Steptoe counsels and represents clients on global privacy and cybersecurity issues, ranging from compliance with the ever-expanding laws and regulations concerning individual privacy and data security, to advising companies on preventing or responding to data breaches, to defending companies facing class action lawsuits or regulatory investigations emanating from a breach or a failure to comply with applicable laws. Steptoe’s lawyers also bring a unique depth of experience in these issues from their time as senior officials in the federal government, where they helped create policies and programs to address cybersecurity and held key leadership positions in law enforcement, intelligence, and security.

Our Team's Experience at a Glance

- Head of the FBI’s cybercrime and infrastructure protection program
- Associate Deputy Attorney General for national security matters
- Assistant Secretary for policy at the Department of Homeland Security
- General counsel of the National Security Agency
- Deputy Assistant Attorney General responsible for cyber investigations

Privacy and Cybersecurity Compliance

Steptoe’s lawyers regularly advise companies on how to comply with the burgeoning field of onerous new laws and regulations in the field, ranging from relatively new ones (such as the California Consumer Privacy Act (CCPA), the European Union’s General Data Protection Regulation (GDPR), and the New York Department of Financial Service’s Cybersecurity Regulation), to more longstanding ones (such as the FTC Act, the Gramm-Leach-Bliley Act and implementing regulations, the Health Insurance Portability and Accountability Act (HIPAA) and its regulations, and the 50 US State and 4 territorial data breach notification laws).

In the European Union, the privacy and cybersecurity landscape is evolving more rapidly than ever before. New services and technologies are challenging boundaries of existing frameworks, such as the GDPR, the Directive on security of network and information systems (NIS Directive), and the Cybersecurity Act, while also prompting new legislative proposals such as the ePrivacy Regulation, and the Digital Services Act package. Increased accountability toward users requires organizations to test new responses such as broader use of standards or certification mechanisms. Steptoe is uniquely positioned to assist organizations facing these challenges, as we have experience dealing with the sometimes conflicting challenges raised by multiple regulatory frameworks and enforcement agencies.

Data Breach Prevention, Response, and Litigation

Steptoe understands the high stakes involved when sensitive data is at risk. Our lawyers work to protect companies both before and after a data breach. We provide assistance in the development or improvement of data privacy practices and incident response plans to ensure our clients’ data is secure. Our goal is to always minimize our client’s risk of a data breach and to put our client in the best position to respond if a breach occurs. In the event of a breach, we provide rapid and comprehensive incident response.
Critical Infrastructure Protection

The US government is increasingly focused on protecting the nation’s critical infrastructure (including companies in the communications, energy, financial, and medical industries) from destructive cyber and physical attacks and ensuring security within its own supply chain. Steptoe advises companies that are related to the nation’s critical infrastructure as well as those seeking government contracts on the existing legal requirements that govern critical infrastructure protection, as well as on prospective new regulations emanating from Congress and the Executive Branch. Drawing on our experience in government, we also provide strategic counseling on opportunities for security and telecommunications companies seeking to adapt their technologies for use by the Department of Defense, DHS, and law enforcement and security agencies.

In the European Union, the NIS Directive is one set of frameworks targeting key industries (such as finance, insurance, utilities, and transportation) and actors (including digital service providers), and imposing high security thresholds for companies across the supply chain. Steptoe advises organizations to meet these requirements.

National Security and Law Enforcement Investigation

Government investigations often require businesses in the technology, communications, e-commerce, Internet service, and financial industries to provide information about their customers and subscribers, thereby forcing them to navigate sometimes conflicting legal obligations arising out of multiple privacy and security laws worldwide. We advise numerous companies regarding law enforcement and intelligence access to communications and information under a variety of applicable laws, including Title III, ECPA, the Communications Act, the Foreign Intelligence Surveillance Act, FCRA, and the USA PATRIOT Act. We also regularly advise companies on compliance with foreign government demands for information. With our extensive government experience, Steptoe lawyers are able to provide direct interface and engagement with the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Department of Justice (DOJ), and DHS, as well as state, local, and foreign agencies.

