



**RSA Conference 2012**  
February 28 – March 2, 2012  
Moscone Convention Center  
San Francisco, CA

*LAW TRACK SESSIONS – Co-sponsored by the ABA Section of Science & Technology Law*

<b>Session Title</b>	<b>Just Because They're Authenticated Doesn't Mean You Should Trust Them</b>
<b>Moderator</b>	<b>Hoyt Kesterson</b> , Terra Verde Services, Senior Security Architect
<b>Panelist(s)</b>	<b>Anne Rogers</b> , Waste Management, Director, Information Safeguard <b>John Facciola</b> , U.S. District Court for the District of Columbia, U.S. Magistrate Judge <b>Andrew Peck</b> , U.S. District Court for the Southern District of New York, United States Magistrate Judge <b>Stephen Wu</b> , Cooke Kobrick & Wu LLP, Partner <b>Steven Tepler</b> , Edelson McGuire, LLC, Partner
<b>Date/Time</b>	Tuesday, February 28, 1:10 PM Room 131
<b>Abstract</b>	A confluence of errors—a health clinic allowed their employees' computers to be contaminated with malware; a certification authority issued a certificate to a knave; and a blood-testing laboratory let that knave see much more than he should have. The result is a massive data breach of medical records, a lawsuit, and a mock hearing. But whose fault is it?
<b>Pre-requisite Knowledge</b>	Attorneys and technical people who work with attorneys are the target audience. A familiarity with the authentication technologies and web services vulnerabilities is useful but explanatory material on the technology will be presented to the presiding judge. These explanations will be tutorial in nature.
<b>Learning Objectives</b>	The hypothetical for this mock session will illustrate the problems encountered in affixing fault when multiple parties have not behaved as they should. The mock hearing held before a Federal Magistrate Judge will require attorneys and their experts to explain the authentication methods in place and their shortcomings. It will be necessary to present audit logs as digital evidence to pinpoint the breakdown that allowed the extensive data breach. This will demonstrate how attorneys and enterprise information technology stakeholders ensure their ESI is admissible and convincing. The breach in the hypothetical will demonstrate to those responsible for securing organizations that authentication should not equate to trust. In addition the mock hearing will show why it is critical even for technology-savvy attorneys to engage with technology experts early, and how the participation and testimony provided by a technology expert can influence a Federal Magistrate Judge's decision.
<b>Session Title</b>	<b>The Dark Side of a Payment Card Breach</b>
<b>Moderator</b>	<b>David Navetta</b> , InfoLawGroup, Founding Partner
<b>Panelist(s)</b>	<b>Branden Williams</b> , RSA, The Security Division of EMC, Director, Security Consulting <b>Serge Jorgensen</b> , The Sylint Group, Chief Technology Officer

**Date/Time** Tuesday, February 28, 2:40 PM  
Room 131

**Abstract** The fallout of a payment card breach doesn't stop when it is contained. From working with an incident assessor, to dealing with the payment processor and navigating the card brand rules and PCI, many pitfalls exist that can drastically increase liability. Coming from security and legal professionals in the trenches, this session explores what really happens after a breach, and how to limit loss.

**Pre-requisite Knowledge** A basic understanding of PCI and the general requirements around payment card incident response.

**Learning Objectives**

- Understand the role of PCI compliance in assessing a merchants ability for a payment card security breach
- Evaluate the obligations in a merchant agreement that impact merchant ability for a a payment card security breach
- Understand the role of Qualified Incident Response Assessors and how to handle a QIRA investigating a payment card security breach
- Identify the key payment card brand rules that dictate a merchants liability for a payment card security breach
- Develop strategy for dealing with and addressing liability arising out of a payment card breach

**Session Title** **eDiscovery and Forensics; Working Together for the Winning Solution**

**Moderator** **John Jorgensen**, The Sylint Group, President & Chief Executive Officer

**Panelist(s)** **Serge Jorgensen**, The Sylint Group, Chief Technology Officer  
**Stacy Arruda**, Federal Bureau of Investigation, Supervisory Special Agent  
**Steven Teppler**, Edelson McGuire, LLC, Partner

**Date/Time** Tuesday, February 28, 3:50 PM  
Room 131

**Abstract** An actual case study will be presented with a short discussion about the elements of the eLitigation and the digital evidence used. The attendees will be grouped into a workshop structure and assisted by the panel in making a presentation on their strategy and use of digital data in litigation. The panel will comment on the validity of the workgroup's strategy and use of data.

