2015 THE NATIONAL LAW JOURNAL

TRAILBLAZERS

CYBERSECURITY & DATA PRIVACY

Custom Publishing Supplement to *The National Law Journal*

Dear Readers,

Welcome to the premiere issue of *Cyber Security & Data Privacy Trailblazers*, a special supplement developed by *The National Law Journal*. In the pages that follow, you'll read 50 profiles of people who have helped make a difference in the fight against criminal cyber activity and towards adding much needed layers of data security in an increasingly digital world of commerce. While those recognized impact the practice of law in different ways, a common thread ties them together: each has shown a deep passion and perseverance in pursuit of their mission, having achieved remarkable successes along the way.

We received hundreds of nominations cast in favor of this year's honorees and a cast of other leading minds who will surely be recognized in years to come. We took time to vet each submission and interviewed each Trailblazer to find out what has driven them to reach success. In the pages that follow, I think you'll enjoy reading these short findings.

As with all Trailblazers supplements, the list is never complete. Our goal is to spotlight those making a big difference and the search never ends. If you have someone you feel should make our next list, please reach out and let us know. We hope you enjoy this special section and look forward to hearing from you with your nominations for next year's list!

Congratulations again to this year's honorees.

All the best,

Kenneth A. Gary
Vice President and Group Publisher, *The National Law Journal & Legal Times*

THE NATIONAL LAW JOURNAL

VP/GROUP PUBLISHER
KENNETH A. GARY

AD SALES, SPECIAL SUPPLEMENTS
LISA ANN VAN DYKE
LVANDYKE@ALM.COM
(202) 828-0351

EDITOR, SPECIAL SUPPLEMENTS
BRAD BLICKSTEIN

COPY EDITOR, SPECIAL SUPPLEMENTS
ASHLEY BENNING

ADVERTISING ACCOUNT REPRESENTATIVES
ROSEANN AGOSTINO, ALANA EZDERMAN, MARNIE MARONEY, BRIAN KLUNK, AND JOE PAVONE

LAW FIRM ACCOUNT MANAGERS
SUZANNE CRAVEN, ELIZABETH ELDRIGE, TRACEY GOLDVARG

CLASSIFIED ADVERTISING MANAGER
JAMES GUALT

PUBLIC NOTICE ADVERTISING
YONATHAN EYOB (WASHINGTON)

PRODUCTION MANAGER
SAMUEL WONG

PRODUCTION COORDINATOR
EVELYN FERNANDEZ

EDITORIAL (212) 457-9400

ADVERTISING (212) 457-9490

CIRCULATION (877) ALM-CIRC

REPRINTS (877) 257-3382

PRESIDENT & CEO
BILL CARTER

PRESIDENT/LEGAL MEDIA
LENNY IZZO

PRESIDENT/INTELLIGENCE, CHIEF DIGITAL OFFICER
JEFF LITVACK

VP/GROUP PUBLISHER
SCOTT PIERCE

CHIEF PRODUCT & CONTENT OFFICER
MOLLY MILLER

SENIOR VICE PRESIDENT/GENERAL COUNSEL
DANA ROSEN

SENIOR VICE PRESIDENT/HUMAN RESOURCES
COLLEEN ZELINA

VICE PRESIDENT/EDITOR IN CHIEF
DAVID L. BROWN

An ALM publication

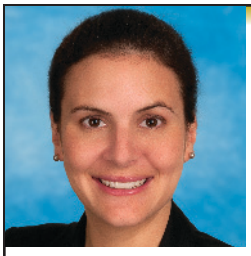
Jack Beard and Justin (Gus) Hurwitz

University of Nebraska

PIONEER SPIRIT Before law school, Gus Hurwitz's background was in computer science. "So cybersecurity has always been a part of my DNA." As an antitrust lawyer at the Department of Justice, his core research area was telecommunications, which faces many cybersecurity issues. Jack Beard served as associate deputy general counsel at the Department of Defense. "As a senior lawyer there, I got to see firsthand the ramifications inside the government and internationally as new technology got deployed, such as smart bombs and drones." At Nebraska, they bring the two elements together.

TRAILS BLAZED "We are skeptical of the perspective that is commonly represented in each of our domains," Hurwitz says. "We are trying to break down silos and get a broader perspective on what we can practically do to improve the state of play in the cyber domain." According to Hurwitz, much of the work around cybersecurity is being done through regulations, such as the Federal Trade Commission's "unfairness authority" to take action against organizations after data breaches. "It's randomly beating up companies." He's constantly pushing back against regulatory "silver bullets." "Every agency seems to want to be the new cyber regulator. I'm skeptical of all of them." Adds Beard, "If you go back to the old rules and the basis for why the laws were made, you just need to apply them to cyber problems."

FUTURE EXPLORATIONS "We've been floundering around so far. It'll get messier before it gets cleaner," says Hurwitz. According to Beard, the Internet was not designed for security. "When you are trying to fix things, privacy, freedom of speech and security all fight it out. Laws are one part of the solution, and new technology needs to be another."



Kate B. Belmont

Blank Rome LLP

PIONEER SPIRIT Kate Belmont focuses on maritime litigation and cybersecurity issues. "It is a new and developing area on the cutting edge."

TRAILS BLAZED The maritime industry straddles the globe and touches many areas. "What's special about the maritime industry is what they are responsible for protecting. In addition to data privacy and personally identifiable information, they protect cargo, the environment, human life and national security." Cyberattacks and data breaches can affect oil rigs, e-navigation on vessels and port operations. "The industry absolutely must focus on cybersecurity." Since the maritime industry has trailed many other industries on cyber issues, Belmont spends a great deal of time advising and educating clients on cybersecurity issues and best practices. "Over the past two years, I've been advising clients on the threats of cyberattacks in the maritime industry and how best to protect their systems, as well as how to respond if they have been breached." The maritime industry also does not have cybersecurity regulations. "This time last year, cybersecurity issues in the maritime industry were not widely discussed. But that has changed. There has been tremendous movement in the past year." In fact, the first-ever congressional hearing to examine cybersecurity at our nation's ports took place in October.

FUTURE EXPLORATIONS The maritime industry is responding to concerns about cybersecurity, as are governments and international bodies. The Coast Guard has launched a cybersecurity initiative and the International Maritime Organization will likely develop cybersecurity guidelines as well. "The maritime industry is responding, but it is only a matter of time until there is a front-page breach."

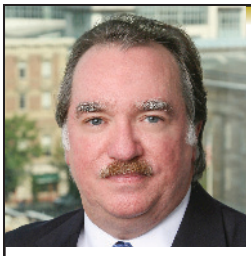
Mary Ellen Callahan

Jenner & Block

PIONEER SPIRIT As the third chief privacy officer for the U.S. Department of Homeland Security, Mary Ellen Callahan focused on cybersecurity issues. She consulted with experts to start systematically embedding privacy in cybersecurity regulations, which were in the early stages in 2009. She also assisted with the White House Cyberspace review.

TRAILS BLAZED While at DHS, Callahan created the cybersecurity subcommittee of the Data Privacy and Integrity Advisory Committee, which provides advice on programmatic, policy, operational, administrative and technological issues. The committee included those outside government, such as academics and advocates, some from the American Civil Liberties Union. "I got the entire subcommittee the highest level of government clearance. It was hard to get them cleared and involved, but it was a clear value add for the department and the federal government." She also involved her staff in the process and served on the executive team of a working group liaising between DHS and the National Security Agency. "It was all about making sure privacy was embedded into the cybersecurity framework for the federal government." Upon joining Jenner & Block in 2012, Callahan founded the firm's Privacy and Information Governance Practice. She has testified twice before Congress on cybersecurity issues, and her testimony influenced the recently passed House cyber bill.

FUTURE EXPLORATIONS Cybersecurity and the connected Internet-enabled ecosystem will become more and more important. "Companies need to integrate cybersecurity into overall risk management and realize it could impact the effectiveness of their business and products. They must deal with that upfront."



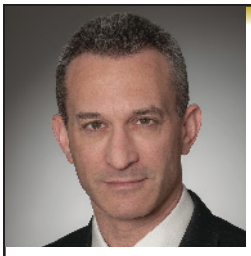
Emilio W. Cividanes

Venable LLP

PIONEER SPIRIT Milo Cividanes first became involved with cyber issues when he worked for Sen. Patrick Leahy in 1987-88 and served as counsel to the Technology and the Law Subcommittee of the U.S. Senate Judiciary Committee. The Electronic Communications Privacy Act had recently been enacted to overhaul wiretaps, and create new digitally stored data protections. "That's how I cut my teeth in the cyber arena."

TRAILS BLAZED Shortly after the California Breach Notification Law went into effect in 2005, LexisNexis experienced a cybersecurity matter with a company it had just acquired. Cividanes served as lead lawyer for LexisNexis through four congressional hearings, as well as an FTC investigation that lasted three years. More recently, he was part of the team that represented the CFO of Target at congressional hearings in early 2014 around the company's credit card breach exposure. "I've advocated successfully for the closing of numerous security-related government investigations." While these cases were reactive, he is also working with clients at the c-suite level and boards of directors to protect their businesses from cyberattacks and breaches. "We help them establish reasonable data security practices and procedures, even though what is deemed 'reasonable' changes all the time. The legal duty to provide security is constantly evolving."

FUTURE EXPLORATIONS New technology will allow companies and counsel to see vulnerabilities more clearly. "Cybersecurity is not a problem we are going to solve right away. It's first going to look worse, but that's part of the process of getting better."



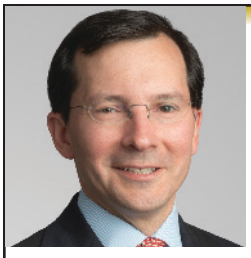
Adam I. Cohen

Berkeley Research Group, LLC

PIONEER SPIRIT In 1997, just a few years into his legal career, Adam Cohen took on a case about computer networks. "I had no background in anything technical." He became interested in computers, and then the Internet. "I fell in love with the technology but also the legal issues that Internet law was creating." In 2003, he published a primer on e-discovery, then shifted his focus to cybersecurity and became a Certified Information Systems Security Professional (CISSP). He moved to Berkeley Research Group in 2015, where he has focused on cybersecurity and overlapping areas such as e-discovery and information management.

