

**Debevoise
& Plimpton**

Data Strategy & Security

Introduction

Data has become one of companies' most valuable assets and greatest risks.

The global flow of information creates constantly changing challenges: How do companies acquire, store, protect, use and share data to keep up with the competition, while reducing their legal and reputational risks?

Companies need an experienced and creative partner to work closely with them to formulate and achieve their overall data strategy, whether they are

- Preparing for a ransomware attack or other significant cyber, privacy or AI event,
- Evaluating the data-related risks and benefits of an acquisition,
- Facing scrutiny over their cybersecurity or privacy policies and practices,
- Responding to investigations or litigation relating to a data breach, or
- Developing an artificial intelligence or big data program.

Named a **winner** in the “Innovation in Digitizing Legal Services” category by the *Financial Times*’ 2022 North America Innovative Lawyers Awards

Ranked as an “elite” firm for Privacy & Data Security.

“The team contains a deep bench of subject matter experts.”

“The depth of the group’s experience and the reach of their contacts within the industry are invaluable.”

Chambers USA, 2024

Ranked as a leading firm for Cyber Law (including Data Privacy & Data Protection).

“The expertise of the lawyers at Debevoise is unmatched. They have some of the most experienced lawyers in the trade.”

“The team’s breadth of knowledge stands out; I would consider them not just practitioners, but experts in the field.”

The Legal 500 US, 2024

Data Strategy & Security Services

The Debevoise Data Strategy & Security (DSS) practice is global and interdisciplinary—combining our cybersecurity, privacy, artificial intelligence, business continuity, M&A diligence and data governance practices into one fully integrated and coordinated group.


Together, we advise leading companies on preparing for and responding to cybersecurity incidents, and handling related regulatory and civil litigation matters. Our incident response matters range from ransomware attacks to insider threats to nation-state intrusions, and our ability to guide clients through the full range of issues in the most complex cross-border incidents has been our calling card.

We also advise our clients on their overall data strategy, including how to manage, protect, and optimize their data, including through the use of artificial intelligence. Our strategic advice includes both legal and technical assistance with the data issues that arise in M&A diligence, licensing and vendor contracting. In addition, we help our clients determine what data they should delete or not collect because of cybersecurity, privacy or other risks.

Our integrated strategic advice on data includes:

- Helping clients across the globe prepare for, and respond to, significant data breaches and related investigations and litigation. In addition to our U.S. offices, we serve clients from offices strategically located in the United Kingdom, France, Germany, China and Hong Kong. We also regularly work on matters that involve a wide range of other non-U.S. jurisdictions, including the EU and EEA, Japan, Singapore, Brazil, Canada, Colombia, Sweden and Argentina, to name a few.
- Identifying existing and proposed laws and standards in the United States and around the world that will impact our clients' use of data, including regulations and guidance relating to cybersecurity, privacy, AI, data minimization, records retention, document discovery and data governance.

Because we are constantly leading responses to significant cyber, privacy and AI incidents, we are able to channel that deep experience into helping our clients improve their preparations and resilience. Based on our incident work, we regularly assess our clients' incident response plans, policies, processes, training and resources, and make suggestions to allow them to more effectively respond to the latest cybersecurity, privacy and AI challenges that they face.



“Ransomware attacks are very complex and sophisticated; however, this group is able to break down this complexity in a tangible way.”

