



Edward J. McAndrew

Partner

ed.mcandrew@dlapiper.com

Wilmington

T: +1 302 468 5685

F: +1 302 397 2470

Washington, DC

T: +1 202 799 4245

Ed McAndrew is a counselor, investigator and trial lawyer who focuses on cybersecurity, privacy and technology matters.

Ed counsels and represents clients on cyber incident response, crisis management, internal and governmental investigations and technology-related litigation. Ed has handled more than 800 cyber incidents and has tried more than 37 cases to verdict over a career split between the private and government sectors. Major substantive areas of his practice include cybersecurity, digital privacy, social media, commercial, employment, intellectual property, corporate governance, regulatory, white collar, and other criminal matters. He also advises on cyber-based national security issues, as well as governmental demands for data and assistance in investigations.

Ed served for nearly a decade as a federal cybercrime prosecutor in the US Department of Justice, in Washington, DC and in the US Attorney's Offices for the Eastern District of Virginia and for the District of Delaware. As a Cybercrime Coordinator and National Security Cyber Specialist, Ed handled a multitude of high-profile, complex and sensitive investigations, trials and appeals – many involving cutting edge legal and technological issues. He has extensive experience in investigations and litigation involving hacking, data theft, ransomware and other cyberattacks; digital espionage; cyberstalking; threats and extortion; identity and intellectual property theft; terrorism and domestic extremism; financial, government contracting, and tax fraud; money laundering; export control violations; obstruction of justice; online child exploitation; and human, narcotics, and firearms trafficking. In 2015, *The National Law Journal* named Ed an inaugural "Cybersecurity and Data Privacy Trailblazer" for his work in the US Department of Justice.

Prior to his government service, Ed was a partner and the deputy leader of the litigation department at an international law firm. He began his legal career as a law clerk to Judge Collins J. Seitz, of the US Court of Appeals for the Third Circuit.

Ed serves by appointment as co-chair of the Delaware Supreme Court's Commission on Law and Technology and as co-chair of the Media Law Resource Center's Data Privacy Committee. He is an avid commentator, presenter and author on legal issues related to cybersecurity, digital privacy, cybercrime, computer forensics and Internet safety.

- Intellectual Property and Technology
- Cybersecurity
- Data Protection, Privacy and Security
- Litigation, Arbitration and Investigations
- White Collar and Corporate Crime

PRIVATE SECTOR EXPERIENCE

Crisis Management, Investigations & Litigation

- Counseling and representation of energy sector company in response to network intrusion and \$35 million business email compromise, including successful recovery of all funds and federal grand jury investigation into incident
- Counseled and represented global technology company in investigations relating to high profile, supply chain incident impacting numerous public and private sector entities
- Representation of parties in federal grand jury investigation into allegations of political corruption, financial and tax fraud by individuals related to the U.S. presidential administration
- Counseling and representation of SaaS provider in responding to advanced persistent cyberattacks impacting financial information for millions of U.S. citizens and related regulatory investigations, class action and commercial litigation
- Counseling and representation of global financial services company in coordinated ransomware/data theft "double extortion" attacks, resulting investigations and commercial dispute resolution
- Counseling and representation of U.S. hospital in response to operationally disruptive ransomware attack and subsequent civil litigation alleging related patient death
- Counseling and representation of global entertainment production company in ransomware/data theft "double extortion" attack impacting operations and data in numerous countries
- Counseled and represented IT managed service provider in response to ransomware attack on US city and successful settlement of related civil disputes
- Defense of global consumer electronics retailer in data breach class action resulting from a payment card breach involving over 2 million customers
- Counseling and representation of media, entertainment and sports organizations and individuals victimized by technology facilitated defamation, extortion, cyberstalking, online threats and fraud
- Counseling and representation of organizations in various sectors in responding to governmental demands for third party data and assistance under FISA, ECPA and the CLOUD Act
- Counseled and represented multinational security company in first-of-its-kind ransomware/data theft "double extortion" attack
- Representation of a global life sciences company as the victim in a federal criminal investigation and prosecution relating to the theft of over \$1 billion in intellectual property by internal and external cyber actors located in multiple countries
- Conducted internal investigation of whistleblower claims regarding privacy law compliance issues for global consulting organization
- Pro Bono representation of national domestic violence and crime victims' rights organizations as amicus in defending the federal cyberstalking statute against First Amendment challenges
- Defense of national retailer in data breach class action resulting from payment card breach involving over 500,000 customers
- Counseling and representation of global life sciences company as the victim in a federal digital advertising fraud prosecution of international cybercriminals
- Counseling and representation of SaaS provider in "double extortion" attack impacting medical billing operations for nationwide customer base
- Counseling of global data and waste disposal company in cyberattack involving data breaches and payment re-direction schemes involving hundreds of Office365 accounts, and representation in regulatory investigations in multiple jurisdictions
- Defense of fraud and breach of fiduciary duty litigation against an international digital entertainment streaming service in the Delaware Court of Chancery
- Defense of an online retailer in computer fraud and intellectual property theft litigation
- Defense of an online marketing organization in data breach litigation
- Representation of a manufacturing company in civil litigation and criminal litigation relating to hacking and cybertheft of intellectual property by a competitor
- Counseling of consumer goods logistics company in ransomware attack that disrupted global operations during holiday season
- Defense of a large hotel and casino in a data breach class action brought by employees alleging the compromise of their personal information and related financial fraud
- Counseling and representation of insurance services company in cyber incident and financial fraud investigation relating to high profile natural gas disaster in the Northeastern United States