TRAILS BLAZED Cybersecurity now touches everyone. "Lawyers are involved and looking for standards and best practices." He focuses on involving lawyers with the technical issues and helping them understand that there are no magic technological solutions. "We need to look at cyberrisk in an informed way." Much of his work is currently focused on security around mobile technologies. "The extent of exposure is impossible to overstate." Many mobile apps are capturing, storing and transmitting data, regardless of privacy policies. "People would be shocked if they knew." He is also looking closely at issues of cloud security.

FUTURE EXPLORATIONS Parallel to what happened in e-discovery, people are now trying to determine what is reasonable in terms of security practices. "The future will be a perpetual raising of the bar in terms of what are reasonable practices. It will be a constant effort that will require a constant devotion of resources."



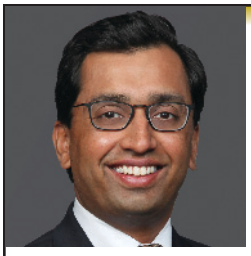
Gus P. Coldebella

Fish & Richardson

PIONEER SPIRIT After 9/11, Gus Coldebella was determined to go into public service. In 2005, he left private practice as a securities and corporate governance litigator to serve as deputy and acting general counsel of the Department of Homeland Security. There, Coldebella helped implement President Bush's Comprehensive National Cybersecurity Initiative, designed to shore up the government's civilian networks from attack and promote cooperation between public and private sectors. "Cybersecurity is where my two legal passions—national security and corporate governance—meet."

TRAILS BLAZED Now back in private practice Coldebella acts as "both a quarterback and a coach." "When I get a call that a client has experienced an attack, it's often their first time, but not ours. I'm gratified that I can manage the response, get answers to the legally relevant questions quickly, and help make informed decisions about disclosures, law enforcement involvement, and the like." In his coaching role, Coldebella advises companies, boards, CEOs and GCs about managing not only the primary risk of an attack, but the secondary risks of litigation, enforcement, and reputational harm. "While cybersecurity seems technical, I tell clients it involves the same kind of risk management that boards and executives have dealt with since time immemorial."

FUTURE EXPLORATIONS Coldebella continues to influence policy at NYU Law's Center on Law and Security and George Washington's Center for Cyber and Homeland Security. He believes the government's policy on cybersecurity has been disjointed. "Some agencies like FBI and DHS help victims of cyberattacks, but some other regulatory bodies have more of a blame-the-victim mentality, even when the attacker is a nation-state. Companies should demand a more rational approach." He also encourages victims to use the legal system when intellectual property is stolen. "We don't have to sit passively by; there are tools companies can use to fight back."



Rajesh De

Mayer Brown

PIONEER SPIRIT Raj De has a long background in national security and with the U.S. Department of Justice. "Serving as staff secretary to President Obama piqued my interest the most. I reviewed all the papers that went to the president, including security briefings. I got to see how big the threats are."

TRAILS BLAZED De next served as general counsel to the National Security Agency. "At the NSA, I was involved in three major areas of cybersecurity: making sure our intelligence community had the legal tools it needed to think about the emerging and evolving cyberthreat, helping to think through information assurance issues to make sure we protected the classified systems that the military and intelligence communities use and helping build the legal structure that other parts of the government use to deal with the types of hacks we read about every day." At Mayer Brown, De tries to think about cyber issues more holistically. "Rather than going straight to thinking about breaches, we want to consider how boards of directors are set to deal with issues and supply chain training issues. Thinking about it strategically is one way the firm breaks new ground."

FUTURE EXPLORATIONS De sees an evolution of cyberthreats. "It used to be about exploitation and theft, and then it started to be layered with disruption or destruction, such as the destruction at Sony. Many are now worried about the threat of manipulation—of data, data integrity or even physical items, with the Internet of Things." There has been an increased focus on putting in place better mechanisms for evaluating cyberrisk. "There's a lot of faith being put in the insurance industry to build models, but it will depend on the right data becoming available."

Jenny Durkan

Quinn Emanuel Urquhart & Sullivan LLP

PIONEER SPIRIT While Jenny Durkan was serving as U.S. attorney in Seattle in 2009, she was asked to join the Attorney General's Advisory Committee and chair the Subcommittee on Cybercrime and Intellectual Property Enforcement. "We were reenergizing and redefining how we address the threat of cybercrime."

TRAILS BLAZED At the Department of Justice, Durkan focused on three particular areas around cyber issues: raising consciousness of cyberthreats; retooling and building capacity to deal with both criminal and national security aspects of threats; and increasing collaboration, investigations and prosecutions. "The first required outreach and education for the public, business, local and federal law enforcement and the national security community. The second required concrete steps, reordering priorities and increased resources. The last involved retooling how the DOJ would use its enforcement capabilities to address new cyberthreats in both the domestic criminal and national security context." Now in private practice, Durkan helps businesses prepare and respond to the new reality. "Like the boxers say, everyone has a plan until they are punched in the face. The legal and operational impacts of a breach are that punch in the face."

FUTURE EXPLORATIONS In many ways, the war on cybercrime has been lost. But it is a pivotal moment now, and the situation is not irretrievable, according to Durkan. "This trend will continue without concrete steps to stop it. If we don't take action, we'll be in a difficult situation regarding personal and national security. How we do business needs to change. Hackers aren't sleeping. They are innovating, and we have to innovate as quickly to stay ahead of them."

Margaret P. Eisenhauer

Privacy & Information Management Services

PIONEER SPIRIT Peggy Eisenhauer has long been interested in technology. After working in-house for companies and at large law firms, she founded her own boutique firm in 2005. "Some of my clients are other law firms. There are other good privacy lawyers out there, but with my computer science background, I may be a bit more comfortable poking at the IT, technical and business process aspects."

TRAILS BLAZED Eisenhauer is an original member of the advisory board for the International Association of Privacy Professionals' efforts to establish the Certified Information Privacy Professional program (CIPP). The group felt it was important to have standards and a certification program, which has now been completed by several thousand people. "I was responsible for developing the law and compliance component and offering the training for that. If I've done anything for the profession, it's been to help create that entry level training for anyone who wants to do privacy law. It gives us all a basic grounding in the key concepts." Since January 2014, she has served as the program director for the Conference Board Council for CPOs. "It's a small group of A-list privacy companies. What we do is tackle the impossible questions, like: Are we measuring the right things? We are measuring what we can, but not necessarily what we need to."

FUTURE EXPLORATIONS There is a great deal of activity internationally, such as the invalidation of the Safe Harbor mechanism. "We are trying to understand what the rules will be. It's not a privacy issue; it's a political issue." The volume and velocity of security threats are enormous and accelerating. "All of that has to take privacy into consideration as well."

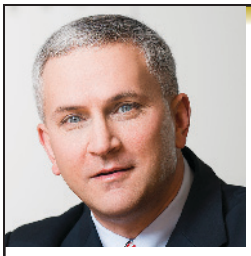
David N. Fagan

Covington & Burling LLP

PIONEER SPIRIT The convergence of privacy and national security brought David Fagan to the cybersecurity realm. "As more cyberthreats have focused on enterprises, it made sense that these two core areas of expertise came together."

TRAILS BLAZED Before California created the first notification law around data breaches, Fagan was involved in the first security-related Federal Trade Commission consent decree with Microsoft for its Passport service in 2002. "The decree did not involve an incident or breach. The FTC first started sticking its toe in based on statements the business would make and then tested whether its practices were consistent with statements. That was the first step." He has also helped set and negotiate the framework for how the U.S. government mitigates risks arising from cross-border deals. "The fact that a transaction needs regulatory approval can be the hook that allows the NSA to review it on cyber issues."

FUTURE EXPLORATIONS Laws apply to obligations between parties. They attempt to set bounds of behavior and develop and apply rules to regulate behavior. In turn, more laws emerge and courts apply existing laws in new ways as the need requires it. "As an example, hundreds of years of common laws, such as invasion of privacy, are being applied to the digital world." That trend will continue. "As long as interconnection grows, there will be bad guys to circumvent the rules and a continued expansion of what is being defined as cybersecurity law. But it is really the reapplication of existing laws for a digital age."



Jeremy Feigelson

Debevoise & Plimpton

PIONEER SPIRIT "When John F. Kennedy was asked how he became a war hero, he replied, 'They sank my boat.'" Jeremy Feigelson similarly got involved in cybersecurity simply because he had clients who needed help. "I came to the law with an interest in IP and technology before cybersecurity became a thing."

TRAILS BLAZED He learned early the importance of being comfortable with technology and being able to explain it to those without a technical background. His introduction came when he advised Sony BMG through the rootkit matter, when the music company placed copyright protections on millions of CDs that caused security issues. That led to investigations by more than 40 state attorneys general, a dozen class-action lawsuits and investigations by international regulators. "That matter created a template even for today: understand the technical facts and explain them to nontechnical audiences. They were also being hit on all fronts with legal and PR fire that intersected with each other." Feigelson and his team also conducted an independent investigation following Home Depot's highly publicized data breach 2014 and more recently helped achieve the dismissal of a class action against Viacom under the Video Privacy Protection Act, where plaintiffs claimed that children watching Viacom videos online were having their data unlawfully shared with Google.

FUTURE EXPLORATIONS Hackers will continue to look for new targets. "Companies are getting better at encryption, so hackers will start looking for the points in corporate networks where data is not encrypted. Hackers will increase attention on sectors like health care and places where there are soft targets." Early and effective adopters will find themselves in the best legal position following the inevitable breach. "There will be a convergence between legal standards and technology best practices."

