

# Internet Safety, Security & Privacy



ORRICK



#### ORRICK AT A GLANCE:

- *Chambers and Partners'* 2011 Global, Europe, Asia and USA editions named **125 Orrick attorneys as leading global practitioners**, and recognized an unprecedented number of Orrick practices
- More than **1,110 lawyers in 23 major markets** across North America, Europe and Asia

#### INTERNET SAFETY, SECURITY & PRIVACY PRACTICE AT A GLANCE:

- More than **30 lawyers and professionals** — five of whom are former government prosecutors
- A dedicated eDiscovery and investigation team with **24-hour response capabilities** based in our Global Operations Center
- Advised clients on **major data breaches, liability for online content** and business model risks
- Took down three spam networks, reducing the world's spam levels by **an estimated 30 percent**

# Internet Safety, Security & Privacy

## TABLE OF CONTENTS

Internet Safety, Security & Privacy . . . . .	1
An Interdisciplinary Approach: Legal and Technical Expertise . . . . .	2
An Interdisciplinary Team: Credentials Snapshot . . . . .	4
Defensive Counseling and Risk Management . . . . .	6
Enforcement and Proactive Measures . . . . .	9
Selected Team Member Bios . . . . .	13



# Internet Safety, Security & Privacy

Through its work for companies like Facebook, LinkedIn, MySpace and Microsoft, Orrick, Herrington & Sutcliffe has emerged as a preeminent law firm for Internet Safety, Security & Privacy.

Our interdisciplinary team — cutting across multiple practice areas and global jurisdictions — counsels companies to manage their risk and enforce their rights regarding online security threats across a range of areas.

Orrick's longstanding work in this area has fostered strong relationships with regulatory bodies, law enforcement and trade groups, and yielded a widely recognized string of courtroom victories. Our team understands the practical and business implications of managing risk in the Internet era and has spent years developing strategic approaches to a host of challenges and enterprises.

# An Interdisciplinary Approach: Legal and Technical Expertise

Helping companies navigate the borderless online world and the patchwork of legal regimes that govern it requires a global team that can work seamlessly across nations and legal disciplines. Orrick's team also works at the forefront of legal knowledge — testing, refining and creating emerging law.

Our attorneys possess the technical and practical experience required for helping Internet businesses manage risk and combat online misconduct. Orrick lawyers work on an array of critical issues in this space:

## DOING BUSINESS ONLINE

- Advertising; Behavioral Targeting
- Adult content
- Affiliate marketing
- Cloud computing
- Consumer and child protection
- Content filtering technology
- Contracts
- Data and personal privacy: Encryption, federated identity, digital signatures, Public-Key Infrastructure (PKI)
- Digital rights management
- e-Discovery/data retention
- File hosting and peer-to-peer technologies
- Gambling, lottery and gaming
- Intellectual property: Copyright, Trademark, Trade Secrets
- Insurance
- Internet revenue models
- IT Infrastructure and agreements
- Legislative efforts and public strategies
- Licensing
- Offshore financial structures and institutions
- Online communities and environments
- Online payment and transactions
- Outsourcing transactions
- Search engine optimization practices
- SEC disclosure rules
- Security standards, certification and accreditation (ISO etc.)
- Social media platforms/tools
- Terms of Service
- User-generated content

## FRAUD AND THREAT PROTECTION

- Account hijacking
- Anti-spam, spyware, phishing, viruses
- Botnets and abuse infrastructure
- Confidence crime and scams
- Counterfeit and forgery
- Cybersquatting/typosquatting
- Credit card theft and fraud
- “Click” fraud
- Computer abuse and privacy in the European Union, China, Russia and elsewhere
- Computer hacking and trespass
- Data “scraping” and collection
- Denial of Service attacks
- Defamation/libel
- Extortion/threats
- False impersonation
- Obscenity
- Piracy of content and software
- Rogue infrastructure providers
- Software flaws and “bugs”
- Unfair competition