- Representation of a federal defense contractor as the victim in criminal and national security investigations relating to nation-state cyberattacks targeting export-controlled intellectual property
- Investigation and response to nation-state advanced persistent cyberattacks on a global business technology and Internet infrastructure company
- Counseling of global consulting firm in intrusion into networks in multiple countries
- Counseling of global insurance company in response to cyber incident involving personal information of thousands of policyholders
- Defense of major U.S. university resulting in pre-complaint settlement of all claims relating to alleged cyberattack on virtual currency managed services provider
- Service as national coordinating counsel for large financial institution relating to privacy and cybersecurity issues in all U.S. civil litigation
- Counseling and representation of multinational pharmaceutical company in response to phishing attack targeting the Office 365 accounts of more than 1,000 employees
- Counseling and representation of medical device company in business email compromise attacks resulting in the re-direction of millions of dollars in vendor payments
- Representation of a national employee benefits organization in the investigation of and response to a web-based payroll re-direction attack
- Representation of a financial services company in a data breach impacting consumers in all states and resulting in multiple state attorneys general investigations
- Representation of a large financial institution in a data breach impacting customers in 30 states
- Representation of online retailers in a malware attacks impacting consumers in every state
- Investigation and response to a ransomware attack on a legal services organization
- Successful defense of nationally prominent membership organization in defamation, invasion of privacy and civil rights action filed by an expelled member following national media coverage of his involvement in domestic extremist and white supremacist groups
- Successfully represented publicly traded media company in arbitrations involving more than \$500 million in broadcasting, intellectual property, advertising, and corporate ownership rights relating to digital media technology
- Successfully represented mortgage purchaser in litigation related to \$43 million mortgage fraud scheme
- Successfully represented the Delaware Insurance Commissioner as receiver in \$20 million fraud, breach of contract, and tax cases against the DC government involving a real estate development project
- Secured one of the first decisions in the United States dismissing privacy and defamation claims against a website for publishing third-party content under Section 230 of the Communications Decency Act
- Successfully represented national supermarket chain in civil litigation relating to invasion of privacy, consumer fraud and newsgathering torts by major television broadcasting network
- Conducted internal investigations on behalf of boards of directors of various organizations relating to allegations of financial fraud and political corruption
- Conducted internal investigation and represented global insurance company in grand jury and SEC investigations of FCPA violations
- Conducted internal investigation and represented transportation technology company in governmental investigations of export control violations
- Represented target of grand jury investigation relating to large-scale environmental spill
- Represented private entities in election fraud litigation relating to ballot referendum on casino gambling
- Represented online advertising business in cybersquatting and trademark infringement actions
- Successfully litigated breach of contract case for advertising agency relating to information technology support contract
- Represented quasi-governmental real estate development agency in breach of lease litigation involving marinas located on Washington, D.C.'s Southwest Waterfront, near Nationals Park
- Litigated through Supreme Court appeal a successful First Amendment challenge to federal commercial casino advertising ban
- Defended global technology company in theft of trade secrets case involving recruitment of a competitor's Internet technology development team and alleging over \$1 billion in damages
- Successfully defended District of Columbia Government in \$75 million negligence case alleging catastrophic brain injury to prominent