Lindsey Finch

Salesforce.com

PIONEER SPIRIT In 2002, Lindsey Finch began her career at the FTC, where she started working on privacy, cybersecurity and protecting information online. "About half of American adults were using the Internet at that point, and cybersecurity was a critical issue." Finch left the FTC for law school, and after her first year, she moved to the Department of Homeland Security to serve as a privacy law clerk in the newly formed privacy office. She started at Salesforce in 2008 as the company's first privacy lawyer.

TRAILS BLAZED Tasked with educating people about safety online at the FTC, Finch had the enviable task of generating publicity for "Dewie the Turtle"—a cartoon turtle who joined the ranks of Smokey Bear as an animated government mascot. At Salesforce, Finch and her team of 12 lawyers work on distilling cloud-computing privacy and security issues and updates into terms customers can easily understand. "I have also worked on creating the legal foundation for protecting our customers' data."

FUTURE EXPLORATIONS As more businesses and sectors transition into the cloud, being able to rely on vendors and cloud providers to store data securely will become crucial. "Our customers can rely on us to be experts in this area and there is no finish line when it comes to protecting information." The future of cybersecurity is in every customer—from mom-and-pop operations to major international enterprises—demanding the highest level of protection, no matter what kind of data is being stored or processed. Companies need to be able to provide the tightest security across the board and remain vigilant all the time.

Suzanne Rich Folsom

United States Steel Corporation

PIONEER SPIRIT Currently the general counsel of U.S. Steel, Suzanne Folsom became deeply involved in cybersecurity while with a previous employer that provided private security. "When I came to U.S. Steel in January 2014, they had already had a significant data breach. So it made sense for the corporate legal department to take a leadership role around cybersecurity."

TRAILS BLAZED Folsom believes corporate legal departments must be involved in cyber issues within their companies because of the ever-changing rules and regulations that impact the space. At U.S. Steel, one of her first priorities was dealing with a hacking incident by five Chinese officials that had occurred in May before she arrived. "I immediately engaged a reputable third-party vendor to do a cybervulnerability assessment to help us better understand how to improve our program." Some aspects of the assessment included information and physical security management and awareness, compliance, threat vulnerability, identification and access management. She worked with corporate security, IT and the chief information security officer, along with the outside vendor. Since then, she has been working on mechanisms for breach detection and new security measures. "A key element is that employees need to be part of the plan and whether our people have the right level of training. We also make sure the board is properly informed."

FUTURE EXPLORATIONS Corporate America needs to be more vigilant and have better oversight in place. "Cyberthreats pose a risk as great as any other to even the mightiest companies and industries. A cyber incident can take down the small companies, and it can take down the big companies. It's a long-term war of survival." Companies need to be aware of and understand the global scope of the problem and put together plans that are forward-looking and evolving.

Joshua P. Galper

Personal

PIONEER SPIRIT Josh Galper began his legal career 15 years ago as one of the first attorneys in the privacy group at a major law firm. After stints in politics, he helped to build a crisis management group at another firm, where his practice focused on high-profile litigation, investigations and controversies that combined legal, regulatory and political and communications issues. "We were handling an increasing number of data breach incidents and privacy-related matters."

TRAILS BLAZED Galper joined the management team at venture-backed Personal in 2011 and is chief policy officer, general counsel and head of business development. The company provides personal clouds to individuals, teams and businesses to share and co-manage information. "Privacy and security are central to our architecture and vital to our users." But Galper focuses on more than cybersecurity. "Security is inextricably linked to privacy, and both are linked to our technology, product and business. They are all connected." He also serves as a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. "I bring the perspective of an emerging technology company and an understanding of the importance of user control and privacy."

FUTURE EXPLORATIONS Cybersecurity is critical to businesses today and cannot be relegated to a silo. "It's integral to every kind of business, and it needs to be built in from the beginning and not treated as an afterthought." One key trend he identifies is the convergence of cybersecurity, privacy and business. "Lawyers need to understand what engineers are doing as much as what the actual rules require."

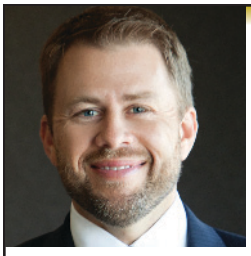
Matthew J. Gardner

Wiley Rein LLP

PIONEER SPIRIT Before law school, Matt Gardner worked for a tech startup, one of the first to sell firewalls. "System administrators would call in with tech problems. I also did a bit of coding, built two websites—and I got a taste of being a system administrator with concerns my own website would be hacked."

TRAILS BLAZED After law school, Gardner spent about nine years as a federal prosecutor. "Most of my time was spent prosecuting computer crimes. The forensics side of it appealed to me." He also worked with forensic experts to determine defendants' states of mind including through browsing histories, search terms, email artifacts and other methods. "Sometimes they were sophisticated and used proxies to hide who they were. We had to overcome these obstacles to make a case." In one of his last cases as a federal prosecutor, which is still ongoing, he investigated a conspiracy where the suspects communicated through TOR on the dark net. "We had to come up with creative techniques to identify individuals' TOR IP addresses."

FUTURE EXPLORATIONS Gardner believes more disgruntled employees or competitors will turn to hacking. "Sometimes, it will be just to vent anger, but others will use it to gain competitive advantage. The threat from sophisticated overseas actors is still present, but to deal with this local threat from insiders, general counsel and other responding lawyers are going to need a basic understanding of forensics." Lawyers will need to use information to make legal decisions, such as whether to sue an employee, take action against competitor or call law enforcement.



Nathan F. Garrett

Graves Garrett LLC

PIONEER SPIRIT Nathan Garrett first encountered cybersecurity issues as an FBI special agent and federal prosecutor in the U.S. attorney's office. He also served as chief of the National Security Section of the U.S. attorney's office in Kansas City. "At the time, it was more about national security and espionage. Cybersecurity was a national security issue, but it was not nearly as common as it is today."

TRAILS BLAZED After Garrett went into private practice, he eventually began working on data breaches. "This law is so new. It's not the time-tested ancient law you see in so many areas." While cybersecurity has expanded beyond national security concerns, the government has given it the highest priority. "What's at stake? Everything." With regulations such as the Sarbanes-Oxley Act, companies began to recognize cybersecurity as more than an accounting problem. "The government will seek to hold leadership accountable." He works to help clients protect themselves from attacks, respond competently and demonstrate a level of awareness to position themselves favorably for government investigations and litigation. "They need to show they acted with awareness and responsibility."

FUTURE EXPLORATIONS Garrett sees conflict at the government level between regulatory and law enforcement authorities over data breaches and cybersecurity attacks. "Law enforcement does not want targets to be concerned about contacting them. But the targets are concerned that if they call the cops, the regulatory people will be breathing down their necks. As we move forward, this conflict will be a big issue."

Francoise Gilbert

Greenberg Traurig, LLP

PIONEER SPIRIT Francoise Gilbert started practicing as a technology lawyer in 1986 and quickly saw issues with viruses, time bombs and other "nasty events." A founding member of the Cloud Security Alliance, she has worked to develop and study cloud computing.

TRAILS BLAZED About 20 years ago, Gilbert received a phone call from the state of Kansas looking for help. At the time, states were trying to understand the legal issues around telemedicine and whether it was worthwhile to develop a telemedicine program considering the risks to privacy and security. Working mostly pro bono, she advised what is now the Western Governors' Association on analyzing the related legal issues. "As part of that, I reviewed every single bill that involved the protection of health care records for six years in a row until finally HIPAA passed." She has also spent a great deal of time working on the Internet of Things and focusing on security awareness and programs, breach response and incident planning. "It's critical to raise awareness—everyone is paying for it."

FUTURE EXPLORATIONS Gilbert is focusing on smart es in particular. "Cities right now are preparing for the City of 2020, putting together all sorts of systems that talk to each other to make our lives better." Consider a major train derailment, which requires coordination of services. "But you need privacy and security so they only talk to each other when necessary and security systems can keep out hackers." A French native, Gilbert is also interested in global issues. "I'm trying to raise awareness on the international level of the concept of security breaches and bring some harmony to the ways that countries deal with these issues. There needs to be more consistency."

Yoram Golandsky

CybeRisk Security Solutions

PIONEER SPIRIT More than 20 years ago in Australia, because he was rooming with a professor, Yoram Golandsky had early access to an Internet connection. "I was playing around with it and realized it would create huge privacy and security issues." When he returned to Israel, he switched his career focus to technology.

TRAILS BLAZED Golandsky has adapted military war game methodology and applied it to private security in the corporate environment. In war games, the "red team attacks" and the "blue team" defends. "I started running red teams and war games with customers. We were pioneers in that area, but it's become quite common now." He expands war games from a technical cybersecurity incident to business issues. "We transform it to crisis management." About seven years ago he began conducting quantitative risk analysis and has applied it to many areas. In 2015, he became CEO of CybeRisk, which provides full cyberrisk advisory services. "We come to the board and assist in asking the technical team—the CIO and the CISO—the right questions."

FUTURE EXPLORATIONS Golandsky believes cybersecurity issues are still in their early stages. "We haven't seen anything yet." He predicts that in the next three to four years, someone will be able to hack into an airplane or power grid. "But it's not all gloomy. Cybersecurity will become a competitive advantage and a c-suite level priority." An enormous amount of information is being collected about everyone. "I'm scared of the moment when that might fall into the wrong hands." Golandsky also predicts rapid changes in legislation. "Traditionally, the law is behind technology, but we are going to have to see better definitions of privacy and when and how people can use information."

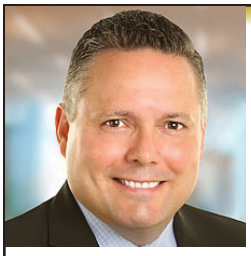
Adam Golodner

Kaye Scholer LLP

PIONEER SPIRIT Adam Golodner began working in technology and telecommunications in the 1990s, as the Internet was starting to grow. He did stints in the government, academia and in-house at Cisco Systems Inc., where he led the company's global cyber focus. He moved to Kaye Scholer in 2014 to lead the firm's Global Cybersecurity & Privacy Group. "I really have to take a holistic approach, especially globally."

