

## Alexander H. Southwell



### Contact:

200 Park Avenue  
New York, NY 10166-0193  
Tel: 212.351.3981  
asouthwell@gibsondunn.com

Alexander H. Southwell is a partner in Gibson, Dunn & Crutcher's New York office and is co-chair of the firm's Information Technology and Data Privacy Practice. His practice focuses on counseling a variety of clients on privacy, information technology, data breach, theft of trade secrets and intellectual property, computer fraud, national security, and network and data security issues, including handling investigations, enforcement defense and litigation. In particular, Mr. Southwell regularly advises companies victimized by cybercrimes and counsels on issues under the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and related federal and state statutes. Mr. Southwell additionally handles a range of white-collar criminal and regulatory enforcement defense, internal investigations, compliance, and complex civil litigation matters. An experienced trial and appellate attorney, prior to joining the firm, Mr. Southwell served as an Assistant United States Attorney in the United States Attorney's Office for the Southern District of New York.

### Recent significant engagements include:

- Represents Register.com in civil litigation brought by a search engine customer concerning the domain hijacking of the customer's domain in a cyber-attack and in the related internal investigation.
- Represents Facebook and Mark Zuckerberg in a breach of contract action brought by an individual in Federal Court in Buffalo, New York alleging an ownership interest in Facebook.
- Represents a prominent U.S.-based online company in its interactions with the United States Department of Justice related to automated attacks on the company's website, which resulted in the indictment and conviction of the attackers.

- Represented Facebook in an investigation into its privacy and safety policies and procedures by the New York Attorney General's Office, which resulted in a groundbreaking settlement that has been hailed as a model of compliance.
- Represents a former high-ranking executive under criminal investigation for theft of trade secrets in violation of the Economic Espionage Act and unauthorized computer access by the Southern District of New York United States Attorney's Office.
- Counseled a Fortune 50 company concerning its corporate information security policies.
- Represents a leading provider of integrated technology solutions for satellite communications-interfaced systems concerning anonymous postings to an online bulletin board intended to damage the company's stock price.
- Represented a company related to a criminal referral of two former employees who illegally accessed the company's computer systems and stole trade secrets. As a result of the representation, the Southern District of New York United States Attorney's Office brought criminal charges against the two former employees.
- Counseled a leading resort company concerning its corporate information security and social media policies, as well as network security and data breach incident response plan.
- Represented an online retailer in responding to a data breach and coordinating with law enforcement concerning the security incident.
- Counseled a prominent individual concerning online reputation management.
- Represented the leading provider of data solutions to financial institutions in a putative class action for alleged violations of the Fair Credit Reporting Act related to reporting individuals apparently matching those on the Office of Foreign Asset Control's list of foreigners against whom economic sanctions have been imposed.
- Assisted a national trucking company with the removal of anonymous attacks on their business posted to a blog.
- Conducted an investigation for a financial institution related to anonymous e-mail attacks directed at a top executive.
- Assisted the leading non-profit digital library on a pro bono basis, regarding compliance with federal child exploitation law and law enforcement interactions.
- Counseled a leading hospitality company concerning a government inquiry related to computer network and related data security breach.
- Counseled an electro-mechanical components manufacturer related to a criminal referral

of a trade secret theft of engineering drawings and schematics.

- Represented a prominent independent school in New York, on a pro bono basis, related to cyber-safety issues for students, faculty, and administration.
- Represents a major retailer in an internal investigation and defense of grand jury investigation and OSHA investigation related to workplace incident.
- Assisted Gibson Dunn partner who served as Independent Monitor for a medical device company pursuant to a Deferred Prosecution Agreement with the United States Attorney's Office in New Jersey, including revising health care compliance policies and training and ensuring compliance with the Anti-Kickback Statute and other relevant health care laws, regulations and corporate policies.
- Represented a private equity principal and fund in the public corruption "pay to play" investigation being conducted by the New York Attorney General's Office and the Securities and Exchange Commission.