plaintiff due to public safety issues

General Technology Law Counseling

- Advise media companies on potential civil and criminal liability related to technology-facilitated newsgathering by journalists
- Advise various cybersecurity companies on legal issues relating to proactive monitoring, threat hunting, intelligence gathering, incident response, forensic investigation, data analysis, law enforcement interaction and service as expert witnesses in litigation
- Advised European government on proposed legislation relating to the monitoring and reporting of Internet crimes against children by electronic communication services
- Advised social media app on content moderation policies and procedures relating to digital threats, domestic extremism and Internet crimes against children
- Advised European government agency on U.S. CLOUD Act and Wiretap Act issues
- Pro Bono counseling of human rights organization on the collection, preservation, authentication, and admission of mobile device evidence in U.S. criminal and civil trials and evidentiary proceedings relating to violent crimes
- Advised global financial services, logistics, automotive and other companies on U.S. law enforcement and global privacy issues related to the Wiretap Act, Stored Communications Act and CLOUD Act
- Counseling and training of multiple organizations, directors, officers and employees relating to technology facilitated defamation, extortion, cyberstalking, online threats, domestic extremism and other criminal activity
- Advised global eDiscovery SaaS provider on cybersecurity risk management, incident response and litigation planning
- Advised numerous organizations on the creation, implementation and enhancement of privacy and cybersecurity programs in the technology, financial services, insurance, government contracts, media, entertainment, sports, manufacturing, consumer goods, logistics, gaming, healthcare, life sciences, education, transportation, energy, and construction industries
- Advised organizations on the cybersecurity aspects of due diligence, contract drafting and negotiation of transactions of various sizes in the technology, financial services, insurance, media, entertainment, manufacturing, consumer goods life sciences and education industries
- Conducted cyber incident exercises for boards, senior executive teams and incident response teams for organizations in various sectors
- Advised various public companies on cybersecurity governance and securities law disclosures relating to cyber risk and cyber incidents

PROSECUTORIAL EXPERIENCE

- First US prosecution of a foreign hackers for theft of trade secrets from American companies. Coordinated 3-year multinational investigations and successful prosecutions of members of international hacking and data theft conspiracy that breached the networks of a leading global technology company, various software supply chain companies, and the US Army, stealing thousands of identities and intellectual property valued in the billions of dollars
- First US convictions for cyberstalking resulting in death. Convicted three members of a multi-year cyberstalking conspiracy resulting in an active shooting of multiple victims and the murders of two women in the lobby of Delaware's largest courthouse
- Convicted a member of an international cybercrime organization of cybertheft, cracking, and online distribution of more than \$100 million in sensitive industrial-grade software owned by more than 200 technology companies to buyers in 28 states and more than 60 countries. One of the longest prison sentences in US history for cybertheft of intellectual property
- Led international online undercover investigations that infiltrated dark web networks, resulting in the identification and prosecution of thousands of suspects engaged in child pornography and child sex trafficking crimes, and the rescue of hundreds of child sexual abuse victims
- Convicted chief scientist of a defense and law enforcement contractor of cybercrime conspiracy involving use of cracked software obtained from international cybercriminals to design components used in Marine One presidential helicopters, Blackhawk helicopters, Patriot missiles, police radar and breath analysis equipment
- Investigated data breaches of an IT enterprise solutions and cloud services provider resulting in the compromise of systems and sensitive data of more than 50 entities and hundreds of millions of individuals
- Convicted a NASA scientist of cybercrime conspiracy involving uploading of cracked software obtained from international cybercriminals onto NASA computer network

