kiesel represents many individuals and their families in significant personal injury and wrongful death cases. Among his many clients, Mr. Kiesel represented former Governor Gray Davis in a challenge to the qualification of the 2003 recall election. Mr. Kiesel currently represents numerous municipalities, including the City of Los Angeles, in a class action on behalf of all cities in the State of California for payment of occupancy taxes owed by the online travel industry.

(c) 2020 Global Cyber Institute. All Rights Reserved.

# Additional Reading

## Books




[Cybersecurity & the Courthouse: Safeguarding the Judicial Process]




[Plugged In: Guidebook to Software and the Law]




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




[Dispute Resolution and e-Discovery]

## Articles




[Confronting the Challenges of Virtual Mediation]




[Avoiding Sanctions: Ethical Considerations for e-Discovery]




[Making Heads or Tails of the California Consumer Privacy Act]

(c) 2020 Global Cyber Institute. All Rights Reserved.