Businesses that are the victims of cyberattacks (whether denials of service, thefts of money or property, espionage, or other malicious acts) also must determine when and how to cooperate with government agencies during investigation of an attack, and how best to do so. The lawyers in our privacy and cybersecurity practice have deep experience, from both government and private practice, in this area, and help companies navigate the often complicated interactions with government agencies.

Additionally, Steptoe’s white-collar defense practice is nationally recognized, enabling us to provide both counseling and representation where the threat of prosecution may arise.

Encryption

Our team has extensive legal and technical experience in data encryption technology, and offers our clients guidance in complying with US and international requirements governing all aspects of encryption, including encryption export and import licensing matters in the United States, France, China, Russia, Hong Kong, and other countries.

Our web-based Country-by-Country Guide to Encryption Regulations is the leading resource on global encryption import, use and export controls, covering more than 130 countries. We counsel both developers and users of encryption products on global licensing and distribution strategies. In addition, we have one of the broadest and most sophisticated public key infrastructure (PKI) practices of any law firm, and are among a very small number of law firms worldwide that regularly practice in this area. Our work includes advising clients on developing and implementing industry PKIs in the insurance, mortgage finance, healthcare, financial services, and natural resources industries. We also advise many clients on developing and implementing enterprise PKI solutions and other secure business solutions that incorporate PKI technology.
Representative Matters

Represented the VTech group of companies regarding a breach of its customer information, including advice on managing the response to the breach, settlement negotiations with the FTC and international data protection authorities, and dismissal of consolidated class action claims.

• Represented best-selling author in suit claiming violation of federal and state privacy and computer crime laws.
  Represented Verizon and other communications and technology companies in amicus briefs challenging government's authority to obtain communications content stored abroad.
  Advising numerous retail companies, financial institutions, and others on compliance with CCPA, GDPR, and other laws.
  Helping a global insurance firm assess and improve their data privacy and cybersecurity policies and practices, including breach response.
  Advising an insurance broker and consultant on its data security and privacy policies and drafting an incident response plan.
  Assessing the cybersecurity policies and incident response plan of a leading data-mining and Internet advertising company and recommending changes, and developing and leading a "tabletop" data breach exercise to assess and improve the company's data breach response posture.
  Advising defense contractors on Defense Department supply chain and service provider cybersecurity requirements.
  Advising some of world's largest financial institutions, communications firms, hardware and software manufacturers, and others on data security requirements, and data privacy and encryption laws and regulations domestically and worldwide.
  Representing a national retailer in a proposed class action brought by employees claiming that their employer used a palm scanner without adequate notice or consent procedures required under the Illinois Biometric Information Privacy Act.
  Obtained dismissal of two class actions against a multinational publishing and education company in connection with a data security incident involving an educational technology product that allegedly resulted in unauthorized access to student information from 13,000 school and university accounts.
  Represented a medical practice and doctor accused of disclosing protected patient health information to a third party in violation of state laws and regulations protecting patient privacy.
News & Publications

PRESS RELEASES
Steptoe Receives 27 Practice Rankings, 31 Individual Awards in Legal 500 US 2021
September 13, 2021

CLIENT ALERTS
European Commission Proposes to Overhaul AML Framework with New Legislative Package
August 16, 2021
By: Guy Soussan, Charles-Albert Helleputte, Diletta De Cicco, Stefan Tsakanakis, Charlotte Brett

Belgium: Balancing Data Protection and National Security
July 2020
By: Diletta De Cicco, Charles-Albert Helleputte

PUBLICATIONS
Personal Data Transfers After Year Zero: A More Appealing Set of EDPB Recommendations?
July 2020
By: Diletta De Cicco, Charles-Albert Helleputte

CLIENT ALERTS
New York DFS Issues Guidance on Ransomware Prevention and Response
July 9, 2021
By: Michael Vatis, Daniel W. Podair