TRAILS BLAZED Golodner has been very engaged in U.S. legislation around cybersecurity in his roles as a member of the White House's E-Commerce Working Group, the Department of Justice's Privacy Council and chief of staff for the DOJ's Antitrust Division. He has also been involved in broad trade areas between the United States, Europe, China, India, Russia and Brazil surrounding regulatory decision-making. "While at Cisco, I was able to help move the needle toward innovation and an open Internet. That helped to avoid some country-specific regulations that would have balkanized the Internet." Golodner also shares his holistic view in his work with clients. "I'm able to bring a big picture to decision-making on how to secure themselves and be good citizens."

FUTURE EXPLORATIONS Golodner is fundamentally optimistic about working through many of the current issues. "It'll be hard and requires work in technology and policy." He is also optimistic that global issues will be worked out between countries, companies and citizens. "Fundamentally the advantages of interconnectivity far outweigh the problems. It will not happen quickly and there will be bumps, but the benefits are so compelling, on balance we'll find our way through this."



David M. Hickey

Hickey Smith LLP

PIONEER SPIRIT David Hickey and his partners have been doing cybersecurity work for the better part of the last decade. His firm has been designed to deliver legal services more efficiently and securely. "From the firm perspective, the conclusion in every jurisdiction is that maintaining client confidences is fundamental to the practice of law, so it follows that cybersecurity is fundamental to the law practice. Maintaining it for the firm is mission critical. Every law firm should be doing it."

TRAILS BLAZED Becoming an adherent of cybersecurity by design changed the game for Hickey. "Every time we do a system, we think about cybersecurity right from the beginning. For example, when clients need to send HIPAA information across borders, we help companies keep cybersecurity in mind, with entire networks for moving medical information around the world." He also advises high-tech clients on embedding cybersecurity by design alongside privacy by design. Rather than bolting security on at the end, he ensures it is part of the design process. "By integrating it, you will have a much better chance of succeeding."

FUTURE EXPLORATIONS Hickey's firm is ISO 27001 certified. "We are one of few firms that are, but most should be. It's fundamental that we maintain our clients' confidences." Policies must be validated, challenged and reviewed on a recurring basis. "Once standards are met, it's all about monitoring them on a day-to-day basis and educating people. Everyone must take responsibility inside and outside the firm." He also foresees regulators becoming more involved and requiring companies to have cybersecurity plans. "More and more companies will be ISO certified and expect their law firms will be, too. I don't see it letting up."

Paul G. Karlsgodt

Baker Hostetler

PIONEER SPIRIT Paul Karlsgodt initially practiced in consumer class-action defense before becoming involved in privacy and health care. When Baker Hostetler launched a data privacy practice about five years ago, Karlsgodt became involved in some of the litigation-related matters.

TRAILS BLAZED Karlsgodt helped convince a California appellate court to dismiss all claims under the state's Confidentiality of Medical Information Act against Eisenhower Medical Center following its data breach in 2013. "It was one of the first cases that covered a lot of people under CMIA. The stakes were high, and the law was not really developed." Patience, a supportive client and a long-term strategy made the win possible. Karlsgodt also recently convinced a federal judge to dismiss a case against GameStop Inc. In that case, the judge found GameStop did not violate privacy policy by incorporating Facebook features into its subscription-based online gaming services and the plaintiffs didn't suffer economic loss because of the information dissemination. "The key question was, what can we collect from consumers and what do we have to tell consumers about what's been collected?"

FUTURE EXPLORATIONS The current wave of hacking incidents is not going away soon. Hackers are ahead of corporate America and know the vulnerabilities before companies can fix them. "Everybody is vulnerable. But on the positive side, we've seen significant progress toward protecting data when it involves theft or loss." Going forward, the ability to collect, store and manipulate data will increase, which will lead to more challenges. "There is a tension between profit potential versus the expectation of consumers."

Bernice Karn

Cassels Brock & Blackwell LLP

PIONEER SPIRIT Bernice Karn has worked with technology contracts since 2000, around the time the Canadian government enacted a new federal privacy law. "For better or worse, some firms didn't know where to point clients, but it seemed like an obvious adjunct to me."

TRAILS BLAZED Karn focuses on developing cybersecurity policies and cyber insurance. In one notable case, she represented a large media corporation that ran the Canada.com website before the privacy commissioner of Canada. The client was considering moving the website's hosting to the United States. "At that time, there was concern about sending data to the United States because of the U.S. Patriot Act." Karn demonstrated that the data wouldn't be less secure in the United States than in Canada, and the transfer was approved. "This case advanced the argument that a consent would not be required to move data to a third party, and that's become the accepted perspective in Canada."

FUTURE EXPLORATIONS While Canada has not historically had as active a class-action bar as the United States, the last 5-10 years have seen more cases of individuals bringing civil causes of action. "Companies are paying more and more attention to measures they take to protect their data. It's not really a question of if you'll be attacked, just when. The potential for class-action litigation in Canada will probably, like in the United States, lead to directors sued directly, shareholder activism and more cyber insurance." There has also been an increase in regulatory activism from the Office of the Superintendent of Financial Institutions. Karn predicts that a national privacy law with breach notifications will take effect in Canada soon. "Once that comes into effect, there will be much more to do."

James H. Koenig

Paul Hastings LLP

PIONEER SPIRIT Jim Koenig brings a legal, technical and business background to issues of cybersecurity. Along with his private law firm experience, he worked for several consulting firms, leading privacy and co-leading cybersecurity for PricewaterhouseCoopers and Booz Allen. "The consulting firms are more technical, but don't necessarily understand the rigor of the law. On the other hand, law firms are not as comfortable with technology. Having been on both sides, I always bring a one-stop solution for my clients."

TRAILS BLAZED Koenig has helped about one-third of the Fortune 100 deal with privacy, security and cyber-related matters. One the privacy side, Koenig has served as an expert to the FTC regarding what constitutes a comprehensive privacy program. "I was involved in all the major follow-cases, including the most recent mobile case involving Credit Karma." He has also helped many companies with data breaches with their responses to the breach, regulators and class-action lawsuits. Last year, he organized the HealthCare Cyber Town Hall, which included high level government officials, health care industry leaders and HITRUST, the industry organization, to talk about cyber issues and health care. Koenig also co-founded the International Association of Privacy Professionals.

FUTURE EXPLORATIONS Koenig sees increased segmentation of types of threats. "We're going see people start specializing in controls and approaches based on industry, the information they hold and specific attackers that would go after their institution." He also sees a more integrated approach from service providers, particularly law firms, that brings together lawyers, security officers, data scientists and cybersecurity specialists. "Why law firms? Because it's under privilege."

Brian Kudowitz

Bloomberg BNA

PIONEER SPIRIT Brian Kudowitz's background is in engineering and intellectual property, and his career has focused on technology and technology law. "Cyber is such an interesting industry in how the growth in technology is changing the risk profile. It's an underserved market. There is tremendous white space in terms of what can be created and delivered to privacy attorneys, information security providers and others."

TRAILS BLAZED At Bloomberg BNA, Kudowitz brings new products to market for data security, privacy and IP. He is the lead architect behind Bloomberg Law: Privacy & Data Security, a recently launched all-in-one platform. "I've built a new platform to streamline the workflow of privacy and data security attorneys and compliance professionals—particularly the aspect of their workflows that deals with problem-solving and developing privacy programs and advising clients." Kudowitz and his team developed the product after hearing about several different categories of needs: practitioners had a very fragmented workflow; the industry is inescapably global; and knowing what's happening today and yesterday is not quite enough since practitioners need to have an idea of what to expect tomorrow. "We provide a global news heat map, an upcoming law enactment timeline, in-depth risk environment profiles for 41 countries and a 'Chart Builder' tool that helps to streamline a privacy program for all the countries involved."

FUTURE EXPLORATIONS Today's practitioners have a lack of clarity and a low level of confidence. "There's a huge opportunity to provide that through data mining and analytics. It's an evolving area, so at the same time it's become more important for businesses to thrive in this field." A vast source of virtually untapped data can be mined to provide qualitative assessments and practice guides as well as analysis.

Ronald D. Lee

Arnold & Porter LLP

PIONEER SPIRIT Ron Lee first became involved in data security as general counsel of the National Security Agency in the mid-1990s. "It wasn't like the Internet was on the tip of the world's tongue." At the NSA, his clients had two missions—to generate foreign intelligence and to protect the government's information and information systems. After serving in the NSA, he worked on many of the same issues as well as counterterrorism and critical infrastructure protection as associate deputy attorney general in the Department of Justice.

TRAILS BLAZED Lee has spent much of his career focusing on the intersection of national security with industry and the private sector. "I've been trying to identify the issues and conflicts and to find some common ground. There is both promise and risk, so there's a need to mediate." To be effective, attorneys need to learn the technology, engineering and architectural bases that drive business, legal and policy areas. Privacy and security also represent enormous themes. "Sometimes they point in same direction; sometimes they are at odds."

FUTURE EXPLORATIONS The days of thinking about cyber law and cybersecurity as solely distinct disciplines could end. "It could happen that cyber issues will increasingly become something that any good lawyer has to be conversant in." All levels of government are increasingly grappling with cybersecurity and privacy issues. "Not just the federal government, but all levels of government are working to build services to do what the government needs to do, such as keeping track of health information."

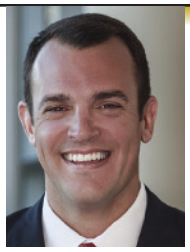
Richard M. Martinez

Robins Kaplan LLP

PIONEER SPIRIT Rick Martinez grew up building computers and writing his own programs. As a litigator, he focused on cases that involved computer hardware, software, memory and Web-based services. "I'm an early adopter, kind of a geeky guy by nature, so I saw how computers created opportunities but also risks."