Prior to joining the firm, Mr. Southwell served as an Assistant United States Attorney in the United States Attorney's Office for the Southern District of New York from 2001 through 2007. As a member of that office's CHIPs unit, Mr. Southwell investigated and prosecuted computer hacking and intrusion cases, intellectual property offenses – including matters arising under the DMCA, the Economic Espionage Act and the criminal copyright and trade secret statutes – as well as other high-technology offenses, with a particular focus on the telecommunications industry. Additionally, Mr. Southwell served as one of the District's resident technical advisors and legal counselors to prosecutors and agents on electronic search and seizures and technology issues and worked on outreach, training and prevention with law enforcement and the digital community. Mr. Southwell also focused on investigating and prosecuting cases under the federal securities laws, including accounting fraud, insider trading, fraudulent offering of securities and market manipulation. In addition, Mr. Southwell prosecuted a wide range of cases including wire and mail frauds, insurance fraud, public corruption, Foreign Corrupt Practices Act violations, Bank Secrecy Act violations, identity theft, firearms crimes, tax offenses, child exploitation and immigration crimes. As a federal prosecutor, Mr. Southwell tried a dozen felony cases and handled over a dozen appeals before the Second Circuit Court of Appeals.

#### Significant government investigations and prosecutions included:

- Investigated and successfully prosecuted computer hacker for unlawful distribution of trade secrets under the Economic Espionage Act for his possession and sale of a stolen copy of the source code for Microsoft Windows products with a significant reported decision interpreting the Act and with media coverage including in New York Times and online media.
- Investigated and successfully prosecuted a number of individuals on criminal copyright

charges for manufacture and sale of pirated computer software, including one who trafficked in over \$1 million worth of counterfeit software and who was sentenced to over three years' imprisonment.

- Investigated and prosecuted individual who ran a sophisticated Internet image distribution system dedicated to the dissemination of child pornography, including successfully trying the nation's first jury trial of a child pornography "F-Server" case and successfully petitioning for mandamus during trial with extensive media coverage including in New York Times.
- Investigated and successfully prosecuted former IT consultant who hacked into client's computer systems in retaliation for fee dispute.
- Investigated a number of cyber-extortion attacks in the financial services industry, usually involving foreign nationals.
- Successfully prosecuted a children's voice and drama teacher for attempting to entice a minor to engage in sexual activity over the Internet and traveling from New Jersey to New York to engage in sexual acts with a minor.
- Investigated telecommunications companies and individuals related to allegations of unlawful call routing with extensive media coverage including in Wall Street Journal, Washington Post and New York Times.

Mr. Southwell is also an Adjunct Professor of Law at Fordham University School of Law where he teaches a seminar on cybercrimes, covering computer misuse crimes, intellectual property offenses, the Fourth Amendment in cyberspace, computer evidence at trial, data breach and privacy issues, and information security, among other areas.

Mr. Southwell earned his Bachelor's degree *magna cum laude* from Princeton University and his Juris Doctor *magna cum laude* from New York University School of Law. Following law school, Mr. Southwell was a law clerk for the Honorable Naomi Reice Buchwald of the United States District Court for the Southern District of New York.

Mr. Southwell is also a member of the firm's Electronic Discovery and Information Law, Intellectual Property, White-Collar Defense and Investigations, Crisis Management, and Appellate and Constitutional Law Practice Groups. Mr. Southwell also serves on Gibson Dunn's firm-wide Diversity Committee and is active with the Federal Bar Council and the Association of the Bar of the City of New York, serving on the Association's Professional Responsibility Committee and previously serving on the Committee on Information Technology Law and the Government Ethics Committee. In addition, Mr. Southwell serves on the Board of Advisors of the Center on Law and Information Policy at Fordham Law School, one of the nation's leading academic centers contributing to the development of the law and policy in the area of information technology, and is a member of the New York Chapter of InfraGard, a partnership between the FBI and the private sector dedicated to

sharing information and intelligence to prevent hostile acts against the United States' cyber and physical infrastructure.

Mr. Southwell is a nationally recognized expert on data and information security, digital privacy, and related areas. He regularly publishes articles and is asked to speak on the areas of his expertise. He is also regularly sought out for comment by national and international media on these areas.