**Pre-requisite Knowledge** Involvement with computer forensic, eDiscovery and the litigation process in gathering, analyzing and presenting electronic information evidence.

**Learning Objectives** This workshop session is intended to provide guidelines for counsel, their assistants, law firm eDiscovery personnel and computer forensic experts understand how to define, recover, comprehend and use digital evidence during litigation. The panel will use an actual case to describe the eDiscovery process and the role that digital data forensics plays. The panel will cover evidence preservation through the actual Hearing and Trial process.

**Session Title** **Whose Fault is it that I Didn't Know it Wasn't You—an Update**

**Moderator** **Hoyt Kesterson**, Terra Verde Services, Senior Security Architect

**Panelist(s)** **David Navetta**, InfoLawGroup, Founding Partner  
**Ken Baylor**, Wells Fargo Bank, Vice President AntiFraud  
**Joseph Burton**, Duane Morris, LLP, Managing Partner  
**John Facciola**, U.S. District Court for the District of Columbia, U.S. Magistrate Judge

**Date/Time** Wednesday, February 29, 8:00 AM  
Room 131

**Abstract** Two recent judicial decisions were announced on customer claims that their banks processed fraudulent funds transfer requests. A bench verdict found for the customer that the bank did not act in good faith but in the other case the magistrate judge found that the bank's security practices were commercially reasonable. This panel will examine the technical and legal implications of these decisions.

**Pre-requisite Knowledge** Attorneys and technical people who work with attorneys are the target audience. A familiarity with the authentication technologies is useful but some will be explained in the course of the discussion. These explanations are tutorial in nature.

**Learning Objectives** The cases, pending and those with rulings, will demonstrate how prevalent this problem is becoming. The results of the case will demonstrate that it is critical to have a common understanding of the meaning of commercially reasonable. Attorneys acting as in-house counsel for financial institutions and for small businesses will realize that the security processes have to be clearly stated. It will be demonstrated how to describe those security procedures so that the court can understand what they do and what they don't do. The examination of UCC § 4A-202's inclusion of the consideration of transactional history in the definition of commercially reasonable security will demonstrate that authentication is more than passwords and tokens. Finally discussion on how guidelines such as that of the FFIEC have been revised since this spate of legal disputes will show both parties what they should be doing to prevent fraudulent transfers of funds.

**Session Title** **Should I Sue? The Perils of Litigation in the Age of Anonymous**

**Moderator** **Gib Sorebo**, SAIC, Chief Cybersecurity Technologist

**Panelist(s)** **Tanya Forsheit**, InfoLawGroup, LLP, Attorney  
**Steven Tepler**, Edelson McGuire, LLC, Partner  
**Bennett Borden**, Williams Mullen, Attorney

**Date/Time** Wednesday, February 29, 9:30 AM  
Room 131

**Abstract** While lawsuits have always been a public relations risk for companies, the latest trends go beyond bad press. In several cases, companies seeking to enforce their rights in court have found themselves to be targets of coordinating hacking campaigns. This session will explore the strategies to address these threats through legal, public relations and information security strategies.

**Pre-requisite Knowledge** Participants should have familiarity with the security threat landscape and should also have a basic understanding of the litigation process.

**Learning Objectives** As a result of this session, attendees will be able to better advise their clients on whether and how to file lawsuits where the consequence may be hacking attacks. Audience members will walk away with a better understanding of how to combine litigation skills with technical knowhow in order to coordinate the filing of lawsuits with the strengthening of network defenses. Additionally, attendees will learn of the legal tools that may be available to draw less publicity to their companies so as to avoid attacks.

