

## Demian Ahn

PARTNER

Data, Privacy, and  
Cybersecurity  
Washington, D.C.

dahn@wsgr.com  
202-255-0937

### FOCUS AREAS

Artificial Intelligence and  
Machine Learning  
Data, Privacy, and  
Cybersecurity  
Government Investigations  
Internet Strategy and  
Litigation  
National Security and Trade  
Strategic Risk and Crisis  
Management

### HIGHLIGHTS

#### Cybersecurity Expertise When It's Needed Most

Demian represents companies confronting data, privacy, and cybersecurity issues, leading the response to cybersecurity incidents, providing practical risk management guidance, strategically engaging with a broad range of regulators and regulatory frameworks, and conducting sensitive investigations that intersect with our public company, litigation, health, and national security practices.

#### Practical Guidance for Start-Ups and Multinationals

Demian advises companies that develop, deploy, and operate emerging technologies, providing practical guidance about rapidly changing regulations involving privacy, cybersecurity, online safety, and artificial intelligence (AI). He has extensive experience helping emerging companies develop and implement data privacy and security programs, helping large and complex organizations adapt to significant regulatory shifts, and advising both private and public companies as they build internal governance structures, engage in partnerships with third parties, and engage in or evaluate strategic corporate transactions.

#### Deep Experience Investigating and Defending Sensitive Matters

Demian has 20 years of experience—both inside and outside of government—conducting and defending high-stakes investigations and litigating cases before both trial and appellate courts. He served as a federal prosecutor in the U.S. Attorney's Office for the District of Columbia, ending his federal career as Acting Deputy Chief of the Fraud Section (2021-2022), where he conducted and supervised innovative and high-impact investigations involving nation-state cyber threat actors, organized identity theft and cybercrime rings, cyber-enabled fraud and harassment, investment fraud, health care fraud, and corporate and consumer fraud.

#### A Recognized Practitioner

Demian regularly speaks about and presents on emerging cybersecurity risks and regulations and is a regular contributor to the WSGR Data Advisor. He has been named as one of the "Incident Response 50" by *Cybersecurity Docket* and as one of *Lawdragon's* 500 Leading Global Cyber Lawyers, and he received numerous awards for outstanding service as a prosecutor, including from the Federal Bureau of Investigation (2018 and 2021) and the U.S. Department of State (2022) for "elite" national security cyber expertise and "exceptional prosecutorial support and relentless efforts in combatting cyber threats" against the United States.

### EXPERIENCE

Demian Ahn is a member of the firm's data, privacy, and cybersecurity practice based in Washington, D.C. He leads the firm's incident response practice and advises companies confronting data, privacy, and cybersecurity risks—risks from threat actors, regulatory risks from federal and state agencies,

and other legal risks related to cybersecurity and technology-driven products and services, including software-as-a-service, AI and machine learning, cloud computing, digital health, fintech, e-commerce, online platforms, social media, and cybersecurity services.

**Incident Response.** Demian advises technology companies in connection with cyber, privacy, technological, and insider threat incidents. He leads incident response and crisis management teams, manages internal investigations, and advises companies on external communications and disclosures. During his federal career, Demian led investigations and supported incident response relating to data breaches at U.S. government agencies. At Wilson Sonsini, Demian leads an incident response team with experience advising clients on hundreds of incidents relating to health, fintech, financial services, e-commerce, social media, cloud computing, defense, and cybersecurity companies.

**Investigations and Defense.** Demian regularly represents clients in connection with cybersecurity and privacy-related investigations by federal and state regulators, including the Department of Health and Human Services, Federal Trade Commission, Securities and Exchange Commission, Department of Justice, Department of Defense, and state attorneys general, as well as state financial regulators such as the New York Department of Financial Services. Demian also has extensive experience conducting, supporting, and leading sensitive internal investigations on a broad range of matters, including insider threat investigations, whistleblower claims, misappropriation of intellectual property, employee misconduct, alleged securities and financial fraud, health care fraud, and matters pertaining to the False Claims Act.

**Information Governance and Compliance.** Demian advises clients on legal and regulatory compliance related to technology-driven products and services. He helps emerging companies build and implement information security programs, and he helps companies of all sizes navigate complex privacy and cybersecurity regulations and requirements, including under HIPAA, GLBA, CMMC, FedRAMP, CJIS, the Department of Justice's Data Security Program, and various state laws and regulations. Demian also advises companies on cybersecurity compliance as they explore initial public offerings and M&A transactions, and in connection with SEC reporting and corporate governance matters.

**Counseling Cybersecurity Providers.** As a Computer Hacking and Intellectual Property Prosecutor and National Security-Cyber Specialist, Demian gained extensive experience working with threat intelligence and cybersecurity experts across the federal government and private industry. He conducted corporate investigations involving cybersecurity services and cybersecurity-related export control violations, including a precedent-setting investigation into former U.S. intelligence officials who provided services to a foreign government. Now, in private practice, Demian advises cybersecurity companies on legal and regulatory compliance, including with respect to the Computer Fraud and Abuse Act, the Wiretap Act, U.S. sanctions and money laundering laws, and security research on the dark web.