- Convicted a website operator of cybertheft and online distribution of more than 24,000 copies of software products manufactured by at least 80 companies to thousands of customers
- Investigated money laundering and Bank Secrecy Act violations involving the use of stolen intellectual property to unlawfully mine, commoditize and sell virtual currencies on black markets
- Investigated and prosecuted numerous individuals for online child exploitation crimes, including:
 - United States Secret Service officer stationed at the White House
 - Teachers, university professors and other school/university employees
 - Youth group leaders, camp counsellors and football, basketball, baseball and soccer coaches
 - Priests, ministers and other church employees
 - Healthcare providers and lawyers in government and private practice
 - Employees, including senior executives, of various types of companies
 - Local, state and federal law enforcement officers and senior managers
 - Active duty military personnel deployed in Operation Enduring Freedom and Operation Iraqi Freedom
 - Senior military and intelligence personnel and contractors stationed at the Pentagon, CIA, Dover Air Force Base and abroad
- Prosecuted a hacker for digital threats and cyberstalking of a federal prosecutor
- Investigated cybercrime ring engaged in the hacking of social media accounts of federal judges
- Conducted international investigation into a series of DDoS attacks against major financial institutions
- Investigated data breaches and theft of hundreds of thousands of identities from multiple financial, educational and governmental computer networks by foreign-based hackers
- Convicted members of a large-scale, Internet-based tax fraud conspiracy centered on electronic submission of more than 450 tax returns using more than 60 different Internet service accounts and 130 financial accounts. Total losses to the United States of US\$8 million in one year
- Convicted a leader of an identity theft and bank fraud conspiracy involving computer-facilitated check fraud using more than 200 stolen identities
- Investigated an entity and individuals for International Traffic in Arms regulatory violations involving Internet-based exports of technology relating to a US Navy contract
- Convicted an individual in a witness intimidation and obstruction of justice case involving use of a mobile device and Facebook to threaten a government witness in a murder-for-hire and drug trafficking trial. Arrest made in courtroom during trial
- Successfully litigated media right-of-access issues relating to courtroom testimony and evidence presentation in cybercrime trials
- Prosecuted cyberstalking and Internet threat campaign involving e-mail account hijacking and online defamation and dissemination of private, explicit videos
- Convicted a disgruntled employee of a domestic terrorism offense for mailing fake anthrax to the headquarters of a prominent media organization
- Investigated hacking into financial institution servers and theft of millions of dollars in customer funds
- Investigated hacking and hijacking of a retail business website by a former third-party vendor
- Investigated unauthorized access to a food supplier's computer network from a shipping port
- Investigated anonymous online threats to federal and state public officials and employees

CREDENTIALS

Admissions

- Delaware
- District of Columbia
- New Jersey
- Pennsylvania

Clerk Experience

- The Honorable Collins J. Seitz, US Court of Appeals for the Third Circuit, 1996-1997

Recognitions

- Director's Award, US Department of Justice, 2019
- *The Legal 500 United States*
 - 2020-21 - Recommended, Cyber Law (including Data Privacy and Data Protection)
 - 2020 - Recommended, Data Privacy and Data Protection
 - 2017 - Recommended, Financial Services Regulation
- Cybersecurity and Data Privacy Trailblazer, *The National Law Journal*, 2015
- Director's Special Recognition Award, Federal Bureau of Investigation, December 2015
- Exemplary Partnership Award, US Department of Homeland Security, US Immigration and Customs Enforcement, Homeland Security Investigations, February 2015
- Director's Award, US Department of Homeland Security, US Immigration and Customs Enforcement, November 2013
- Assistant Attorney General's Award for Outstanding Advocacy in Protecting Citizens from Online Crime, US Department of Justice, November 2008

For more information, pursuant to New Jersey Lawyer Advertising guidance, please click here.

Education

- J.D., Catholic University of America 1995
 - magna cum laude*
 - Editor-in-Chief, *Catholic University Law Review*
- B.A., The College of New Jersey 1992

Memberships

- Supreme Court of Delaware, Commission on Law & Technology – Co-Chair
- Media Law Resource Center, Data Privacy Committee – Co-Chair
- American Bar Association, Litigation, Criminal Justice and Business Law Sections, Communications Law Forum
- International Association of Privacy Professionals
- Law360 Cybersecurity & Privacy Editorial Advisory Board

INSIGHTS

Publications

US Senate unanimously passes the Strengthening American Cybersecurity Act

14 March 2022

Prior versions of this and related legislation failed to win passage in recent years.

Google files groundbreaking civil suit to disrupt massive botnet with blockchain backup system

10 December 2021

Civil actions to take down botnets have been around for years, but the blockchain aspect adds a new twist.