**Session Title** **Data Breach Laws: Will They Save or Sink You in a Massive Attack?**

**Moderator** **Lucy Thomson**, CSC, Senior Engineer - Attorney

<b>Panelist(s)</b>	<b>Thomas Smedinghoff</b> , Wildman Harrold, Partner <b>Robert Thibadeau</b> , Wave Systems Corp., Chief Scientist & SVP <b>Eric Hibbard</b> , Hitachi Data Systems, Chief Technology Officer Security & Privacy
<b>Date/Time</b>	Wednesday, February 29, 10:40 AM Room 131
<b>Abstract</b>	To address the problem of escalating data breaches, nearly all states have passed data breach laws and HITECH covers health records. Using recent massive breaches as case studies, legal and encryption experts sort out the complexities and ambiguities that result in uncertainties for global business and health providers – focusing on both the legal and technical aspects, including encryption.
<b>Pre-requisite Knowledge</b>	Working knowledge at an advanced level of information security vulnerabilities, data breaches, and encryption, and legal and public policy issues and requirements related to information security.
<b>Learning Objectives</b>	<ul style="list-style-type: none"> <li>• Gain familiarity with fundamental legal terminology and be able to speak with both security experts and legal counsel about the most up-to-date security requirements of the data breach laws, including the new HITECH Act</li> <li>• Thoroughly grasp the core security requirements, including encryption, of the federal and state data breach laws</li> <li>• Obtain a working knowledge of the data breach laws sufficient to avoid the numerous pitfalls in compliance on both the federal and state levels, and be able to classify and evaluate the inconsistencies between the various laws</li> <li>• Analyze the root causes of the major data breaches and understand how egregious security failures lead to massive data breaches even when sensitive records were encrypted</li> <li>• Inspire security professionals to commit to and adopt a proactive strategy specifically designed to prevent data breaches in 2012</li> </ul>

<b>Session Title</b>	<b>Tackling the Identity Management Liability Problem</b>
<b>Moderator</b>	<b>Thomas Smedinghoff</b> , Wildman Harrold, Partner
<b>Panelist(s)</b>	<b>Scott David</b> , K&L Gates LLP, Partner <b>Randy Sabett</b> , ZwillGen PLLC, Partner
<b>Date/Time</b>	Wednesday, February 29, 1:00 PM Room 131
<b>Abstract</b>	This session will address what many consider to be the single most important legal hurdle to developing a viable online federated identity management system – the problem of potential legal liability. The panel will examine the liability risks of concern to participants in an IdM system, the current state of the law regarding such liability and potential solutions to the “liability problem.”
<b>Pre-requisite Knowledge</b>	A working knowledge of federated identity management concepts and general legal principles is recommended.
<b>Learning Objectives</b>	<p>This session will explore the IdM liability problem in a manner designed to help participants:</p> <ul style="list-style-type: none"> <li>• Understand how the law treats liability generally/li</li> <li>• Identify the key existing laws and regulations that affect IdM liability</li> <li>• Understand how those laws currently allocate liability in a federated identity management system</li> <li>• Understand the varying impact of the liability issue across different participant roles, levels of assurance, and IdM system models</li> <li>• Identify possible liability risk mitigation strategies appropriate for each participant role</li> </ul>

- Examine the various contractual legal models and options for modifying the liability rules under existing law