TRAILS BLAZED For Martinez, advising clients on emerging risks has been of deep interest. "Obviously, responding to incidents that do occur in a wise fashion is important, but just as important is the counseling that gets done ahead of time. You need to identify not just technology risks, but the hand-in-glove relationship between tech consultants and lawyers." He does the same thing with emerging legal standards such as considering regulators and their priorities. "That's what plaintiffs are doing. People see what the law says, but they aren't seeing how standards are changing." Until a robust legal framework is in place, companies will need to plan for what's coming now and what's coming down the road.

FUTURE EXPLORATIONS Martinez sees an increased role for digital currencies, such as Bitcoin. "The financial industry is looking at Bitcoin technology to streamline and lower the cost of financial transactions. That will open up a number of other stressors." He also sees tension between the national security posture and the success of computer hardware companies and software services. "For example, there is sometimes a perception that U.S. hardware has back doors for the NSA. Competitors can throw this mud, whether or not it is true." He also sees risk around health care, particularly as it relates to the Internet of Things. "This can be handy for researchers with a lot of great stuff, but it also involves a lot of litigation and exposure."

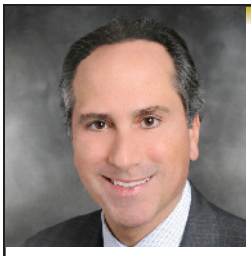

Edward J. McAndrew, Jamie M. McCall and Shawn Weede

U.S. Attorney's Office, District of Delaware

PIONEER SPIRIT Assistant U.S. Attorneys Jamie McCall, Ed McAndrew and Shawn Weede recently convicted three defendants in federal court in a first-of-its-kind indictment for conspiracy to commit cyberstalking with the intent to injure, harass and kill. "We follow the evidence. All these social media tools are a big part of every case we handle right now," says McCall. McAndrew agrees that all investigations are becoming cyberinvestigations. As chief prosecutor for the district, Weede's perspective is that "cyber is just another means by which people commit their crimes."

TRAILS BLAZED When unraveling the case *U.S. v. David Thomas Matusiewicz et al.*, prosecutors found a "vicious harassment campaign against the victim," McCall says. The case stemmed from a long-standing custody dispute between Christine Belford and her former husband David Matusiewicz. "He and his family launched a three-prong campaign to effectively assassinate Christine's character, with the intent of getting the children back. They used the Internet, YouTube, Facebook, physical surveillance and the mail. Ultimately, the family decided to murder her," says McCall. Since the federal system doesn't recognize a classic accessory to murder charge, prosecutors relied on the cyber component of federal stalking statutes, including the "resulting in death" element that is part of the Violence Against Women Act. According to McAndrew, a state-level charge of murder would have been underinclusive. "It wasn't a murder case that included stalking; it was a stalking case that resulted in a murder." Sentencing is scheduled for February 18.

FUTURE EXPLORATIONS "This is a very powerful tool that Congress has given us, that we found a new way to use," says McAndrew. Notes McCall, "It's a part of the Violence Against Women Act that allows for flexibility. We are hoping this case helps prosecutors to look at cases differently to avoid these crimes." Adds McAndrew, "The idea is to use this evidence before someone gets shot in a courthouse."



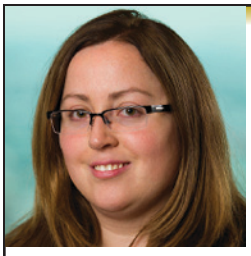
Mark Melodia

Reed Smith

PIONEER SPIRIT Mark Melodia took an early academic interest in cyberspace. For his senior thesis at Princeton University in 1985, he wrote on information and the law. Yet his early legal career focused on class-action and government enforcement defense, primarily in financial services. "When data breaches started, I was positioned to get some of the earliest cases in the battles involving class actions against financial institutions."

TRAILS BLAZED "Many of the arguments I used in the earliest cases are still in play." For example, in *Giordano, et al. v. Wachovia Securities,* he established that merely losing a copy of Social Security numbers and other personal information alone cannot support a class action. "That was the first federal court decision finding as a matter of constitutional law that absent real harm to the named plaintiff there is no standing to proceed. That's still usually the first defense in a data breach class action." That case was among the approximately 75 class actions Melodia has defended arising from data breaches or allegations of data misuse. Nearly a decade ago, he also oversaw some of the earliest class settlements for clients such as ChexSystems creating templates for how those settlements could win judicial approval. "What was then creative is now common."

FUTURE EXPLORATIONS Melodia, who co-chairs Reed Smith's Global Intellectual Property, Information and Innovation Practice Group and its Innovation Think Tank, is now focused on the Internet of Things and potential liability issues arising out of the proliferation of objects besides phones and computers that connect to the Internet, such as cars, medical devices and airplanes. "All those things collect data, which will continue to raise cyber issues."



Leah Mooney

Minter Ellison

PIONEER SPIRIT Leah Mooney's background is in insurance and corporate risk. "I became interested many years ago when insurers in Australia started to write cyberrisk polices. I saw that it was likely to become the pinnacle of corporate risk." That led to work developing insurance products, advising on policy wordings and helping insurers amend traditional policies to make sure cyberrisk wasn't covered where it was not intended to be covered. "We are trying to make them more cyberresilient."

TRAILS BLAZED While insurance is important, it's not enough, Mooney believes. "We have developed our own five pillars of cyberresilience. We were at the forefront of this in the Australian market." That involves having a plan, being prepared, having a board that understands IT issues, being invested and training employees. It also involves allocating risks contractually and understanding cross-border issues. Current legislation in Australia could reverse the usual allocation of liability, so Australian companies must understand their contracts and know where their servers are, where the risks lie and what the law is. Mooney is also working with insurers on the wording of traditional policies. "We're trying to help insurers close the gap with liability policy exclusions."

FUTURE EXPLORATIONS Cyberrisk and insurance with directors' duties will be a growing issue. "It's being considered in the United States with three cases, but not in Australia. But regulators in Australia have sent clear indication that cyberrisk is a matter of good governance." In Australia, legislation to require mandatory notification of data breaches is expected by the end of 2015, and the Commonwealth network has committed to it. "This will cause a big uptick in cyber insurance, and there will be a big regulatory cost."

Cinthia Granados Motley

Sedgwick LLP

PIONEER SPIRIT Before going into private practice, Cindy Motley worked at the Seventh Circuit Court of Appeals, so when she joined the private sector, it made sense for her to participate in a Seventh Circuit electronic discovery pilot program. As a litigator, she also handled class actions. "All of these areas merged, and it was a nice marriage of all my backgrounds into data security and privacy. I'm uniquely positioned because my experience has allowed me to focus on the preparedness aspect."

TRAILS BLAZED Motley has been advocating risk mitigation for years. "Having handled data breaches, it saddens me. You can't necessarily prevent a client from being hacked, but you can limit the exposure." She has developed programs for clients that take into account many factors, including knowing what information they have and where it is. She also suggests clients go on a "data diet." "They have more data than they need. I've worked on breaches with millions of records—all the way back to the 1960s." When companies get rid of old data, they limit their exposure in case of a breach. Motley has also worked on the insurance side. "Companies are more comfortable if they have better prepared insureds." Motley not only brings a breach response team when companies are hacked, she also brings a litigation readiness team.

FUTURE EXPLORATIONS Motley is bilingual, and some of her clients are involved with Latin American and European markets. "I anticipate more awareness of this as a global risk. They know this stuff is coming their way. They are bracing themselves."

John F. Mullen

Lewis Brisbois Bisgaard & Smith LLP

PIONEER SPIRIT Before law school, John Mullen worked with hospital computer information systems, where he gained an early understanding of technology. Early on, he worked with underwriters and brokers to do presentations for their risk management clients. "It helped drive cyberrisk sensitivity in the insurance world."

TRAILS BLAZED When claims first arose around data privacy events, insurance carriers referred him to the insureds. "Companies would call and say, 'We have an insurance policy with a certain carrier and may have been hacked. What do we do?' Our team developed a legal claims response protocol." Mullen's team also developed a standard litigation hold notification for when breaches occur, as well as a protocol for dealing with credit card-related breaches. "I basically fell into something that turned out to be awesome. Our team is viewed as understanding both the cyber insurance business and real-world business impacts of data privacy events." He was also among the first to start using 800 numbers to deal with cyber crisis management. "Carriers give 800 numbers to their insureds. The insureds call and their message blasts to 15 lawyers on the team and to critical players at the carrier. After less than an hour, we know what coverage is in place and we're already helping the insured. A lot of this is about customer service, and it's extremely market-facing."

FUTURE EXPLORATIONS Data privacy issues are not going away in the United States or the rest of the world. "The insurance aspect has really taken hold in the last five years. The market has only been penetrated 10-15 percent, so that means that the amount of premiums written will quadruple in next five to seven years. If you are on the other end of that and managing claims, it means there will be a lot more work. And it will grow in directions we can't predict."

Craig A. Newman

Patterson Belknap Webb & Tyler LLP

PIONEER SPIRIT Craig Newman's introduction to cybersecurity was pure happenstance. His litigation background enabled him to oversee a two-year global internal investigation. "This was 15 years ago, before cybersecurity was popular."

TRAILS BLAZED Since cybersecurity is an evolving area, Newman has developed a flexible practice. "I'm working on advising corporate boards' leadership and companies on cyberpreparedness and risk mitigation." Companies in the midst of data breaches that are in highly regulated fields also call on him for regulatory investigations and assisting the SEC. Much of his practice involves internal investigations. "Cybersecurity is a perfect storm—it is multidimensional, challenging and always changing." It's also an area where lawyers can make a difference by helping clients think proactively. "Most areas of law are not very proactive. With cybersecurity, you can move the needle to help clients prepare for a breach, put controls in place and manage the case ahead of time. The better prepared companies are, the better the response and the lower the cost."

FUTURE EXPLORATIONS Hackers are becoming increasingly sophisticated and developing a growing number of nondetectible viruses. That makes it more difficult for organizations to become cybersecure. On the other hand, companies are more aware now than ever, regulators are keenly focused on cyberrisks and the law is just beginning to evolve. "We are in the second inning of what I believe is going to become a very long and interesting ballgame."