## NAVIGATING THE LATEST STATUTES

- Anti-Cybersquatting Consumer Protection Act
- Bank Secrecy Act and anti-money laundering
- CAN-SPAM Act
- Children’s Online Privacy Protection Act
- Communications Decency Act
- Computer Fraud and Abuse Act and similar statutes
- Data Protection Directive
- Digital Millennium Copyright Act
- Distance Selling Directive
- Domain name laws and regulations
- E-Commerce Directive
- Economic Espionage Act
- Electronic Communications Privacy Act
- European Cookie and Privacy Laws
- European Intellectual Property Law
- Fair Credit Reporting Act
- Federal Trade Commission Act
- Gramm-Leach-Bliley Act
- HIPAA
- RICO and other racketeering
- Sarbanes-Oxley Act
- SEC Cybersecurity Disclosure Rules
- Stored Communications Act
- UK Computer Misuse Act (hacking)
- UK Copyright Law

# An Interdisciplinary Team: Credentials Snapshot

## EXPERIENCED ATTORNEYS FROM ACROSS THE GLOBE:

- In addition to our U.S.-based attorneys, litigation and technology law counsel in Europe and Asia with experience investigating and prosecuting actions against computer abuse and crime.

## FORMER GOVERNMENT PROSECUTORS:

- The former U.S. Attorney who chaired the U.S. Attorney's National Computer Hacking and Intellectual Property Committee;
- A former Assistant U.S. Attorney who has handled complex financial crime cases involving Internet-based fraud, money laundering, Bank Secrecy laws and asset forfeiture;
- A former Assistant U.S. Attorney who prosecuted computer crimes and was a member of the Justice Department's Computer Crimes and Intellectual Property Unit;
- A former Federal Trade Commission trial lawyer who focuses on matters involving Internet advertising, privacy protection and data breach issues;
- A former senior special agent with the U.S. Department of Homeland Security assigned to the Financial and Trade Investigations Division, investigating money laundering, terrorist finance, bulk currency smuggling and bank, wire and identity fraud.

**PUBLIC RELATIONS AND LEGISLATIVE STRATEGISTS:**

- A Public Strategies and Crisis Group experienced in managing media exposure resulting from high-profile legal crises and interacting with government to manage legislative affairs.

**TECHNICAL KNOWLEDGE:**

- Eighteen attorneys with a bachelor's, master's or Ph.D. in computer science or computer engineering.

**e-DISCOVERY PROFESSIONALS:**

- A team of staff attorneys trained in complex Internet investigations enabling Orrick to rapidly assess large volumes of data and pursue offenders immediately.

**Orrick Internet  
Safety, Security  
& Privacy Team**

**IN-HOUSE FORENSIC INVESTIGATIONS:**

- A sophisticated infrastructure to support in-house investigation of Internet abuse, including dedicated Internet and computer forensics labs and testing resources.

# Defensive Counseling and Risk Management

We focus on legal and technical issues at the core of Internet business. This includes helping clients with business management, regulatory compliance, customer and employee protection, brand policing, and overall risk profile analysis. We work with companies to evaluate online revenue models and ensure optimal results in light of the thicket of legal issues affecting online commerce.

Our defensive counseling and risk management work for clients generally falls into three categories:

**Expertise with Internet Business Models.** Orrick has been at the forefront of online business since the Internet's first commercial breakthroughs. We are familiar with online revenue streams and monetization. We understand the behaviors of users, customers and third parties who interact online with our clients. We have sophisticated expertise in drawing the line between aggressive business models and unacceptably high risk. We're experts in the underlying technologies and familiar with the web of relationships underlying the online business world.

## SELECTED EXAMPLES:

- Developed content review policies and practices to comply with the Digital Millennium Copyright Act and ensure responsible handling of users' copyright infringement.
- Advised a social search company regarding product design issues and best practices to manage potential liability regarding copyright and other intellectual property issues.

- Supported major online services provider in telemarketing and e-marketing efforts directed toward subscribers and potential subscribers, and implementation of privacy safeguards.
- Advised social networking site on data protection compliance and information disclosure under EU Data Protection laws.