Supreme Court significantly limits the scope of the Computer Fraud and Abuse Act

4 June 2021

The decision will largely gut the CFAA as a tool for addressing insider data theft.

Supreme Court dives into circuit split over the Computer Fraud and Abuse Act

28 January 2021

What does it mean to "exceed authorized access" to an Internet-connected device?

- "Coronavirus: Cybersecurity considerations for your newly remote workforce (United States)," March 31, 2020
- "Are you ready for CCPA class action litigation?," March 30, 2020
- "Coronavirus: Cyber hygiene practices," March 25, 2020
- "Cybercrime: Beware the Business Email Compromise," October 2019
- "Surviving the Service Provider Data Breach," *The Legal Intelligencer*, July 18, 2019
- "ABA's Data Breach Disclosure Opinion: A Must-Read for All Lawyers," *The Journal of the Delaware State Bar Association*, March 2019
- "You've Been Breached! Now What?" *SCMagazine*, September 18, 2018
- "Welcome Back to America! Now Gimme Your Phone," *ABA Journal of the Section of Litigation*, Spring 2018
- "Malware Everywhere – What's a Reasonable Lawyer to Do?" *Delaware Lawyer*, November 2017
- "Author, '10 Critical Steps to Create a Culture of Cybersecurity,'" *Dark Reading*, July 26, 2017
- "Companies Must Prepare for Future Filled with Ransomware Attacks," *The Hill*, May 20, 2017

Events

- "The Ransomware Threat Is Changing – Sectoral Implications," DLA Piper Webinar, June 17, 2020
- "Cybersecurity for a 2020 Workforce," DLA Piper Webinar, May 28, 2020
- "Cyber Considerations in the Time of COVID-19," Media Law Resource Center Webinar, April 29, 2020
- "Cybersecurity: What Should Keep You Up at Night," ESRA Privacy Symposium, March 10, 2020
- "Mobile Data: Issues in Data Privacy and Data Protection," Legalweek, New York, February 5, 2020
- "Cybersecurity for Your Legal Practice," Delaware State Bar Association CLE, January 23, 2020
- "Cybersecurity: New War, New Rules – Tales from the Trenches," IAPP, Luxembourg, January 16, 2020
- "Are You Ready for CCPA Data Breach Litigation?" DLA Piper Webinar, January 9, 2020
- "Cybersecurity for Delaware Lawyers: Delaware Supreme Court Pre-Admission Conference," Wilmington, November 21, 2019
- "Protecting Yourself and Others in a Digital World," Kennett Middle School, October 1, 2019
- "Government Data Demands: What You, Your Clients, and Your Companies Should Know," Relativity Fest, Chicago, October 22, 2019

