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 helping boards and executive teams navigate rapidly evolving legal compliance issues involving cybersecurity, AI and privacy. Formerly a Pentagon special counsel and chief cyber counsel to the U.S. Cyberspace Solarium Commission, Mr. Simon regularly assists clients as the lead investigator and crisis manager for high-stakes, cross-border incidents involving cyberattacks, data breaches and extortion, and AI, and handles related internal investigations 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 incidents requiring analysis of breach reporting obligations under U.S. and EU law, including the EU General Data Protection Regulation (GDPR) and investigations by European data protection 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 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 often advises clients on complex regulatory issues involving the collection, storage, use, transfer and sharing of personal and other sensitive data. 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
- negotiation and engagement 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
- 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
- cybersecurity vulnerability 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 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

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)

AI

- 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

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.

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)