**Legal and Regulatory Depth.** How do you respond to a call from the State Attorney General about your online ads? What do you do when a class action suit is filed claiming that a hacker stole your customers' data? Who is responsible for copyright infringement or inflammatory speech by users in your online environment? What must go in your Web site's terms of service, and what should you leave out? What are you required to disclose to the public in SEC filings regarding cyber attacks and data security issues? Managing risk from Internet activities triggers many legal and regulatory uncertainties. Orrick's team can help you ask the right questions and find the best answers.

#### **SELECTED EXAMPLES:**

- Advised an online business on how to contain a hacking incident in which customer account information was compromised, including management of FTC investigation and class action lawsuit.
- Defended major online retailer in FTC investigation related to online behaviorally-targeted advertising policies and practices.
- Defended software company in lawsuit alleging injury as a result of purported security vulnerabilities in the company's products.
- Represented social media company defending against legal proceedings in France over fake user profiles of politicians and artists.
- Defended user generated content platform against allegations of copyright infringement brought by a music publisher.
- Advised several U.S. technology companies entering into agreements with EU-based purchasers and navigated them through the EU electronic, Internet and privacy regulatory framework.
- Conducted legal Web site audits for European multinationals from marketing to financially regulated businesses.

**Practical Solutions.** Orrick lawyers understand that building a thriving online business requires cost-effective risk management solutions. To this end, our team helps clients prioritize potential and existing risks. We have created workable programs for assessing and resolving user misconduct, devised technical infrastructure to protect companies, and helped manage exposure through creative contractual and insurance arrangements. Our team strives to provide practical counsel that will not impede business operations.

**SELECTED EXAMPLES:**

- Represented a global gaming company in insurance coverage matters after a hacking incident and data breach.
- Helped client develop a cease-and-desist program to deal with software piracy on peer-to-peer networks.
- Reverse engineered and inspected a malware product delivered through client's online platform and advised on legal implications.
- Advised an instant messaging services company regarding potential exposure regarding IM system interoperability features.
- Advised software company regarding legal methods by which company could "clean" software on user computers after computers were subject of a malware attack.
- Implemented anti-spamming and similar IT protection tools for European clients.
- Advised technology companies on how to comply with EU data protection legislation regarding the transfer of personal data outside of the EU.

## Enforcement and Proactive Measures

Our attorneys, investigators, computer forensics professionals and Internet security specialists are experienced in identifying, locating and prosecuting cases against defendants involved in a variety of Internet abuses.

The team has brought enforcement actions against cybersquatting/typosquatting, copyright/trademark infringement, online advertising fraud and financial fraud, as well as security threats such as trade secret misappropriation/corporate espionage, spam, phishing and malware. Applying its broad experience and technological resources, the team works effectively to disrupt and deter malicious activities and to protect companies, brands and customers. Our enforcement and proactive measures work for clients generally falls into four categories:

**Investigation Infrastructure.** Orrick's technical infrastructure supports rapid and thorough investigations of Internet abuse, including dedicated Internet and computer forensics labs and testing resources in Orrick's Global Operations Center. The team is experienced with a variety of industry-standard tools and has also developed its own proprietary investigation technologies.

### SELECTED EXAMPLES:

- Identified three major fake pharmaceutical spam operations. We identified three China-based and two Russia-based participants and hundreds of discovery leads to pursue as "Doe" defendants. We are pursuing a lawsuit to disrupt the organization and push deeper toward high-level participants.

- Unraveled a complex spam e-mail campaign, which included participants from the U.S., Argentina, Russia and Bangladesh. Tracked defendants through physical monitoring and technological means to pursue them and serve process through international treaties, as the defendants fled the U.S.
- Investigated and initiated international civil litigation and law enforcement referrals against an “advance fee fraud” ring based in India and Nigeria.

**Practical Experience.** Dealing with a spectrum of evolving online wrongdoing has given the team deep insight into how malicious actors carry out and monetize misconduct, where they shift assets, how they evade enforcement, and what weaknesses consistently undermine their schemes. This experience allows the team to prioritize its efforts, apply the best investigative and legal tools, anticipate common problems and intelligently use resources for investigation and enforcement.