<b>Session Title</b>	<b>Hot Topics in Information Security Law 2012</b>
<b>Moderator</b>	<b>Michael Aisenberg</b> , Cyber Security Division, Center for Integrated intelligence Systems, Principal, The MITRE Corporation
<b>Panelist(s)</b>	<b>Benjamin Tomhave</b> , LockPath, Inc., Principal Consultant <b>Jon Stanley</b> , Law Office of Jon Stanley, Partner <b>Peter McLaughlin</b> , Foley & Lardner, LLP, Senior Counsel
<b>Date/Time</b>	Thursday, March 1, 8:00 AM Room 131
<b>Abstract</b>	The legal risk and regulatory environment for information security is in a state of constant flux. New regulations, lawsuits and compliance obligations arise on a regular basis. This panel, put on by the American Bar Association's Information Security Committee provides up-to-the-minute reporting on key infosec legal developments, and provides insight into where the law is going in the future.
<b>Pre-requisite Knowledge</b>	Basic understanding of the intersection of information security and the law; a desire to understand how lawyers, judges and regulators view decisions made by security professionals on information security.
<b>Learning Objectives</b>	<ul style="list-style-type: none"> <li>• Understanding of key regulations and laws passed and proposed since RSA 2011 and how they impact security compliance obligations</li> <li>• Overview of key lawsuits and litigation trends impact on the concept of legally reasonable security</li> <li>• Evaluate when and how it is appropriate to work with inside and outside legal counsel for assistance with security compliance obligations</li> <li>• Understand trends and security legal issues arising out of social media, mobile computing, cloud computing and other new IT paradigms</li> <li>• Up-to-the minute knowledge of current trends and issues impacting information security law and the activities of information security professionals</li> </ul>
<b>Session Title</b>	<b>3 "C" Words You Need to Know: Custody - Control - Cloud</b>
<b>Speaker(s)</b>	<b>Bradley Schaufenbuel</b> , Midland States Bancorp, Director of Information Security <b>James Christiansen</b> , Evantix, Inc., Chief Executive Officer & Chief Information Security Officer
<b>Date/Time</b>	Thursday, March 1, 9:30 AM Room 131
<b>Abstract</b>	In the rush to reduce expenses in tough economic times, your company moves to the cloud to save money and increase efficiencies. How will you meet the 2006 e-discovery amendments to the FRCP? How will document retention rules be enforced? How do new privacy regulations add complexity to the mix? This presentation will give you tactical advice and strategies for coping with the great migration.
<b>Pre-requisite Knowledge</b>	Participants should either be currently in information security management, corporate compliance, legal or IT audit or ready to make the jump into these fields.
<b>Learning Objectives</b>	The presentation is designed as an interactive session on eDiscovery in the Cloud - this is an area that requires planning to avoid the penalties outlined in the FCRP (Federal Rules of Civil

Procedure). Using actual cases, the audience will learn how to manage this risk throughout the entire lifecycle of a cloud computing relationship.

- The speakers outline the risks associated with the different cloud computing service models
- E-discovery challenges associated with cloud computing - how to effectively perform electronic discovery
- Manage risks throughout your relationship with your cloud service provider
- Before contracting: Cloud service provider due diligence process
- During negotiations: What needs to be in the service contract
- During relationship: Proactively monitor risk exposure
- Ending the relationship: Verifying return or destruction of potentially discoverable information
- Learn how to assess your program against the FCRP requirements

<b>Session Title</b>	<b>Social Media in Marketing and the Workplace: Legal and Regulatory Compliance</b>
<b>Speaker(s)</b>	<b>Behnam Dayanim</b> , Axinn Veltrop & Harkrider LLP, Partner <b>David Adler</b> , Leavens, Strand, Glover & Adler, LLC, Partner
<b>Date/Time</b>	Thursday, March 1, 10:40 AM Room 131
<b>Abstract</b>	The past few years have witnessed an explosion of legal and regulatory activity involving social and other new media. This session will examine several key areas, including copyright, trademark and related intellectual property concerns; defamation, obscenity and related liability; false advertising and marketing restrictions; gaming; data privacy issues presented by social media; and impacts of social media on employees and the workplace. Attendees will learn how to identify legal risks and issues before they become full-scale emergencies and how to develop appropriate policies and guidelines covering social media activity.
<b>Pre-requisite Knowledge</b>	Interest in the legal and compliance issues that social media create. Appropriate for legal, marketing and compliance functions.
<b>Learning Objectives</b>	Attendees will learn how to identify legal risks and to develop policies covering social media.
<b>Session Title</b>	<b>Mobile Services: A Privacy &amp; Security Check-In</b>
<b>Moderator</b>	<b>Demetrios Eleftheriou</b> , EMC Corporation, Senior Counsel
<b>Panelist(s)</b>	<b>Nicole Ozer</b> , ACLU of Northern California, Technology & Civil Liberties Policy Director <b>Laura Berger</b> , Federal Trade Commission, Senior Attorney <b>Ashkan Soltani</b> , Ashkansoltani.org, Consultant
<b>Date/Time</b>	Thursday, March 1, 1:00 PM Room 131
<b>Abstract</b>	Mobile services is one of the fastest growing segments of the technology sector. This panel will discuss the current state of legal and technical privacy and security protections for mobile consumers; how individuals, businesses, and policymakers can work together to update and enhance these protections; and practical suggestions for complying with legal requirements.
<b>Pre-requisite</b>	General understanding of mobile technology and privacy and data security concerns as related