CLIENT ALERTS
Colorado Becomes Third State to Adopt a Comprehensive Privacy Law
July 8, 2021
By: Michael Vatis, Daniel W. Podair

PUBLICATIONS
Personal Data Transfers After Year Zero: Are the New SCCs a Paradigm Shift?
June 30, 2021
By: Diletta De Cicco, Charles-Albert Helleputte

CLIENT ALERTS
Big Apple Takes a Bite at Biometrics
June 21, 2021
By: Michael Vatis, Daniel W. Podair

CLIENT ALERTS
To Understand the CFAA, It Depends on What the Meaning of the Word ‘So’ Is
June 7, 2021
By: Michael Vatis

PRESS RELEASES
Steptoe’s Diletta De Cicco Tapped to IAPP Diversity in Privacy Board
May 18, 2021
Events
WEBINARS
Data Privacy for Retailers: Recent Developments in CCPA and GDPR
December 10, 2019
Speakers: Paul Hughes, Daniel W. Podair, David O’Sullivan

WEBINARS
The Long Arm of the New EU Data Protection Jurisdiction
The Global Reach of GDPR (Part I)
December 6, 2017
Speakers: Stewart A. Baker, Maury Shenk

SEMINARS & EVENTS
Election Cybersecurity
How Bad Is It and What Can We Do About It?
November 7, 2017
Speaker: Stewart A. Baker
Steptoe
1330 Connecticut Avenue, NW
Washington, DC 20036

SEMINARS & EVENTS
Emerging Cyber Attack Trends and Technical and Legal Remedies
A co-sponsored event with Kroll
February 24, 2016
Speakers: Stewart A. Baker, Steven K. Davidson, Michael Campion Miller
The Harvard Club
35 W. 44th Street
New York, NY 10036

WEBINARS
Digitizing Financial Services in Europe: Managing Risks, Maximizing Benefits
June 25, 2015
The Cyberlaw Podcast

THE CYBERLAW PODCAST
Episode 374: What's the Opposite of Facial Recognition? Ask Your "Smart Toilet."
September 13, 2021

THE CYBERLAW PODCAST
Episode 373: We Can't Run a Twelfth-Century Regime Without WhatsApp!
September 7, 2021

THE CYBERLAW PODCAST
Episode 372: Blockchain and Cryptocurrency Regulatory Roundup
August 24, 2021

THE CYBERLAW PODCAST
Episode 371: Fighting Ransomware by Pushing All the Buttons on the Dashboard
July 19, 2021

THE CYBERLAW PODCAST
Episode 370: Should We Add “Jumping U.S. Red Lines” to the 2021 Olympics?
July 12, 2021

THE CYBERLAW PODCAST
Episode 369: This Episode Could Be Worth $1,000 to the ACLU
July 6, 2021

THE CYBERLAW PODCAST
Episode 368: The Trustbusters Come for Big Tech
June 28, 2021
By: Stewart A. Baker

THE CYBERLAW PODCAST
Episode 367: President Biden’s European Cybertour
June 21, 2021

THE CYBERLAW PODCAST
Episode 366: Are Stealth Quotas the Cure for AI Bias?
June 14, 2021
By: Stewart A. Baker

THE CYBERLAW PODCAST
Episode 365: Transatlantic Drift
June 7, 2021

Resources

RESOURCES
EU General Data Protection Regulation (GDPR)
Key Compliance Issues for US Companies

RESOURCES
The Value of Understanding International Encryption Regulation
Toolkits

Data Breach Toolkit
By: Stewart A. Baker, Michael Vatis, Alan Cohn

Explore Related

Primary Contacts

Michael Vatis
Charles-Albert Helleputte

Practices

Commercial Litigation
Export Controls
Blockchain & Cryptocurrency
Insurance & Reinsurance
National Security/CFIUS
Retail & E-Commerce

© 2021 STEPTOE & JOHNSON LLP. ALL RIGHTS RESERVED. ATTORNEY ADVERTISING.