#### SELECTED EXAMPLES:

- Initiated a John Doe lawsuit to disable 276 domains that controlled the 400,000 computer “Waledac” botnet, capable of sending nearly 1.5 billion spam e-mail messages per day. This action was the first civil action of its kind.
- Initiated a John Doe lawsuit to disable 96 IP addresses and thousands of domains that controlled the million-computer “Rustock” botnet, capable of sending 30-40 billion spam e-mail messages per day — the single largest source of spam in the world. This action decimated a massive criminal enterprise.
- Prosecuted action against Web site publisher and internet traffic provider in a novel Internet case related to “click” fraud and related fraudulent online advertising practices.
- Successfully pressured international adult content companies and financial institutions in Curaçao and other “offshore” venues to share information leading to specific defendants engaged in IP infringement and other online abuse. Many such sources were located in countries with no civil discovery relationship or treaties with the United States.

**Legal Expertise.** Orrick’s attorneys have legal expertise in all areas necessary for a successful enforcement strategy, including intellectual property, computer abuse, unfair competition and commercial and criminal law. The group has brought novel actions resulting in new law to curb Internet abuse and

understands the complex procedural tactics necessary to enforcement. This expertise extends far beyond the U.S., as the team includes lawyers located everywhere Orrick operates, including China, Russia, Germany, Italy, France and the UK.

#### SELECTED EXAMPLES:

- Identified and brought actions against many major U.S.-based “cybersquatters” responsible for thousands of domains infringing our clients’ trademarks. We have achieved significant settlements, including monetary recoveries and transfer of infringing domains to our clients.
- Successfully implemented enforcement program to disrupt pirated software distribution through offshore file-sharing and peer-to-peer networks.
- Brought action on behalf of major social networking site against a rival site creator’s attempts to illegally circumvent client’s terms of service by employing a combined “spoofing” attack on the site, resulting in the extraction of hundreds of thousands of e-mail addresses and sending of thousands of spam e-mail messages.
- Assisted several major pharmaceutical companies in identifying and tracing online distribution of counterfeit drugs, initiated raids against the counterfeiters, worked with customs officials to stop distribution and followed with administrative sanctions against the counterfeiters.

**Relationships.** Orrick’s dense network of relationships spans diverse and disparate institutions including domestic and international law enforcement, government, academia and policy groups. These relationships allow Orrick to tackle the most complex cross-border Internet misconduct, pursue both legal and legislative solutions, and to refer matters to law enforcement agencies throughout the world.

#### SELECTED EXAMPLES:

- Identified and sued a Canadian defendant, part of an Eastern European-based criminal organization responsible for an enormous volume of fake pharmaceutical and adult spam e-mail. Tracked defendant’s location and retained a former FBI agent to pose as an industry participant and serve the complaint on the defendant when he attended a conference in the U.S.

- Investigated and traced sources and distribution networks for counterfeit goods in China, including successful raids and seizure orders, working closely with China's local administrations for industry and commerce (AICs), public security bureaus (PSBs), State Food and Drug Administration (SFDA), General Administration of Quality Supervision, Inspection and Quarantine (GAQSIQ), Chinese Customs and Chinese courts.

## Selected Team Member Bios

Orrick's Internet Safety, Security & Privacy Practice comprises numerous attorneys and professionals based across the globe who can provide seamless and comprehensive service to clients. Below is a list of key practitioners:



**Neel Chatterjee** (*Partner — Silicon Valley*)

Neel is a recognized expert on Internet law, privacy and Web security issues and has been leading Internet security investigations and litigation since 1998. He participated in some of the first online antipiracy enforcement investigations, litigated the first civil case under California Penal Code 502(c), has obtained the largest civil judgment to date under the Federal CAN-SPAM Act and has litigated numerous first impression cases involving computer trespass and hacking of Web sites.



**Russell Cohen** (*Partner — San Francisco*)

Russell represents technology companies in critical litigation matters, particularly in the areas of insurance and antitrust. He has particular expertise relating to cyber and data breach coverage, and is currently representing Sony in pursuing property and liability insurance claims arising out of cyber attacks on its online gaming, video and music networks. He also has represented a large computer hardware company in pursuing coverage for data loss resulting from employee sabotage. Russell also has extensive experience litigating antitrust claims involving technology products, and has represented Microsoft in numerous matters of this kind.



