David A. Simon

Skadden

Partner, Washington, D.C.

Co-Head, Cybersecurity and Data Privacy; Artificial Intelligence; National Security

T: 202.371.7120
david.simon@skadden.com

Education

J.D., Harvard Law School

M.Phil., International Relations, Trinity College, University of Oxford (Rhodes Scholar)

B.A., University of Minnesota (Truman Scholar)

Bar Admissions

District of Columbia

Brussels (B-List)

Government Service

Chief Counsel for Cybersecurity and National Security, U.S. Cyberspace Solarium Commission (2019-21)

Special Counsel, U.S. Department of Defense (2011-15)

David Simon is co-head of Skadden's global Cybersecurity and Data Privacy Practice and a member of the firm's National Security Group. Mr. Simon has deep experience advising *Fortune* 500 companies, private equity sponsors and their portfolio companies on cybersecurity, data privacy and AI matters. Accordingly, he works closely with boards, executive teams, product teams and security teams on relevant legal, regulatory, compliance and policy issues involving cybersecurity, AI, privacy and online safety.

Formerly a Pentagon special counsel and chief cyber counsel to the U.S. Cyberspace Solarium Commission, Mr. Simon played a key role in developing the Department of Defense (DoD) Directive on Autonomy in Weapons Systems and helped write more than 40 enacted cyber and privacy laws. Dual qualified in the U.S. and EU, with experience practicing EU law in Brussels, he frequently utilizes his background in both jurisdictions to provide clients with strategic counsel on AI governance, autonomous systems and cross-border regulatory requirements.

Mr. Simon advises developers and businesses deploying AI on product development, enterprise integration and governance of AI agents and other autonomous systems. His work involves guiding clients on human oversight, agent permissions and allocation of responsibility, as well as AI safety and supply chain risk. He also advises boards and management on AI oversight and the development and implementation of enterprise-wide AI governance programs.

Mr. Simon has advised on some of the most significant cyber incidents on an international scale. His experience includes representing victims of state-sponsored cyber activity, ransomware and other cyber extortion attacks, as well as breaches of health information, sensitive government information, intellectual property and personal data. He often represents global companies in connection with cyber incident preparedness and response investigations requiring analysis of breach reporting obligations under U.S. and EU law, including the EU General Data Protection Regulation (GDPR), NIS2, Digital Operational Resilience Act (DORA) and Cyber Resilience Act, and investigations by European data protection authorities and national cyber authorities. He has counseled companies on major cyber incidents and incident preparedness across virtually every industry, including financial, health care, energy, chemical, defense and aerospace, telecommunications, food, transportation, online retail and hospitality.

Companies and private equity sponsors regularly retain Mr. Simon to lead their cyber incident response strategy. He serves as lead investigator, cyber counsel and incident commander in high-stakes, cross-border incidents involving cyberattacks, data breaches and extortion. He frequently counsels boards, C-level executives and other management on preparedness, cyber vulnerabilities and breaches, and associated legal, regulatory and reputational consequences. He also convenes regular roundtables on cybersecurity, AI and privacy risk management with CISOs, CIOs and CTOs from leading global private equity firms and their portfolio companies.

Mr. Simon also advises global technology companies on regulatory defense and cross-border investigations involving the GDPR, DORA and NIS2, and helps clients manage conflicts between U.S. and European regulatory regimes. His data governance and privacy compliance work has involved ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Electronic Communications Privacy Act (ECPA), the California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA) and EU GDPR.

His online safety and platform regulation practice includes advising multiple very large online platforms (VLOPs) on EU Digital Services Act (DSA) compliance in connection with new features. He also counsels on product cybersecurity under the EU Cyber Resilience Act.

Mr. Simon is widely known for his experience regarding the legal and policy issues at the intersection of cybersecurity, privacy, AI and national security. In addition, he has significant experience with the evolving cybersecurity and privacy legal framework applicable to the internet of things (IoT) and product cybersecurity, operational technology (OT) and industrial control systems (ICS).

He has been recognized by *Chambers Global*, in which a respondent noted he has an "extraordinary command of cyber, privacy and the evolving threat landscape," and *Chambers USA* for his "global, holistic view of the cybersecurity world." He has also been honored by *The National Law Journal* as a Cybersecurity & Data Privacy Trailblazer, *The Legal 500* for his "extensive experience of cyber incidents and investigations" and repeatedly as part of *Cybersecurity Docket*'s Incident Response Elite (including in its 2026 edition), a collection of some of the "best incident response lawyers in the business." In addition, he has been named one of *Lawdragon*'s 500 Leading Global Cyber Lawyers and 100 Leading AI & Legal Tech Advisors.