- Knowledge** to such technology as geolocation and data aggregation.
- Learning Objectives**
- Identify significant privacy and data security issues relating to the use of mobile devices
  - Analyze current legal requirements, pending legislation and policy developments
  - Recommend best practices

**Session Title** **Fraud and Data Exfiltration: Defending Against the Mobile Explosion**

**Speaker(s)** Randy Sabett, ZwillGen PLLC, Partner  
Aaron Turner, IntegriCell, LLC, President

**Date/Time** Friday, March 2, 9:00 AM  
Room 131

**Abstract** Mobile devices offer numerous opportunities for wrongdoers to commit fraud or steal data. What are the risks of targeted mobile service fraud, who are the players, and what can organizations do about it based upon the law? What monitoring technologies exist and how can those technologies be used legally by enterprises for monitoring cellular communications? This session will cover these and other troubling mobile device issues.

**Pre-requisite Knowledge** General understanding of cellular communications and US wiretap regulations.

- Learning Objectives**
- Awareness of cellular communications monitoring systems
  - Awareness of legal & policy constraints for deploying certain tools

**Session Title** **Updating the Law on Government Access to User Data in the Cloud**

**Speaker(s)** **Jim Dempsey**, Center for Democracy & Technology, Vice President for Public Policy  
**Richard Salgado**, Google, Senior Counsel

**Date/Time** Friday, March 2, 10:10 AM  
Room 131

**Abstract** The Electronic Communications Privacy Act of 1986 established rules for law enforcement access to email and other electronic communications and transactional data held by service providers. The law has not been meaningfully updated to protect privacy in over 25 years. It no longer fits well with the way technology is used. This session will describe the problem and discuss proposals to update the law.

**Pre-requisite Knowledge** Aiming for the intermediate level, but there is little or no pre-requisite knowledge necessary. The session will be introducing some legal and constitutional concepts around government surveillance and privacy rights to a non-legal audience, recognizing that the RSA audience is sophisticated and many of these concepts will be familiar even if the degree of legal expertise itself is low.

**Learning Objectives** Demonstrate value to companies of having clear, strong legal standards for government access to the data they hold. Narrow the gap between technologists and policy debates by explaining to RSA audience how current law fails to map privacy rules to cloud computing, LBS and other leading trends. Illustrate the law's limits with simple examples and outline recommendations for updating the rules to better match technology design and current business models. Equip audience to participate in debate over updating rules for government access.

<b>Session Title</b>	<b>More Art than Science: Negotiating Privacy and Data Security Language</b>
<b>Moderator</b>	<b>Anjali Garg</b> , Citi Institutional Clients Group, Senior Vice President, Assistant General Counsel
<b>Panelist(s)</b>	<b>Demetrios Eleftheriou</b> , EMC Corporation, Senior Counsel
<b>Date/Time</b>	Friday, March 2, 11:20 AM Room 131
<b>Abstract</b>	Two privacy experts with 20+ years of combined privacy experience will engage in a live negotiation on issues that make senior lawyers sweat, including: What are adequate security measures? What is a reportable security breach? What are breach notification requirements? Join us to learn the latest and greatest tricks of the trade, and arm yourself for your future data protection negotiations.
<b>Pre-requisite Knowledge</b>	Simple privacy and data security background is sufficient.
<b>Learning Objectives</b>	<ul style="list-style-type: none"><li>• Identify the most significant issues in privacy and data security negotiations, including vendor agreements</li><li>• Analyze the latest privacy and data security legal requirements</li><li>• Recommend solutions to negotiation sticking points</li><li>• Highlight differences in privacy perspectives at a global level</li><li>• Arm the audience with good negotiation tactics as take-aways</li></ul>