**Richard DeNatale** (*Partner — San Francisco*)

Rich's practice focuses on complex commercial litigation and trials, with a special emphasis on insurance recovery matters. He has a great deal of experience with data privacy and cyber-torts. Earlier this year, he was retained by one of the world's largest electronics companies to pursue insurance coverage for claims and losses arising out of cyber attacks on the company's online customer networks, which according to press reports resulted in the largest data security breach in history. Orrick is representing the company in coverage lawsuits in New York and California. DeNatale is also representing a major travel Web site in pursuing defense and indemnity coverage for more than 40 lawsuits around the country related to alleged tax liabilities.



**Beth Goldman** (*Partner — San Francisco*)

Beth is an established expert in trademark and copyright law, licensing, Internet and advertising law and protects some of the world's most valuable brands. She leads a very successful group that polices Internet trademark misuse and brings civil enforcement actions and UDRP proceedings against parties engaged in cybersquatting/typosquatting and other brand abuses. She has been actively involved in the International Trademark Association and has handled many domain name policies and dispute procedures.



**Paul Gupta** (*Partner — New York*)

Paul's practice focuses on representing Fortune 500 and other clients in district courts and courts of appeals. He handles intellectual property, IT and antitrust matters in the computer, e-commerce, outsourcing, telecommunications and Internet industries. He has also carried out antipiracy enforcement actions involving software and other technologies.



**Frédéric Lalance** (*Partner — Paris*)

Frédéric is chair of Orrick's European Litigation Group and focuses on commercial matters as well as arbitration and alternative dispute resolution. He has acted as lead litigation counsel for Facebook in France in all disputes involving Internet safety issues, and has litigated numerous cases involving online fraud, intellectual property rights infringement, libel and privacy. Frédéric is regularly asked by the legal press to comment on online security and risk management issues.



**Thomas McConville** (*Partner — Orange County*)

While serving as an Assistant U.S. Attorney in the Central District of California from late 1996 to early 2007, Tom was a member of the Computer Crimes and Intellectual Property (CCIPS) Unit. He worked closely with the FBI on investigations and prosecutions involving denial of service attacks, computer intrusion and phishing. At Orrick, Tom's connections and credibility within the CCIPS community have facilitated law enforcement referrals of IP infringement and computer hacking matters on behalf of clients.



**Sam Millar** (*Partner — London*)

A former general counsel at a global derivatives trading firm, Sam has significant experience with in-house data protection issues, including data subject to access under the UK's Data Protection Act. His practice focuses on regulatory investigations, litigation and eDiscovery, and he has worked with IBM UK on large tech litigation matters. He has also advised a leading technology company in relation to a dispute involving a UK government IT outsourcing contract and a global counterfeiting operation.



**Gabriel Ramsey** (*Partner — Silicon Valley*)

Gabe has extensive experience litigating cases against malicious actors engaged in fraud, abuse and technical threats. He has led enforcement efforts against defendants involved in spamming, online advertising fraud and scareware, phishing and malware distribution. He also led a team that obtained court orders dismantling the “Rustock,” “Waledac” and “Kelihos” botnets—each capable of sending billions of spam e-mails a day—and has experience combating IP abuse, data theft and network intrusions.



**Garret Rasmussen** (*Partner — Washington, D.C.*)

A former FTC trial lawyer, Garret focuses on FTC matters involving Internet advertising and privacy protection issues. He has represented several companies that have been the subject of security breaches and has successfully petitioned the FTC to initiate investigations regarding conduct harmful to our clients. He regularly advises companies on strategies for managing data breaches and online advertising practices.



**McGregor Scott** (*Partner — Sacramento*)

A former U.S. Attorney for the Eastern District of California from 2003 to 2009, Greg chaired the national Computer Hacking and Intellectual Property Committee for U.S. Attorneys, which coordinated the DOJ's efforts on hacking and IP policy, enforcement and legislation. In addition, he served as the U.S. Attorneys' representative on the DOJ High Tech Task Force.