The breadth of Mr. Simon's practice is reflected in the following sampling of his experience advising clients, including:

Cybersecurity, Espionage, Electronic Surveillance and Privacy

- *Fortune* 500 companies in responding to ransomware and extortion attacks from malicious hackers and cyber criminals involving extensive regulatory, law enforcement and intelligence investigations on multiple continents
- multiple clients with regard to:
  - responding to cyber incidents, requiring analysis of breach reporting obligations under U.S. law, the U.K. and EU GDPR and data protection laws on four continents
  - counter-extortion negotiation with cyber threat actors
  - crafting innovative cyber legal options to deter malicious cyber extortionists and to locate, seize and prevent the dissemination of stolen client data
  - disrupting cyber threat actor infrastructure and intrusion campaigns in collaboration with law enforcement and national cyber authorities
- a network of more than 30 airports and related aviation infrastructure in Asia as lead cyber counsel and breach coach, including with regard to a sophisticated ransomware attack that required counter-extortion negotiations and coordination with domestic, regional and international aviation, data protection, finance and law enforcement authorities
- a leading global network of laboratories and health care facilities on a ransomware attack and associated counter-extortion negotiations, regulatory engagement and notification
- a global pharmaceutical manufacturer in responding to a ransomware attack involving industry disruptions, includiong with regard to guidance on regulatory notification obligations across the U.S. and EU
- multiple clients as lead counsel in responding to nation-state-sponsored cyberattacks, including with regard to global forensic investigations, extensive law enforcement engagement, congressional inquiries, grand jury proceedings and advice to boards of directors and senior management regarding fiduciary duties. Served as lead counsel in attacks involving global and U.S. technology companies, a U.S. defense contractor and an entire consumer-facing sector
- cloud computing, data warehousing and backup companies in responding to complex nation-state cyberattacks attributed to Silk Typhoon and telecommunications companies in connection with nation-state sponsored attacks attributed to Salt Typhoon
- multiple clients in assisting on cybersecurity vulnerability management and disclosure policy and related coordination processes involving cybersecurity researchers, DHS and computer emergency response teams, including US-CERT, ICS-CERT and CERT/CC
- leading tabletop exercises on hypothetical cyber, AI and business continuity incidents involving ransomware, insider threats, nation-state attacks, third-party and supply chain attacks, bomb threats, active shooters and natural disasters

Regulatory Investigations and Defense

- multiple health care companies, tech companies, online retailers and financial institutions on investigations by attorneys general and data protection authorities in the EU, Canada, Latin America and Asia following major data breaches
- public companies in connection with material cyber incident disclosures and related SEC cyber investigations following ransomware attacks and data breaches
- a leading cloud infrastructure provider on multiple state attorneys general inquiries concerning data privacy practices

David A. Simon

Continued

Private Equity Sponsors, Portfolio Companies, Boards, Management Teams and Deal Teams

- multiple clients with regard to:
  - complex cyber incident and supply chain attack preparedness and response
  - portfolio-wide cyber compromise and cyber resilience assessments under privilege
  - tailored cyber, privacy, AI and business continuity legal assessments and global regulatory compliance planning involving the EU GDPR, CCPA/CPRA and PRC PIPL
  - responses to cyber audits conducted during or in the aftermath of cyber incidents

Critical Infrastructure and Operational Technology

- owners and operators of operational technology across industries — including power generation, water, alternative energy, data centers, life-science manufacturing, automotive, aerospace and defense — on disruptive cyberattacks, AI governance and business continuity matters
- global mining companies on insider threat investigations, cyber incidents and data breaches, including leading sensitive internal investigations

AI Governance and Autonomous Systems

- AI developers on the deployment and enterprise integration of AI agents, including with regard to human oversight, agent permissions, allocation of responsibility, AI safety and supply chain risk
- a leading cloud infrastructure provider and its board on its expansion into developing and hosting AI models, including with regard to AI governance, safety and supply chain risk across the U.S. and EU
- a national security technology company on building a responsible AI governance program with its IT and cybersecurity teams, including translating the framework into a formal governance document and an interactive questionnaire for business owners to assess risks and identify when and to whom to escalate them
- a leading pharmaceutical company on developing and implementing an enterprise-wide AI governance program, including an AI use policy tailored to its operations, third-party AI procurement and vetting, vendor risk, contractual protections, data handling and a framework for ongoing risk assessment
- developers of generative AI models for government contractors, government agencies and critical infrastructure operators, including with regard to model design; testing for fairness, bias, accuracy and explainability; and compliance with privacy and data governance frameworks
- leading AI model developers and integrators on safety and legal and policy risks related to chemical, biological, radiological and nuclear weapons
- leading model developers on product liability and legal exposure under U.S. and European law, including with regard to compliance with the EU AI Act and Cyber Resilience Act
- management teams and boards of global financial institutions and technology companies on AI governance, including governance of AI agents and autonomous systems, involving cybersecurity, privacy, fairness and bias, safety and IP considerations; policy and procedure development and tabletop testing; supply chain risk management; and evolving accountability frameworks
- several automobile manufacturers and autonomous vehicle companies on product development and implementation in the U.K., U.S., multiple countries in Europe and Japan, including product counseling and advice on legal, regulatory and legislative developments, and litigation related to emerging cyber threats and autonomous technologies
- leading tabletop exercises on hypothetical AI incidents

