Joshua Silverstein

Skadden

Counsel, Washington, D.C.

Cybersecurity and Data Privacy; National Security

T: 202.371.7148
joshua.silverstein@skadden.com

Education

J.D., Yale Law School, 2014

M.Phil., University of Cambridge, 2012
(Gates Cambridge scholar)

B.A., Yale College, 2010
(*summa cum laude*; Phi Beta Kappa)

Bar Admissions

District of Columbia

New York

Joshua M. Silverstein leverages his extensive problem-solving experience in the private and public sectors to help clients navigate complex and high-profile cybersecurity, data privacy and national security challenges. Prior to joining Skadden, Mr. Silverstein was a senior counselor and policy adviser at the U.S. Department of Homeland Security's (DHS') Cybersecurity and Infrastructure Security Agency (CISA). He provides full-spectrum support on these matters, spearheading coordinated litigation, regulatory, operational, business and policy solutions.

Mr. Silverstein has substantial experience serving as a solutions-oriented counselor to clients facing severe crises. He has guided large multinational enterprises through the challenging process of managing multijurisdictional data breaches, significant ransomware and data extortion attacks, and high-profile national security and white collar criminal investigations.

Mr. Silverstein works with clients proactively to establish processes and technology to diminish the likelihood and consequences of cybersecurity, data privacy and national security challenges. He has worked with enterprises across economic sectors to build tailored cybersecurity, data privacy, incident response, vulnerability management, operational risk management and insider threat programs. Mr. Silverstein is regularly consulted on a wide range of important public policy issues, including encryption, public-private cybersecurity collaboration, critical infrastructure cybersecurity, cybersecurity norms and international law, and surveillance and intelligence activities. Mr. Silverstein is currently a term member at the Council on Foreign Relations and has been recognized as one of Lawdragon's 500 Leading Global Cyber Lawyers. He regularly writes about topics related to cybersecurity issues and is the co-author of "The Cyberspace Solarium Commission" chapter of the Practising Law Institute's treatise *Cybersecurity: A Practical Guide to the Law of Cyber Risk*.

During his career, Mr. Silverstein has represented clients in confronting numerous concerns, including:

Cybersecurity, Espionage, Electronic Surveillance and Privacy

- ransomware and extortion attacks from malicious hackers and cyber criminals involving extensive regulatory, law enforcement and intelligence investigations across multiple jurisdictions on behalf of large, global companies
- data breach incidents requiring analysis of and compliance with breach reporting obligations under U.S. state and federal laws, the U.K. and the EU General Data Protection Regulation (GDPR), and numerous other global data protection regimes
- the management of legal and business risks involving national security criminal investigations
- negotiation and engagement with cyber threat actors through experienced private sector cyber operators
- innovative technical, operational and legal options to deter malicious cyber extortionists, and to locate, seize and prevent the dissemination of stolen client data
- telecommunications legal and regulatory issues related to government surveillance operations
- 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

- cybersecurity threat information sharing with information sharing/analysis centers and diverse federal entities, both on voluntary and mandatory bases
- cybersecurity vulnerability disclosure policies and related coordination processes involving cybersecurity researchers, the DHS and computer emergency response teams, including the U.S. Computer Emergency Readiness Team (S-CERT), Industrial Control Systems Emergency Response Team (ICS-CERT) and CERT Coordination Center (CERT/CC)
- privileged contractual arrangements for management of third-party vendor risk involving cybersecurity and national security investigations
- risk management frameworks to govern the conduct of private sector cybersecurity operations
- tabletop exercises on hypothetical cyber and business continuity incidents involving ransomware, insider threats, nation-state attacks, and third-party and supply chain attacks

Public International Law and Cybersecurity

- the application of U.S. and international law involving cross-border cybersecurity, including cyber norms, sovereignty, critical infrastructure, jurisdiction, attribution standards, international humanitarian law, human rights law, espionage, and the conduct of cyber defensive and intelligence activities
- advice to the United Nations regarding international legal issues surrounding 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
- advice to the U.S. Cyberspace Solarium Commission on legal issues related to its recommendations and legislative proposals under U.S. and international law

AI

- legal, regulatory and litigation developments related to the development and deployment of autonomous and connected vehicle technologies
- penetration testing and other adversarial analysis of autonomous technologies

While at CISA, Mr. Silverstein was responsible for helping develop and coordinate critical infrastructure cybersecurity policy across the agency, the federal government and the White House National Security Council. He provided strategic guidance and policy advice on various cybersecurity challenges, including ransomware, incident reporting and response, regulatory and legislative actions, performance measurement and data collection, vulnerability management and disclosure, and operational collaboration with the private sector. Mr. Silverstein created and oversaw the implementation of a first-of-its-kind coordination and reporting structure for agency response to specific nation-state cyber threats. He also contributed to numerous initiatives related to private sector cybersecurity. Most notably, he supported the development of the implementing regulation for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) — landmark legislation that will facilitate a cross-sectoral critical infrastructure incident reporting regime. He also contributed to the rollout and analysis of the inaugural Cybersecurity Performance Goals, a prioritized subset of cybersecurity practices that private sector entities can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.

Before joining CISA, Mr. Silverstein worked at another global law firm in its Washington, D.C. office, where he helped establish its global cybersecurity and data privacy practice. During this time, he also served on a *pro bono* basis as deputy chief counsel for cybersecurity and national security to the U.S. Cyberspace Solarium Commission, a high-profile, bipartisan commission established by Congress to develop a strategy to defend the U.S., including the private sector, from cyberattacks. Earlier in his career, Mr. Silverstein served in the Department of Defense and advised on cybersecurity, counterterrorism, intelligence and CFIUS matters in the National Security Division of the U.S. Department of Justice.