- "Recent Developments in Data Security and E-Discovery 2019," Delaware State Bar Association CLE, October 8, 2020
- "Cybersecurity and Privacy Regulatory Framework: Best Practices for Compliance," Association of Insurance Compliance Professional Annual Meeting, Denver, September 25, 2019
- "It's a Hostile Takeover: New Threats in Cybersecurity and How to Address Them," Association of Insurance Compliance Professional Annual Meeting, Denver, September 24, 2019
- "Friday the 13th: Cybersecurity & Technology for Lawyers," Delaware Supreme Court Commission on Law & Technology/Office of Disciplinary Counsel, September 13, 2019
- "Healthcare Compliance Symposium 2019," First Healthcare Compliance, April 2019
- "Recent Developments in Data Security and E-Discovery," Delaware State Bar Association CLE, November 2018
- "The Weaponization of the Internet," Temple University Law School, Philadelphia, October 2018
- "Mission Critical Cybersecurity: Navigating Data Privacy and Cybersecurity Threats from an In-House Perspective," ACC Annual Meeting, Austin, October 2018
- "From Carpenter to the GDPR: 2018 Data Privacy and Protection Law Update," Relativity Fest, Chicago, October 2018
- "The Internet of Things from a Legal and Regulatory Perspective," Relativity Fest, Chicago, October 2018
- "Outside Our Borders: How New Laws Will Affect Businesses," Colorado Cybersecurity Summit, Denver, September 2018
- "Technology facilitated Harassment and Stalking," Delaware Judges Conference, Wilmington, September 2018
- "Current Issues in Cybercrime and Cybersecurity," Delaware Law School, Wilmington, August 2018
- Panelist, "Key Takeaways from the 2018 ACC State of Cybersecurity Report: An In-House Perspective," ACC Mountain West Lunch and Learn, Salt Lake City, August 2018
- "Working with Law Enforcement," American Bar Association's Third National Institute on Cybersecurity Law, New York, June 2018
- "Requirements and Best Practices for Staying Ahead of and Responding to Cyber Threats," 13th Annual ABA/FCBA Privacy and Data Security Symposium, Washington, DC, March 2018
- "Shining a Light on Technology-Facilitated Exploitation," Archdiocese of New Orleans Human Trafficking Summit, March 2018
- "Cybercrime & Cybersecurity Law in 2018," Washington and Lee University School of Law, February 2018
- "From the Iron Rooster to Amazon Alexa: Mobile Discovery and the Internet of Things," LegalTech New York 2018, January 2018
- "Navigating a Breach & Activating a Proven Incident Response Plan," OpenText webinar, January 2018
- "The Two Sides of Cybersecurity: Proactive Planning & Incident Response," Delaware State Bar Association, Wilmington, January 2018
- Roundtable Discussion of Law Enforcement Interaction with Organizational Victims of Cybercrime, FBI/U.S. Department of Justice Regional Pharmaceutical Conference, Collegeville, Pennsylvania, November 2017
- "Incident Response on the Down Low," IAPP 3rd Annual Florida Privacy & Cybersecurity Law Symposium, Jacksonville, November 2017
- US Department of Justice National Security Specialists Conference, Washington, DC, October 2017
- "Internet of Things: Law, Technology & Practice," Relativity Fest, Chicago, October 2017
- "Game Planning for Cyber Incidents: Practicing and Executing Effective Cyber Incident Response," Delaware Trust Conference, Wilmington, October 2017
- "Hack Yeah! Cybersecurity @ the Ball Park!," Hispanic Bar Association of Pennsylvania, Philadelphia, June 2017
- "Privacy & Data Security: A Simulated Breach & Response Plan," Enfuse Conference, Las Vegas, May 2017
- "From the Lab to the Courtroom: Harnessing Digital Evidence to Win Cases," Keynote Address, Access Data User Summit, San Diego, May 2017
- "Learning Lab: Investigating and Prosecuting Cybercrime – Enter the Law Enforcement Trenches," RSA Conference, San Francisco, February 2017
- "Hot Topics on the Internet and Data Privacy," ABA Forum on Communications Law, New Orleans, February 2017
- "E-Discovery for Investigations and Criminal Matters," Legaltech New York, New York City, February 2017
- "An Exercise in Cyber Incident Response," ACC Cybersecurity Summit, Washington, DC, January 2017

NEWS

DLA Piper partners and firm COO named to *Law360* 2021 Editorial Advisory Boards

10 May 2021

DLA Piper is pleased to announce that 11 of its lawyers, as well as firm COO Bob Bratt, have been named to *Law360*'s 2021 Editorial Advisory Boards.

MEDIA MENTIONS

- Quoted, "Legal Research May Be Headed Back to the Future of Privacy," *LegalTech News*, December 19, 2019
- Quoted, "Money Laundering on Video Games: Play On or Game Over?" *Law.com*, November 7, 2019
- Quoted, "Location Privacy Warrant Lines Still Murky After Carpenter," *Law360*, August 19, 2019
- Quoted, "The 6 Biggest Cybersecurity Episodes So Far In 2019," *Law360*, July 11, 2019
- Quoted, "A CCPA Class Action Is Coming and Preparedness Is The Best Way to Avoid It," *Corporate Counsel*, June 21, 2019
- Quoted, "Report: Executives Likely to Be Targeted for Cybercrime," *Corporate Counsel*, May 13, 2019
- Quoted, "Legal Departments Must Keep Rising Email Scams on Their Radars," *Corporate Counsel*, April 26, 2019
- Quoted, "Utah Warrant Bill Raises Stakes For Cops' Digital Data Grabs," *Law360*, April 23, 2019
- Quoted, "Mueller Rips 'Disappearing Data' Prized by Corporations," *Bloomberg Law*, April 23, 2019
- Quoted, "Report: data breaches will be the next trend in class action litigation," *Corporate Counsel*, April 16, 2019