Mauricio F. Paez

Jones Day

PIONEER SPIRIT Mauricio Paez has been playing the cat-and-mouse game of cybersecurity since before the law started to take shape. In law school, he realized he wanted to help companies commercialize technology for the Internet. "My dream was to get involved with international law, and Internet technology was the path. If you were dealing with this, you had to deal with data protection."

TRAILS BLAZED While the Internet bubble was in full swing in the late 1990s, Paez was primarily helping clients deal with security due to the European data restrictions. "I was in the right place at the right time." He has also done some work on the data exposure side. "At Jones Day, I'm in front of large multinational clients who are looking at the implications of technology, data, etc., through the business lens." Paez represents ICANN, the governing structure for domain name registrations. "Early on it became clear that for Internet governance work, it would have to be transparent. I was part of the team that created the requirements for data collection and retention for the domain name regulatory system." He founded the Data Breach Forum, a coalition of the Jones Day team and the Center for Democracy and Technology, to provide the best framework for data security notification laws in the United States. He is also actively involved in discussions with data authorities in Europe and part of the ABA Cybersecurity Task Force.

FUTURE EXPLORATIONS Paez predicts a 30-year cycle for cybersecurity. "First, companies reacted. Then they prepared. Now we are moving to offensively looking for the attacks that are coming." The trend will also be toward more localization of data, such as requirements for local data centers.

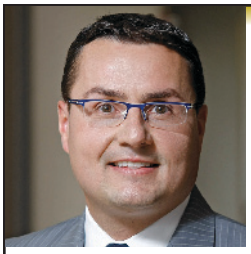
Harriet Pearson

Hogan Lovells

PIONEER SPIRIT When Harriet Pearson was named IBM's chief privacy officer in 2000, she was one of the first, if not the first, CPOs in the United States. IBM later named her its first security counsel, responsible for all cybersecurity, legal and policy matters.

TRAILS BLAZED Pearson joined Hogan Lovells in 2012, where she is lead for the Global Cybersecurity Group. "I figured that more and more companies would need real legal and policy expertise, and it would make sense to offer it from outside." She conducted a high profile privacy review for Uber and helped Home Depot handle its 2014 payment card breach. In 2013-14, Pearson led a coalition to shape a key section of the NIST Cybersecurity Framework focused on the intersection of privacy and cybersecurity. She currently co-chairs the Georgetown Cybersecurity Law Institute, serves on the ABA President's Cybersecurity Task Force and was on the CSIS Commission on Cybersecurity for the 44th Presidency.

FUTURE EXPLORATIONS Lawyers will become increasingly important in helping companies deal with the inevitable breach and also assisting them in managing risk. "I left a great company to enter private practice because I believe companies will need experienced lawyers at their side. It's not just about technologies; it's about policies and strategies." Since 80-90 percent of critical infrastructure is in the hands of the private sector, that's where the greatest amount of work will be done. "Informed and experienced lawyers need to be part of the solution, with management and the board."



Fernando M. Pinguelo

Scarinci Hollenbeck, LLC

PIONEER SPIRIT Fernando Pinguelo's interest in cybersecurity began in 2006 in the middle of a trial, when a company IT director who was a witness revealed an undisclosed technology glitch that caused data to resurface unexpectedly. "Dealing with a scenario like that required both a working knowledge of technology and creativity in applying long-standing legal principles and procedural rules to an unprecedented situation—in fact, it was the first of its kind in New Jersey."

TRAILS BLAZED Much of Pinguelo's practice involves crisis litigation. "I handle emergency applications in both federal and state courts seeking various forms of legal and equitable relief." Most recently, he has been retained to serve as local counsel to address a data breach reportedly involving the theft of millions of customers' sensitive data. He mobilized his team in conjunction with lead counsel efforts, filed a complaint, served nonparty subpoenas and secured highly important documents in less than seven days. "There are so many layers of local, federal and international laws that may be at play in any given situation." He also serves as national coordinating counsel for Opice Blum Advogados Associados. "Their practice has had one of the most influential impacts on the development of Brazilian jurisprudence in this area."

FUTURE EXPLORATIONS All eyes are on the FTC, particularly since the August 2015 Third Circuit decision affirming that the FTC could use the prohibition on unfair practices to challenge data security lapses. "When I recently met with FTC Chairwoman Edith Ramirez, she reiterated the important and increasing role she sees the FTC playing in the data security arena." Pinguelo also sees big data in a way similar to the Gutenberg printing press. "It promises to permanently alter the structure of society as we know it, but this time within a matter of years, not centuries."

Michael Rhodes

Cooley LLP

PIONEER SPIRIT Mike Rhodes began working on cybersecurity issues serendipitously. In the 1990s, he represented small software developers and companies with trade secret work. That led to issues concerning the Internet and digital music. From there, he became part of Cooley's privacy group. "You do one case, and you're the expert now because you've done one and they have done none."

TRAILS BLAZED Around 2001, Rhodes represented eBay in a dispute around the Digital Millennium Copyright Act. He did more work for eBay, then went on to represent other tech companies using his class-action experience. "They were always disputes over misuse of information." He also represented Facebook in the Beacon privacy class-action litigation. That case was appealed to the Supreme Court, which denied cert. He negotiated and finalized the settlement. "That created the Digital Trust Foundation, which eventually the Ninth Circuit Court of Appeals approved." Last year, Rhodes successfully argued motions to oppose class certification in the Gmail case where plaintiffs' claimed privacy violations. He has also done some litigation under the Video Privacy Protection Act.

FUTURE EXPLORATIONS Rhodes predicts that the first wave of privacy litigation has run its course. "What the company was telling you they were doing with your information wasn't very clear, so they would be sued for using information in different ways than they said they would." There will be more pressure on companies to protect information. There will also be more policy arguments around drones. "I was at an organic farm where the farmer uses his drone to test temperatures. It's part of the Internet of Things. And it's a question of how that gets used."

Alfred J. "Al" Saikali

Shook Hardy & Bacon L.L.P.

PIONEER SPIRIT As an associate, Al Saikali worked in litigation. As a partner, he was looking to build a book of business and distinguish himself. "This was 2008-9. I'm interested in technology, and privacy and data security stood out as an area that hadn't taken off yet."

TRAILS BLAZED Around that time, Saikali started a blog called Data Security and was brought in to spearhead the team advising a client that had suffered a cyberattack. Soon after he worked on a pro bono case involving a data breach that affected hundreds of thousands of individuals. "An employee had misused access to a database. We had to issue notices to all 50 states. That gave us the experience we needed, and it started to snowball. We've been hired by DuPont and other major corporations." Other experience-defining cases include defending a major university in a class-action lawsuit that arose from a data breach and several that involved credit-card skimming. Along with breach responses, he handled a case for a retailer that suffered a cyberattack affecting payment card information for individuals in over 150 countries around the world. "My practice is two parts: before the breach and after the breach."

FUTURE EXPLORATIONS Saikali sees a shift where courts are allowing class actions to proceed past the motion to dismiss and finding that a breach constitutes damages. "The plaintiffs' bar is getting very creative." On the proactive side, there are no silver bullets, "so instead, companies are bracing themselves with response plans and trying to shore up safeguards to prevent them from happening." He points to efforts to encrypt sensitive information. "If encrypted information is taken by a hacker, there is no need to notify under the law."

Andrew B. Serwin

Morrison & Foerster LLP

PIONEER SPIRIT Before becoming involved in IP licensing, Andy Serwin spent much of his time working on Internet content and unfair competition issues. "During the first dot-com boom, everyone was focused on content and felt the rules would be figured out later. There were no privacy lawyers, per se."

TRAILS BLAZED Serwin has worked on major FTC matters and represented Target on the data breach involving the theft of credit card and other personal information from up to 70 million individual customers. Yet one of his most notable accomplishments has been writing a treatise on privacy and security, "Information Security and Privacy: A Guide to Federal and State Law and Compliance," and "Information Security and Privacy: A Guide to International Law and Compliance." The three-volume set is collectively 5,000 pages and examines all aspects of privacy and security laws. "I may not be the world's expert, but I know it and I've written on it."

FUTURE EXPLORATIONS An advisor to the Naval Postgraduate School's Center for Asymmetric Warfare, Serwin believes cyberthreats will get worse before they get better. "Cyber is the ultimate asymmetric threat. You used to have criminals, the intelligence community and commerce, all in separate channels. But now we are all in the same pipe." Since the future is all about connectivity, the question will be how to manage risk in that environment. "We don't know yet. The old lines don't exist anymore."

Shahryar Shaghaghi

BDO Consulting

PIONEER SPIRIT Shahryar Shaghaghi began his consulting career at Andersen Consulting developing large-scale custom-built applications. At the time, information security was an afterthought; the focus was on mitigating the risks of viruses or malware. Even then, Shaghaghi prioritized data security. "Security has always been a component of my work. As the Web and cloud environment have matured, the information security landscape has become a far more complex challenge."

TRAILS BLAZED About 10 years ago, Shaghaghi joined Citigroup to lead the transformation of its IT risk management. "I took over all IT risk management implementations globally, reporting to the chief IT risk officer and head of operations and technology, and regularly updated the CEO and board of directors." At the time, Citigroup needed to strengthen its cybersecurity before it could continue with several acquisitions. "We had 18 months to meet the OCC's and FRB's regulatory requirements and bring the bank back to a satisfactory rating." So he fast-tracked the program, involving hundreds of implementation projects and resources—and made the deadline. "Fundamentally, everything I did at Citi has kept it relevant and created a framework for long-term success." In recent years, Shaghaghi has focused on cloud security and advising clients on different risk management scenarios.

FUTURE EXPLORATIONS As technology has become ingrained in many products and services, no industry is spared from the cyberthreat. "But to stay competitive, products also need to be user-friendly. The winners will be those that are designed with core security functionalities without compromising the user experience."

Richard A. Shutts Jr.