**Stephanie Sharron** (*Partner — Silicon Valley*)

Stephanie is an experienced transactional lawyer with expertise in all facets of IT infrastructure, cloud computing, software, new media, e-commerce and Internet business models. She regularly advises on transactions, licensing arrangements and risk-management strategies involving data access, security, outsourcing, intellectual property, content, proprietary technologies and technical infrastructure. She has addressed these matters in the context of mergers, acquisitions and other strategic relationships and deals. Recently, Stephanie has negotiated a multinational collaboration for the development, hosting and operation of a cloud-based mobile payment service, as well as a wireless, cloud-based system for the automotive industry.



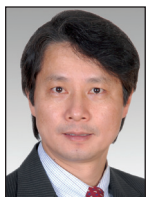
**Kolvin Stone** (*Partner — London*)

Kolvin advises on commercial transactions where technology, intellectual property and digital media are the focus. This often includes counseling on privacy laws and regulation affecting technology and the Internet. Kolvin regularly negotiates and drafts complex commercial agreements and technology transactions, often on a cross-border basis, including advising on technology licenses, content licenses and digital distribution agreements, SaaS agreements, supply, distribution and development agreements, services agreements, franchise agreements, terms of business and outsourcing agreements.



**Thomas Zellerbach** (*Partner — Silicon Valley*)

Tom has extensive experience helping clients address a wide range of Internet safety issues, including phishing, hacking, cybersquatting and typosquatting. He has expertise regarding online advertising and brand protection matters. Clients he advises in this area include social networking, online gaming, consumer services and other kinds of companies.



**Xiang Wang** (*Partner — Beijing, Shanghai, Silicon Valley*)

Xiang is the lead partner for Orrick's China-focused intellectual property practice and is the administrative partner-in-charge in our Beijing office. He has extensive experience representing both foreign and Chinese companies on technology-related matters, such as anti-piracy efforts and social media, as well as litigation. He is one of the only IP lawyers who has a doctorate in electrical and computer engineering, a Chinese Certificate of Laws and admission to practice law in New York, Indiana and before the U.S. Patent and Trademark Office.



**Noël Chahid-Nourai** (*Senior Counsel — Paris*)

Noël is a leading authority on data protection and government affairs in France. He served for many years as a member of the French data protection authority, where he was in charge of banking and insurance sectors. Noël's data protection practice has involved advising numerous highly regulated multinationals, and he has extensive experience on cross border flow of information.



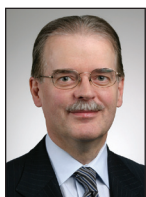
**Laura Becking** (*Of Counsel — New York*)

Laura is a member of Orrick's Global Corporate Solutions Group. She has significant experience with international data privacy and data protection regimes. Prior to joining Orrick, Laura worked for a major international consulting firm and its allied law firms in Europe, Tokyo and New York.



**Wendy Curtis** (*eDiscovery Of Counsel — Washington, D.C.*)

Wendy consults with Orrick attorneys and clients on eDiscovery strategy in litigation matters. She has been engaged by Fortune 100 companies and major financial institutions to create and deploy eDiscovery and records and data management programs.



**Clifford Michel** (*Of Counsel — New York*)

Cliff regularly represents clients in matters concerning patent, trademark, copyright and trade secrets litigation, antipiracy enforcement actions, technology licensing, Internet domain name disputes, securitization of intellectual property, privacy, document retention and information security.



**Andreas Splittgerber** (*Of Counsel — Munich*)

Andreas's practice focuses on matters connected to data privacy and IT security compliance, as well as Internet and media law. He works with the firm's M&A teams to assist on IT and IP matters. He frequently advises companies on other IP and technology-related transactions such as licensing, distribution, consultancy and outsourcing agreements.



**Antony Kim** (*Senior Associate — Washington, D.C.*)

Tony regularly advises and represents clients before the FTC on a broad range of data security and privacy issues with a focus on online practices involving the collection and use of personal and financial information for marketing/advertising purposes.