**Trust and Safety.** Demian advises clients that are developing or deploying technology platforms, including AI-driven platforms, on content moderation and Trust and Safety matters, including with respect to the REPORT Act, the Take it Down Act, and related laws in the United States and elsewhere.

**Law Enforcement Requests.** Demian has extensive experience and a deep understanding of the Electronic Communications Privacy Act (ECPA), the CLOUD Act, and other U.S. laws relating to legal process, surveillance authorities, and voluntary requests for information from U.S. state and federal government entities. He regularly advises clients subpoenas, court orders, search warrants, and government requests for information, as well as proactive engagement with law enforcement.

Prior to joining the Department of Justice, Demian worked at a prominent multinational law firm, where he represented clients in high-stakes litigation and investigations, including matters before Congress, federal and state regulatory bodies, and federal and state trial and appellate courts.

Immediately following law school, Demian clerked for the Honorable Frederick J. Martone of the U.S. District Court for the District of Arizona. During law school, he also served as a law clerk for the South African Human Rights Commission in Durban, South Africa.

## CREDENTIALS

---

### Education

- J.D., University of Michigan Law School
- B.A., Cornell University

## Honors

- Named to the 2025 "Incident Response 50" list by *Cybersecurity Docket*
- Selected for inclusion in the 2025 edition of the Lawdragon's "500 Leading Global Cyber Lawyers" guide

## Admissions

- Bar of the District of Columbia

## INSIGHTS

---

### Select Publications

- Co-author, "The Busy Lawyer's Guide to the New "Data Export Control" Rules," Wilson Sonsini Alert, February 4, 2025
- Co-author, "Ransomware Attacks: UK Government Proposes Ransom Payment Ban and Mandatory Notification Requirements," Wilson Sonsini Alert, January 24, 2025
- Co-author, "Not Just for DoD Anymore: New Proposed CUI Rule to Apply to All Federal Contractors," Wilson Sonsini Alert, January 23, 2025
- Co-author, "HHS-OCR Announces Proposed Modifications to the HIPAA Security Rule," Wilson Sonsini Alert, January 14, 2025
- Co-author, "New Year, New Developments: 2025 U.S. Privacy, Cybersecurity, and Consumer Protection Predictions," Wilson Sonsini Alert, January 7, 2025
- Co-author, "Cybersecurity: A Critical Element in Your 2025 Business Forecast," Wilson Sonsini Alert, September 30, 2024
- Co-author, "SEC Expands Security and Breach Notification Requirements for Investment Firms," Wilson Sonsini Alert, May 30, 2024
- Co-author, "New Minor Safety Obligations for Online Services: REPORT Act Expands Child Sexual Exploitation Reporting Requirements," Wilson Sonsini Alert, May 10, 2024
- Co-author, "New Executive Order Restricts Certain Cross-Border Transactions Involving Sensitive Personal Data of U.S. Citizens," Wilson Sonsini Alert, March 6, 2024
- Co-author, "Cybersecurity: What to Watch for in 2024," Wilson Sonsini Alert, January 3, 2024
- Co-author, "FBI, DOJ, and SEC Provide Guidance and Requirements for Requests to Delay Form 8-K Disclosures for Material Cybersecurity Incidents," Wilson Sonsini Alert, December 15, 2023
- Co-author, "FTC Amends Safeguard Rule with Requirement for Non-Banking Financial Institutions to Report Data Security Breaches," Wilson Sonsini Alert, November 6, 2023
- Co-author, "SEC Adopts Cybersecurity Disclosure Rules for Public Companies," Wilson Sonsini Alert, August 1, 2023
- Co-author, "Executive Order 14028 Update: OMB Clarifies Cybersecurity Guidance for Federal Contractors; Delays Secure Software Attestation Requirement," Wilson Sonsini Alert, June 30, 2023
- Co-author, "SEC Adjusts Anticipated Action Date for Publication of Final Rules for Cybersecurity Reporting and Enhanced Standardized Disclosure," Wilson Sonsini Alert, June 29, 2023
- Co-author, "White House Releases National Cybersecurity Strategy: Key Takeaways for the Private Sector," Wilson Sonsini Alert, March 14, 2023
- Co-author, "DoD to Contracting Officers: Demand Compliance and Seek Consequences for Material Breaches of Cybersecurity Requirements by Contractors," Wilson Sonsini Alert, August 08, 2022
- Co-author, "DOJ Acknowledges Limits to the CFAA, but Questions (and Possible Civil Liability) Remain for Security Researchers and Others," Wilson Sonsini Alert, May 25, 2022

### Select Speaking Engagements

- Panelist, "Data Privacy Compliance: Pre-Attack Risk Mitigation and Post-Attack Best Practices," Incident Response Forum Masterclass 2024, April 18, 2024