Harris Beach PLLC

PIONEER SPIRIT Before joining Harris Beach 15 years ago and becoming its chief information officer, Rick Shutts had a consulting business. "I had been meeting with law firms about increases in malware, cyberthreats and attacks. I started by talking about firewalls, but the firms didn't quite understand why they would need them. Then, I started at Harris Beach and realized there's a lot of interesting data, all of it considered by the firm and clients to be confidential. So it made sense to start thinking about security."

TRAILS BLAZED Shutts began by writing policies and processes. "We needed to document what we wanted people to do. With any project, you need a plan and you need documentation. About 12 years ago, this was pretty unique. Most firms are not doing this even now." He has hired a manager of information security, because the firm gets audited by a dozen clients a year in the financial services industry. "It takes a lot of time to complete the questionnaires; they are complicated and difficult to respond to." He also started education and training on information security for attorneys. "I explain why we have passwords, why we don't provide access to all people and other issues."

FUTURE EXPLORATIONS Shutts predicts more regulation for the legal industry. "Not just by our clients and not just by extension of regulatory bodies by our clients, but maybe by the ABA, state bar or state banking systems. We'll all be spending a whole lot more money on security, and things are getting more complicated. Cloud professionals will have the ability to make their systems more secure than most law firms can probably make theirs."

Rhea Siers

Zeichner Ellman & Krause LLP and The George Washington University Center for Cyber and Homeland Security

PIONEER SPIRIT Rhea Siers spent 30 years with the government working on cybersecurity and intelligence. "I was in cybersecurity before it was even 'cyber.'" Along with cyber operations, she is familiar with privacy and data issues, as well as threats in the cyber domain. When she retired from her government work at the NSA, FBI and Department of State, she went into academia. "I didn't think I'd be practicing law, but I appreciate getting companies to the right place in terms of cybersecurity."

TRAILS BLAZED Siers believes that companies have been too reactive. "We are working to really prepare companies ahead of time for incident response and create a successful cyber playbook. So when they have an incident, they are able to react." She also works with counsel to help them understand the true areas of risk. "A lot of the news reports are scary, but the key is to practice, practice, practice ahead of time."

FUTURE EXPLORATIONS There will be an incredible increase in regulatory practices related to cybersecurity, both at the state and federal level. "For example, state regulation on financial institutions will skyrocket. Also, the SEC will expect more protections." Companies will need to assess their liability in terms of insurance. "We will see a mushrooming effect in terms of what's appropriate and protects them through insurance." Boards of directors also need to have regular conversations about cybersecurity that are not too technical. "Especially in the legal practice, cybersecurity cannot be so exclusive. We need more people, and a lot have to be working on policy and law, not just technology."

Randi W. Singer

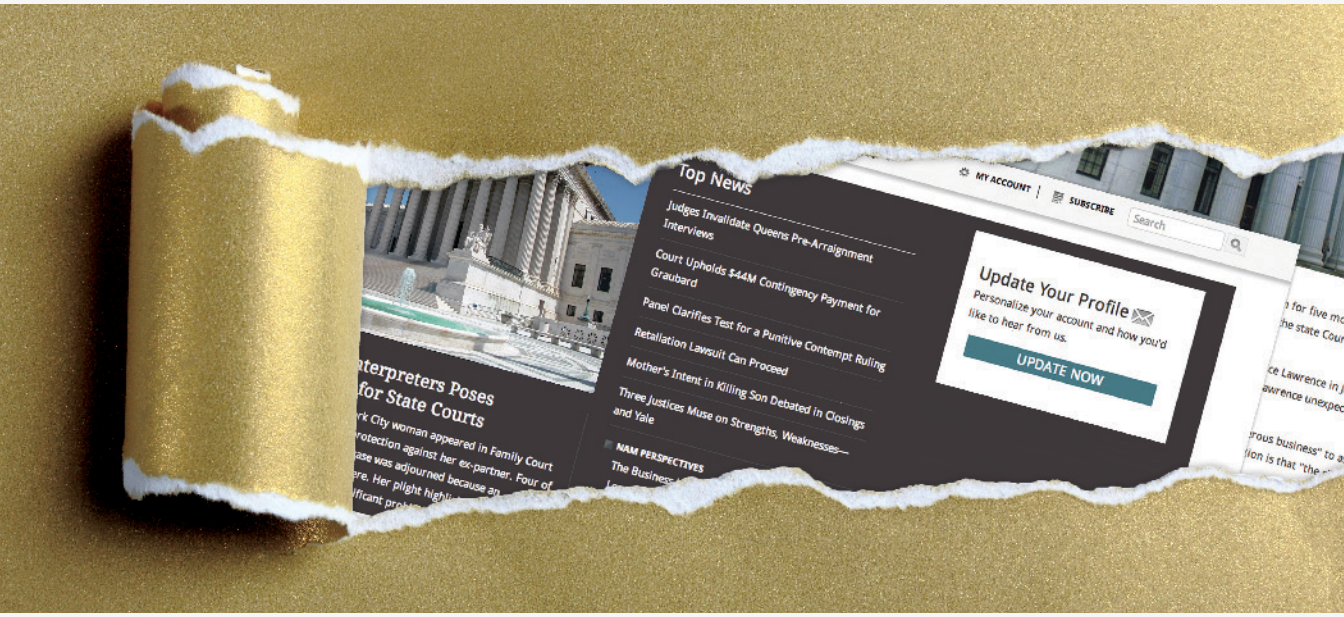
Weil, Gotshal & Manges LLP

PIONEER SPIRIT Randi Singer's willingness to work with technology goes back to her days after college as a theater administrator. "I ran a network and would literally have to repair it by tracing the wires, finding a static electricity buildup and releasing it—by shocking myself." She became involved in privacy from an advertising and IP background. "The issue was becoming how do you protect data that isn't exactly IP and doesn't fall into the trademark or patent or copyright bucket?"

TRAILS BLAZED Singer also focuses on privacy from a transactional perspective. "At Weil Gotshal, the spectrum of deals is fascinating. And you see the different ways that people approach things, and the concerns are different for different organizations." While there are certain areas that must be covered, Singer bases her approach on what clients are looking to protect. She also works to help companies define what personally identifiable information they have and what the parameters are to protect it. She aids companies by being sensitive to customers' expectations, such as when supermarket chain A&P went bankrupt and had to address customer information compiled through loyalty cards.

FUTURE EXPLORATIONS Many cybersecurity solutions are being driven by technology and self-regulation. "It's going take the courts forever to catch up, and legislation may not be fast either." That includes the ability to access information. In a global economy, policy regulations will also need to become more consistent. "It's untenable for companies to be subject to the laws of 50 states and suddenly have the rug pulled out in terms of data transfers from Europe." Lawyers also need to become more tech-savvy. "It's important for lawyers to be able to know if the IT people know what they are talking about."

THE NATIONAL LAW JOURNAL



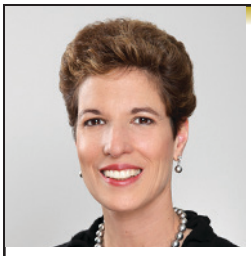
Give Your Clients a Gift with Real Value.

Grant your clients unlimited access to award-winning legal news coverage with an ALM Gift Subscription.

Get Started
Visit at.law.com/gift

NationalLawJournal.com

ALM



Lisa J. Sotto

Hunton & Williams LLP

PIONEER SPIRIT Lisa Sotto began doing privacy work in the early 2000s, when California passed the first data breach notification law. When the issue hit the national radar in 2005, she jumped in with both feet. Once, she was summoned to the Bahamas on a private plane to meet with the president of a hospitality company. "I spent the next five days dealing with one of the very first data breaches that involved an extortion attempt. I worked with Dick Hyde of Hill & Knowlton, an iconic figure in the risk world, to write the breach notification documents that still form a basis for what we do today."

TRAILS BLAZED Sotto next handled the data security breach at TJX and has handled more than 1,000 others since then. "That includes a data breach at a Fortune 100 company that hit between 80-90 million individuals in 78 countries." In the early days, the focus was on three issues: nation-states conducting advanced persistent threats looking for intelligence data, trade secrets and other information; traditional hackers looking for financial gain; and hacktivists pursuing an ideology. Now, there are many actions by nation-states looking for true spy data and information to jump-start industries.

FUTURE EXPLORATIONS After the demise of the U.S.-European Union Safe Harbor agreement, clients are transitioning to a system based on model clauses. "When the whole thing was declared invalid, 4,400 U.S. companies were scrambling to fix compliance gaps." The Department of Commerce and EU are working on the next version of Safe Harbor, and there is essentially a moratorium until the end of January. "But it's difficult because you can't put data transfer mechanisms in place so quickly. To do it fast means you are at risk of not putting a compliance program behind the mechanism."

Alexander H. Southwell

Gibson, Dunn & Crutcher LLP

PIONEER SPIRIT Alex Southwell first became involved with cyber issues as an assistant U.S. attorney in the Southern District of New York. "I was on duty and a child exploitation matter came in. From there I wound up doing a series of child exploitation cases." In one case, he faced a "virus defense" where the defendant argued he wasn't responsible for the computer's content. "That got me interested in the intersection of technology and law." His interest expanded when he started teaching and then went into private practice.

TRAILS BLAZED At the beginning of the "advanced persistent threat" era, when network intrusions became more sophisticated, Southwell represented a prominent executive search firm that faced a serious cyberattack. "We were able to quickly get a handle on what occurred and ultimately got the client's systems locked down and secured. We managed the fallout and got the client through the crisis." Data breaches today are getting more notoriety, which has led to congressional hearings and multiple class actions.

FUTURE EXPLORATIONS Southwell sees two trends playing out. The first is how the field develops as new technologies emerge. "You never know what new disruptive technologies will emerge, but the law will often be a step behind." Uber, and the regulatory and legal issues it has faced, is an example. The second issue is the global scope of the issues and conflicts that arise. "The bad guys don't follow political borders. Someone can be anywhere in the world, and that can lead to challenges in terms of conflict of laws."

2016 THE NATIONAL LAW JOURNAL

TRAILBLAZERS

Do you know attorneys who have changed the way law is practiced?