#### Recent articles, lectures, and presentations include:

- Presenter, "Practitioner's Guide to Social Media," Corporate Executive Board General Counsel Roundtable and Compliance and Ethics Leadership Council webcast, December 2010.
- Speaker, "Annual Review of Key Legal Developments: Trademarks, Copyright, and Trade Secrets," ABA's Fourth Annual National Institute on Criminal Enforcement of Intellectual Property Rights, November 2010.
- Panelist, "The Evolution of Cybercrime and How to Combat It," The Coalition Against Domain Name Abuse's Online Brand Abuse and Internet Governance Forum, October 2010.
- Presenter, "Cyber Crimes: Phishing, Pharming and Beyond," Lorman Educational Services webcast, September 2010.
- Presenter, "Recent Developments in Privacy and Data Security," Education Finance Council/National Council of Higher Education Loan Programs 2010 Student Loan Finance and Legal Meeting, August 2010.
- Speaker, "Legal Responses to Current Cyber Security Threats," International Conference on Cyber Security hosted by the FBI and Fordham University, August 2010.
- Speaker, "Healthcare Privacy and Information Security," Association for Healthcare Risk Management of New York Annual Conference, June 2010.
- Panelist, "Incident Response," Cyber and Intellectual Property Crime Symposium, hosted by the U.S. Attorney's Office for the District of New Jersey and Rutgers School of Law-Newark, June 2010.
- Guest Lecturer, "Advanced Persistent Threats and the Criminal Enforcement of Cyber Security," for Cyber Security and Applications seminar at Fordham University Graduate School of Arts and Sciences, May 2010.
- Panelist, "Hot Topics in Cybercrime: Investigating and Responding To Source Code Thefts and Anonymous Attacks," ABA's 24th Annual National Institute on White Collar

Crime, February 2010.

- Speaker, “Litigation Issues Under the Economic Espionage Act,” ABA’s Third Annual National Institute on Criminal Enforcement of Intellectual Property Rights, October 2009.
- Panelist, “Cyberspace–The Black Hole Where Ethics, Strategy, and Technology Collide,” NACDL & Fordham Law School’s 2009 White Collar Seminar on Defending the White Collar Case, October 2009.
- Speaker, “Privacy in Litigation,” PLI’s Tenth Annual Institute on Privacy and Data Security, June 2009.
- Author, “A Sword of a Shield? The New Administration’s Approach to Cybercrime and Cybercrime Fighting,” *The Champion*, May 2009.
- Speaker, “Data Security 101: An Ounce of Prevention is Worth a Pound of Cure,” LegalTech New York, February 2009.
- Panelist, “Legal and Technical Policy Issues in Cyber Security,” International Conference on Cyber Security hosted by the FBI and Fordham University’s Department of Computer and Information Services, January 2009.
- “Data Security Breaches: Preparing for and Addressing the Enterprise-Threatening Risks” presentation to client, September 2008.
- Author, “Data Breaches: Expect A Rise in Litigation,” *New York Law Journal: Investigations & Computer Forensics*, May 2008.
- “Update on Federal and State Data Privacy Laws” presentation to Gibson, Dunn & Crutcher LLP Intellectual Property Institute, December 2007.
- “Trends in Cyber-crime and Information Security Enforcement” presentation to John Jay College of Criminal Justice Center for Cybercrime Studies, December 2007.
- Speaker at New York University Journal of Legislation and Public Policy Symposium, “Leviathan’s Network: Municipal Wireless and Civil Liberties,” November 2007.
- Speaker, “Trends in Cyber-crime and Information Security Enforcement,” John Jay College of Criminal Justice Center for Cyber-crime Studies, Fall 2007.
- “Internal Investigations: The Role of In-House Counsel” presentation to client, July 2007.
- Speaker, “Increasing Regulatory Scrutiny In The Digital Age,” Fordham Law School Summer Program in U.S. Law, July 2007.

- Panelist, “Protecting Borders in the Information Age – Balancing Data, Privacy, and National Security in North America,” Fordham Law School Center on Law and Information Policy/The Americas Society/North American Consortium on Legal Education Workshop, April 2007.
- Speaker, International Data Protection and Binding Corporate Rules Invitational Workshop, Fordham Law School Center on Law and Information Policy, November 2006.
- “Cyber-crimes” presentation to Criminal Prosecution clinic, New York University School of Law, March 2005.
- “Cyber-crimes” presentation to Federal Criminal Law seminar, New York University School of Law, November 2004.
- “Anatomy of an F-Server Case: Investigation and Prosecution Case Study, United States v. Pabon-Cruz” presentation to Investigation and Prosecution of Advanced Child Exploitation Cases Seminar, U.S. Department of Justice, National Advocacy Center, March 2004.
- Presentation to Operation Candyman Prosecution Seminar, U.S. Department of Justice, December 2002.