

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. He has deep experience working closely with boards, executive teams, product teams and security teams to develop holistic and pragmatic strategies for navigating rapidly evolving U.S. and European legal, regulatory, compliance and policy issues involving cybersecurity, AI and privacy. Formerly a Pentagon special counsel, chief cyber counsel to the U.S. Cyberspace Solarium Commission and practitioner of EU law in Brussels, Mr. Simon regularly assists clients as the lead investigator and crisis manager for high-stakes, cross-border incidents involving cyberattacks, data breaches, extortion, AI and regulatory defense.

Mr. Simon has dealt with some of the most significant cyber incidents on an international scale. His experience includes advising 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. Dual qualified to practice in the U.S. and the EU, 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 GDPR, NIS2, DORA and the 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.

Mr. Simon is known as a go-to cyber and privacy counsel to leading global private equity sponsors and their portfolio companies, stepping in to serve as cyber counsel and incident commander when portfolio companies face ransomware or other disruptive cyberattacks. He frequently counsels boards, C-level executives and other management as they address cyber vulnerabilities and breaches, and manage associated legal, regulatory and reputational consequences. In recent years, Mr. Simon has convened regular roundtables with CISOs, CIOs and CTOs from leading global private equity firms and their portfolio companies to assess trends and risk management strategies concerning cybersecurity, AI and privacy.

With years of experience working in data protection privacy compliance, Mr. Simon regularly advises global tech companies in regulatory defense and cross-border investigations involving GDPR, DORA and NIS2. He often helps clients manage conflicts between rapidly evolving U.S. and European regulatory regimes. He counsels clients on data governance and privacy compliance with HIPAA, ECPA, CCPA/CPRA, EU GDPR and a range of EU laws governing data protection and technology supply chain risk management.

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 50 (including in its 2024 edition), a collection of some of the "best and brightest" incident response attorneys in the country. 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 regarding:

Cybersecurity, Espionage, Electronic Surveillance and Privacy

- ransomware and extortion attacks from malicious hackers and cyber criminals involving extensive regulatory, law enforcement and intelligence investigations on multiple continents on behalf of *Fortune* 500 companies
- 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
- innovative cyber legal options to deter malicious cyber extortionists and to locate, seize and prevent the dissemination of stolen client data
- disruption of cyber threat actor infrastructure and intrusion campaigns in collaboration with law enforcement and national cyber authorities
- lead cyber counsel and breach coach for a network of more than 30 airports and related aviation infrastructure in Asia, handling a sophisticated ransomware attack that required counter-extortion negotiations and coordination with domestic, regional and international aviation, data protection, finance and law enforcement authorities
- advised a leading global network of laboratories and health care facilities on a ransomware attack and associated counter-extortion negotiations, regulatory engagement and notification
- advised multiple health care companies, online retailers and financial institutions in investigations by attorneys general and data protection authorities in the EU, Canada, Latin America and Asia following major data breaches
- advised public companies in connection with material cyber incident disclosures and related SEC cyber investigations following ransomware attacks and data breaches
- advised a global pharmaceutical manufacturer in responding to a ransomware attack involving industry disruptions; provided guidance on regulatory notification obligations across the U.S. and EU

- nation-state-sponsored cyberattacks involving 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
- advised cloud computing, data warehousing and backup companies responding to complex nation-state cyber attacks attributed to Silk Typhoon and telecommunications companies in connection with nation-state sponsored attacks attributed to Salt Typhoon
- 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
- 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

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

- 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

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

David A. Simon

Continued

AI

- advised developers of sensitive and generative AI models for government contractors, government agencies and critical infrastructure operators on model design, testing for fairness, bias, accuracy and explainability, and compliance with privacy and data governance frameworks
- counseled leading AI model developers and integrators on safety and legal and policy risks related to chemical, biological, radiological and nuclear weapons
- advised leading model developers on product liability and legal exposure under U.S. and European law, including compliance with the EU AI Act, Cyber Resilience Act and AI Liability Directive
- on behalf of management teams and boards of global financial institutions and technology companies, advice on AI governance 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
- advice to several automobile manufacturers and self-driving car companies on legal, regulatory and legislative developments, and litigation related to emerging cyber threats and autonomous technologies
- cybersecurity vulnerability management and disclosure programs, bug bounty programs and product cybersecurity risk management and assessments under privilege on behalf of 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
- tabletop exercises on hypothetical AI incidents

Data Privacy And Compliance

- assessed the overlapping and distinct obligations of a multinational medical supplier under HIPAA, U.S. state privacy laws and consumer health data privacy laws
- conducted a comprehensive overhaul of privacy and AI policies and procedures for an automotive company to account for recent developments in U.S. privacy and AI law
- remediated a consumer-facing retail company's CCPA program in response to a subpoena from the California Privacy Protection Agency
- reviewed and streamlined privacy documentation for a global private equity firm, coordinating with local counsel across jurisdictions to accommodate local legal nuances
- overhauled the data privacy compliance program for an electrical testing organization to comply with U.S. state privacy laws, including revising privacy notices, developing opt-out mechanisms and drafting template data sales and sharing agreements

Board and Executive Advisory

- recognized by public and private boards across industries as a trusted adviser; counsels directors and executive teams on cyber and AI risk management, data privacy compliance and cross-border incident response
- conducts board-directed post-cyber incident reviews and related matters
- regularly leads tabletop exercises and governance trainings to prepare boards for crisis management and fulfill fiduciary duties
- advises boards on navigating conflicting U.S. and European regulatory regimes in connection with cyber incidents, AI governance and national security matters

Public International Law and Cybersecurity

- 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
- advice to 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
- on behalf of internet and social media companies, counsel regarding cross-border government requests for consumer data, and compliance with Mutual Legal Assistance Treaties (MLAT)

Government experience provides Mr. Simon with unique insights into regulatory and policy issues affecting companies. He 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. In addition, he advised on broader matters concerning cyber policy, plans and operations, as well as 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. Mr. Simon also played a key role in the development of the Department of Defense (DoD) Directive on Autonomy in Weapons Systems, which established the department's policies on the development, acquisition and employment of unmanned, semiautonomous and fully autonomous weapons technologies. The directive represented the first policy announcement by any country regarding fully autonomous weapons. In recognition of his national security work at the DoD, Mr. Simon received the Office of the Secretary of Defense Award for Excellence.

David A. Simon

Continued

Mr. Simon served from 2019-21 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. During this time, he helped write more than 30 recently enacted cyber and privacy laws.

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