The National Law Journal is now accepting nominations for the 2016 Trailblazers!

We are looking for legal professionals who have moved the needle in the legal arena in terms of ADR, defense, new strategies or types of court cases, technological innovation, strategy, billing or any other significant improvement.

Below are key dates for the 2016 Trailblazers:

ADR Champions Trailblazers

Publication Date: February 29, 2016

Nominations Close: December 23rd, 2015

Submit your nominations to Lisa Van Dyke at
LVanDyke@alm.com

LAW.COM

One login. Access to all your legal news.

Your legal news coverage is now available all in one place. You can customize your news to follow the clients, competitors and cases that matter to you. Plus, you can enjoy on-the-go reading with the Law.com app and receive daily headlines to your inbox.

Law.com brings you award-winning coverage from journalists steeped in both the practice and business of law.

Get Started Now

Visit at.law.com/LawNews

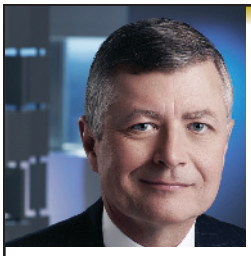
R. Jason Straight

UnitedLex

PIONEER SPIRIT Jason Straight became involved in the intersection of law and technology when he did forensic and e-discovery work to help lawyers use technology in their cases. "I was in the right place at the right time to get exposed to some data breach response work in the mid-2000s. I started to get involved in cyberprivacy. I liked it and saw potential, so I started committing myself to it more and more."

TRAILS BLAZED One of Straight's major focuses has been to help lawyers understand the role they play, not just in responding to data breaches but in managing cyberrisk overall. "I've been explaining to lawyers that it's not just something you can leave to the IT department. Now there are a lot of people saying different versions of that, but it was very different 10 years ago." He also works to demystify technology for lawyers. Action is most urgent during a data breach. "I've used my role many times to make sure my team is providing the kind of actionable intelligence and information that will help lawyers provide the ultimate client with good legal advice." The corollary is bringing legal and IT professionals together to talk about cyberrisk and understand each other's perspectives and priorities.

FUTURE EXPLORATIONS Straight believes issues of cybersecurity and privacy will get worse before they get better. "I wish I could be sunny about the overall state of global cybersecurity and privacy. We are a ways away from a system of global privacy laws; they are now very often in conflict with each other." Lawyers will be well-served by learning about cybersecurity and privacy. "It will make them much more effective counselors."



Mark Szpak

Ropes & Gray

PIONEER SPIRIT Mark Szpak has been a litigator for more than 30 years. His practice spans all types of cases, including consumer cases, which is how he became involved in the recent wave of class actions around retail and credit card breaches. "When these break, there are instantly class actions all around the country, filled with issues of first impression."

TRAILS BLAZED In privacy and data security cases, attorneys and clients are immediately confronted with a range of problems. "A maelstrom of challenges is foisted on you and the client overnight from multiple fronts." Along with consumer class actions, companies also face actions by payment card brands and financial institutions, and state, federal and international regulators and state attorneys general. Szpak immediately recognized the significance of *Clapper v. Amnesty International*, which reiterated the requirements for Article III standing. "We flagged it for analyzing the injury-in-fact requirement in data breach cases, both in articles and in our cases. That issue has had an enormous impact in these cases generally." He has also worked to emphasize putting expert forensics at the forefront of handling these cases and maintaining privilege around the effort.

FUTURE EXPLORATIONS Regulators and courts are starting to develop a more sophisticated sense of data security issues. "Everyone agrees there is no such thing as perfect security. And the hackers are smart. So is your hack really actionable?" Big data continues to present issues of collection and retention versus use. People are also beginning to recognize that hackers are interested in all types of data, not just personally identifiable information. "As a part of every company's operation, security will only grow both compliance-wise and in terms of litigation."

Brookes Taney

Epiq Systems, Inc.

PIONEER SPIRIT Brookes Taney started his sales career at Epiq Systems six years ago working in the corporate services division, which prints and mails millions of checks per month. That's where his work in data breaches began, and where he returned after several other roles at the company. "We handle breach response, and if companies need to notify customers or patients, we do the mailings and set up the call center."

TRAILS BLAZED In Epiq's first year handling breach response, they notified about 300,000 people. In 2015, it will be around 50 million. Epiq typically gets this type of work from the insurance companies underwriting cyber policies or the attorneys handling the breach remediation on behalf of their clients. Taney has heard from plaintiffs' lawyers that in order to reduce the number of class-action lawsuits filed, the affected individuals must come away feeling satisfied with the outcome of the situation. They've told him that the worst-case scenario is when customers or patients sit on hold for 10-20 minutes trying to get information about an unfortunate, inconvenient incident. "I've driven home how important customer service is. We've changed the industry view on how the customer can walk away feeling satisfied and remediated so they don't file a class-action lawsuit."

FUTURE EXPLORATIONS Taney believes there will be more regulations globally around data breaches. Currently, only the United States and a few other countries have rules requiring notification when a breach occurs. "We'll see a lot of growth around the world as they create those regulations." He also predicts a wider variety of monitoring tools for data breaches, such as health care monitoring. "Overall, there's no way to stop data breaches."

Danielle Vanderzanden

Ogletree, Deakins, Nash, Smoak & Stewart, P.C.

PIONEER SPIRIT Before going to law school, Dani Vanderzanden was involved with several privacy-related pro bono cases as a paralegal. "This was back before it was a big focus, but it fostered my interest." As a lawyer, she first focused on employment law. As electronic discovery became more of an issue so did questions of privacy. "Massachusetts was the first state to have a written information security program requirement, and I was heavily involved in that before co-founding the Data Privacy Practice Group at Ogletree."

TRAILS BLAZED Vanderzanden works with clients to get them ahead of the curve. "The FBI says there are two types of companies—those that have been breached and know it and those that have been breached and don't know it. I meet with chief privacy officers, boards of directors and human resources to try to help companies in the first instance be aware of what their obligations are and then respond." She also advises on cross-border discovery issues. "I have been actively involved with the e-discovery side of privacy issues with multinational companies with records located in multiple jurisdictions, even if the litigation is based in the United States."

FUTURE EXPLORATIONS Vanderzanden believes the vast majority of breach and hack situations involves some human failure along the way. "The best approach to managing the problem will be effective information governance practices, ongoing employee training and creating a culture of security and awareness." Companies should work to improve internal protections. "It really will require a meaningful cultural focus on how we equip everyone who touches sensitive data with the tools—technical and knowledge-based—to be able to act safely every time they touch a computer."

Michael Vatis

Steptoe & Johnson LLP

PIONEER SPIRIT Michael Vatis began his legal career 20 years ago, working on national security matters with the Department of Justice. While there, he helped lead the development of the first policies regarding critical infrastructure protection. After some of that work touched on cyber issues, he became more deeply involved in the area.

TRAILS BLAZED While at the FBI, he was named founding director of the National Infrastructure Protection Center. "The real moving of the needle was starting the government policy on cyberattacks of all sorts. Developing policies and organizations to deal with these issues laid the foundation for what exists in the government." Now in private practice, he is able to manage sophisticated threats from sophisticated actors, such as advanced persistent threats from nation-states that endanger a company's existence. Vatis also co-founded the Steptoe Cyberblog, which features articles, interviews and opinions. Its success led to the January 2014 launch of Steptoe's Cyberlaw Podcast. "The podcast is opinionated and informal. We have a very significant audience. It's exciting and fun."

FUTURE EXPLORATIONS Cyberthreats will continue to increase at a dramatic pace. "There's really nothing you can do to keep out a sophisticated adversary that wants in. Given the existing technology, you have to figure out how to minimize legal, economic and reputational risks." Another issue will be international data transfers and their restrictions from places such as the European Union. "What does the move to data localization requirements portend? It can create chaos in international business. It would have a detrimental impact on the world economy."

Patrick J. Whalen

Spencer Fane

PIONEER SPIRIT Pat Whalen has been to law school and business school, and he's worked with software startups so his background in legal, business and intellectual property has allowed him to pursue cyber law, often on behalf of financial institutions, which were at the epicenter of cybersecurity issues. "When these opportunities started presenting themselves, no one had been doing cyber work. So if you had some understanding of legal and technology, you had an opportunity."

TRAILS BLAZED Going back to the late 1990s, Whalen has chaired ABA committees relating to cyber issues. Fifteen years ago, he litigated one of the first data intrusion cases. "There was no blueprint, but I developed a playbook." While he still does some post-breach litigation and negotiations, most of his focus is at the front end, proactively counseling clients to create risk mitigation plans. "Then, when a breach occurs, I help companies deal with dozens of issues and stakeholders. I'm like the captain of a multidisciplinary team."

FUTURE EXPLORATIONS Whalen predicts more class-action litigation in the short term. "Up until a couple of months ago, it was hard for plaintiffs to get standing, but case law is developing rapidly." Legislators at all levels have also been very active. "They will get more robust in the regulations they impose." Whalen also sees organizations putting together holistic teams that bring together IT, data security, risk, insurance and law firms. There will continue to be inevitable trade-offs between ease of access and data use with security. He points to the TSA as an example. "We may need to trade some convenience for security. Now, the balance is toward ease of use, but it will have to become more aligned."

2015 BEST OF THE NATIONAL LAW JOURNAL

Winner | Citi Private Bank | Attorney Escrow Services
Business Bank
Private Banking Services
Wealth Management/Financial Asset Advisory Provider

Private Bank

Law Firm Group

Trusted by Am Law's top-ranked firms, Citi Private Bank Law Firm Group has provided innovative banking services to lawyers and their firms for more than 40 years. From credit solutions and investments to custody and escrow assistance, we deliver tailored solutions to help clients achieve their goals. Please contact us to learn more.

Naz Vahid
Law Firm Group Head
mehrnaz.vahid@citi.com
212.559.9236

Dan DiPietro
Law Firm Group Chairman
dan.dipietro@citi.com
212.559.8645

citi®
The World's Citi℠