Product Cybersecurity

- multiple clients with regard to product cybersecurity requirements under the EU Cyber Resilience Act
- global automakers and suppliers of internet-connected products, such as semiautonomous and fully autonomous cars, implanted medical devices, connected-home products, mobile devices and telecommunications devices with regard to cybersecurity vulnerability management and disclosure programs, bug bounty programs and product cybersecurity risk management and assessments under privilege

Online Safety and Platform Regulation

- multiple VLOPs on DSA compliance in connection with new features

Data Privacy and Compliance

- a multinational medical supplier on assessing the overlapping and distinct obligations under HIPAA, U.S. state privacy laws and consumer health data privacy laws
- an automotive company on conducting a comprehensive overhaul of privacy and AI policies and procedures to account for recent developments in U.S. privacy and AI law
- a global private equity firm on reviewing and streamlining privacy documentation, including coordinating with local counsel across jurisdictions to accommodate local legal nuances
- an electrical testing organization on overhauling its data privacy compliance program to comply with U.S. state privacy laws, including revising privacy notices, developing opt-out mechanisms and drafting template data sales and sharing agreements

David A. Simon

Continued

Board and Executive Advisory

- the board of a multinational regulated energy utility operating across North America on directors' AI oversight responsibilities and board-level risk reporting ahead of expanded AI adoption, addressing the privacy, cybersecurity and critical infrastructure requirements applicable across jurisdictions
- public and private boards across industries, including directors and executive teams, as a trusted adviser on cyber and AI risk management, data privacy compliance and cross-border incident response
- multiple clients with regard to:
  - board-directed post-cyber incident reviews and related matters
  - tabletop exercises and governance trainings to improve crisis management and fulfill fiduciary duties
  - navigating conflicting U.S. and European regulatory regimes in connection with cyber incidents, AI governance and national security matters

Public International Law and Cybersecurity

- multiple clients on the application of U.S. and international law in the context of cross-border cybersecurity, involving cyber norms, sovereignty, critical infrastructure, jurisdiction, attribution standards, international humanitarian law, human rights law, espionage and the conduct of cyber activities
- the United Nations regarding international legal issues related to the prevention of cyber warfare, cyber threats to critical infrastructure and terrorist exploitation of the internet and social media, as well as data privacy law applicable to cross-border data sharing for law enforcement and counterterrorism purposes
- internet and social media companies regarding cross-border government requests for consumer data and compliance with Mutual Legal Assistance Treaties (MLAT)

Mr. Simon served as Pentagon special counsel from 2011-15, helping to develop a legal and policy framework to address cyber threats, including the response to North Korea's cyberattack on a major media and entertainment company. He also advised on cyber policy, plans and operations, social media, autonomous technologies, the use of force, counterterrorism, treaties, sensitive investigations and regional matters involving China, the Korean Peninsula, Syria, Russia, Ukraine and other countries in Asia and the Middle East. The DoD autonomy directive he helped develop established policies for the development, acquisition and employment of unmanned, semiautonomous and fully autonomous weapons technologies and represented the first policy announcement by any country regarding fully autonomous weapons. He received the Office of the Secretary of Defense Award for Excellence for his national security work.

From 2019-21, Mr. Simon served as chief cyber counsel to the Cyberspace Solarium Commission, a bipartisan commission established by Congress to develop a strategy to defend the U.S., including the private sector, from cyberattacks.

Prior to joining Skadden, Mr. Simon was a partner and co-chair of the cyber incident response team at another major global law firm.

Associations

Adjunct Fellow in Cybersecurity and International Law, Technology Policy Program, Center for Strategic and International Studies

Member, CISA Task Force, Center for Strategic and International Studies (developing recommendations for the U.S. Cybersecurity and Infrastructure Security Agency)

Senior Advisor, CSC 2.0 Project: Preserving the Legacy and Continuing the Work of the Cyberspace Solarium Commission

Honorary Member of Senior Common Room, Trinity College, Oxford University (2022-23)

Visiting Research Fellow, College of Information and Cyberspace, National Defense University (2018-21)

Experts Committee Member, UN Security Council Counter-Terrorism Committee Executive Directorate, United Nations (2017-21)

Term Member, Council on Foreign Relations (2016-21)

Member, Cyber Policy Task Force, Center for Strategic and International Studies (developed cybersecurity recommendations for the 45th presidential administration) (2015-17)

Peer Reviewer, Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual 2.0) (2015-17)