**Joyce Chen** (*Managing Associate — New York*)

Joyce assists U.S.-based multinational corporations with cross-border intercompany issues, particularly with respect to data privacy compliance management.



**Jeffrey Cox** (*Managing Associate — Seattle*)

Jeff concentrates his practice on technology with an emphasis on software and computers. He worked in software development as a Lead Program Manager with Microsoft and as a Software Product Senior Manager with both Compaq and Digital Equipment Corporation, giving him significant technical experience with computer software and hardware. Jeff has substantial experience investigating and litigating cases involving online advertising fraud, spam and malware.



**Jacob Heath** (*Managing Associate — Silicon Valley*)

Jake has a broad background in white collar criminal issues, anticompetitive conduct and commercial disputes. He has substantial experience investigating and prosecuting enforcement actions against online fraud, spam, malware and botnets. Within the team, Jake has specialized experience concerning international procedural issues, such as service of process and discovery, as well as investigating and locating defendants and assets.



**Emily Somers Tabatabai** (*Managing Associate — Washington, D.C.*)

Emily is a member of the Antitrust and Litigation groups and the Consumer Protection and Privacy practice. She has advised clients on an array of consumer protection and privacy issues, including data privacy and security compliance and procedure, online privacy, sales/warranties, HIPAA and marketing and advertising issues.



**Dan Barry** (*Associate — London*)

Dan advises clients in relation to their online business and intellectual property requirements. This includes advising on terms of service, privacy matters and all online regulatory requirements, in particular clients with global businesses. In addition, Dan helps clients to protect their brands across multiple jurisdictions.



**Jeffrey McKenna, CIPP** (*Career Associate — San Francisco*)

Jeffrey is a member of Orrick's eDiscovery Working Group. His work focuses on eDiscovery strategy and data privacy issues. He also works with outside counsel and IT professionals to implement effective strategies to get the best results during the discovery phase of active litigation, while minimizing risk and reducing cost.



**Mark Coleman** (*Network Security Engineer — Global Operations Center*)

Mark has over 15 years of experience investigating and assessing network security threats of all types, referring threats to law enforcement and designing and installing security systems to counter such threats. He is highly experienced with network communications, connectivity and routing protocols. Mark maintains the team's Internet investigation lab at the Global Operations Center and has substantial experience conducting technical investigation of online schemes.



## ABOUT ORRICK

Orrick is an international law firm with more than 1,100 lawyers located throughout North America, Europe and Asia. The firm traces its roots back to 1863 and, since that time, we have expanded our practice groups and extended our global reach with one core strategy in mind—focusing on solutions and results in response to our clients' current and future needs. Our size, resources, geographic breadth, advanced IT systems and business-oriented culture ensure that our clients receive responsive, value-added services. Orrick's depth and breadth of experience include a wide range of transactional and litigation matters. Orrick lawyers are committed to providing high-quality, innovative solutions to the most complex legal challenges.

### TRANSACTIONAL

Banking and Finance  
Capital Markets  
Compensation and Benefits  
Emerging Companies  
Energy  
Global Infrastructure  
Mergers and Acquisitions  
Outsourcing and Technology Transactions  
Public Finance  
Real Estate  
Restructuring  
Structured Finance  
Tax

### LITIGATION

Antitrust and Competition  
Commercial Litigation  
Employment Law  
Insurance  
Intellectual Property  
International Arbitration  
Mass Torts and Product Liability  
Public Policy and Government Affairs Practice  
Securities Litigation and Regulatory Enforcement  
Supreme Court and Appellate Litigation  
White Collar Criminal Defense and Corporate Investigations



ORRICK

UNITED STATES | ASIA | EUROPE

[WWW.ORRICK.COM](http://WWW.ORRICK.COM)

---

Orrick, Herrington & Sutcliffe LLP | 51 West 52nd Street | New York, NY 10019-6142 | United States | tel +1-212-506-5000  
Attorney advertising. As required by New York law, we hereby advise you that prior results do not guarantee a similar outcome.