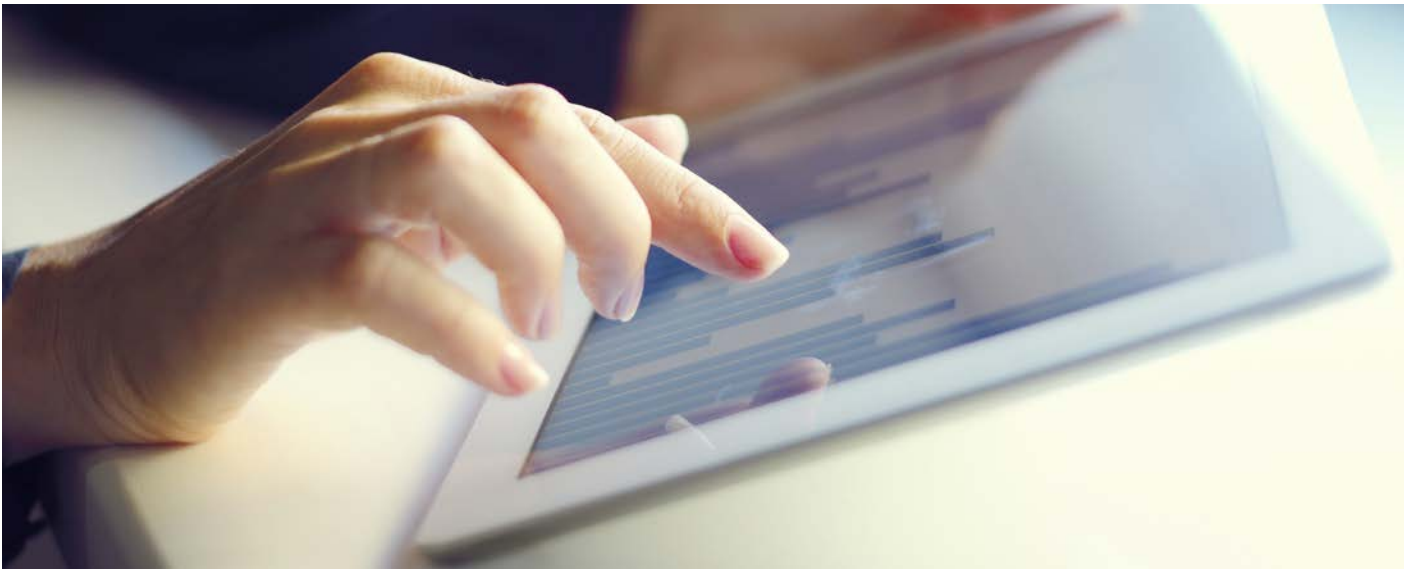
Chambers USA, 2023

A FULL RANGE OF DATA GOVERNANCE, PROTECTION AND PRIVACY SERVICES, INCLUDING CYBER INCIDENT RESPONSE AND MANAGING AI RISK

Our experience and advice covers the full spectrum of cyber threats (including from nation states, criminal ransomware groups, insiders, and critical vendors), as well as compliance with the ever-growing array of cybersecurity, privacy and AI regulations in the U.S. and across the globe.

- **360° Incident Response Services.** Debevoise helps clients navigate cyber incidents with the full range of services, including immediate crisis management, internal and external communications, fact investigation, breach notification, regulator and law enforcement engagement, civil regulatory investigations, defense of class action and derivative litigation and briefings to the board and C-Suite.
- **Engaging with Law Enforcement in the U.S. and Globally.** We are able to leverage our worldwide network of law enforcement contacts in the event of an incident. Our team includes several former federal cybercrime prosecutors, including the former leader of the Justice Department’s Criminal Division, the former leader of the Department’s response to national security cyber threats, and two other former Assistant U.S. Attorneys who brought landmark cyber cases in the country’s federal courts.
- **Review/Update Data Policies and Governance.** We can provide an assessment of the company’s policies and procedures for the protection and handling of consumer and employee personal data, as well as sensitive company information, with particular attention to mitigation of legal, business and reputational risks.

- **Cyber-, Privacy- and AI-Risk Assessment.** In today's dynamic regulatory environment, managing risks at the intersection of law and technology means measuring data protection and data optimization strategies against existing laws and regulations, as well as anticipated changes in the legal and threat environments. We review companies' cybersecurity, privacy and AI programs and assess them against existing and emerging legal standards. Our work ranges from leading a full legal and technical risk assessment of various data programs, typically performed in tandem with a technical vendor, to a targeted review of areas known to attract regulatory and enforcement focus.
- **Board/Executive Briefings and Training.** We regularly brief boards and company executives on the latest threats their companies face relating to data in order to help them assess risk, allocate resources, maintain appropriate insurance, prevent avoidable losses and discharge their oversight obligations. We also provide training on cybersecurity, privacy and AI risks to new executives and board members, as well as anyone wishing to learn more about their responsibilities in these areas.



- **Realistic Tabletop Exercises.** We are known for running extremely realistic cyber incident simulations or “tabletops” to help our clients prepare for adverse cybersecurity, privacy and AI events by conducting real-world drills of actual data events for various functions within the organization including Legal, Compliance, IT, Risk, Communications, Executive Management and the Board. These exercises, which regulators increasingly expect companies to conduct, allow our clients to test their incident response plans and see how their organization works through emergency data events, including ransomware attacks that shut down operations, insider data theft, whistleblower allegations of AI bias, state-sponsored hacking of sensitive commercial information, leaking of large volumes of customer or employee personal information and compromise of a critical vendor's information systems.

- **Vendor Risk Review.** Cyber incidents often involve exploitation of a vendor’s trusted access to the company’s systems, its handling of sensitive data on behalf of the company or risks posed by the vendor as a single point of operational failure. Accordingly, regulators have honed in on this challenging area. We work with our clients to develop practical, risk-based strategies to manage third party cyber, privacy and AI risks through their policy development, diligence efforts, contractual terms, and insurance strategies.
- **M&A Due Diligence.** Data risks are increasingly prominent in M&A due diligence and in the post-acquisition integration process. We often lead cyber, privacy and AI diligence investigations around the world, including advising on policies and procedures for due diligence and for integration generally, as well as on risks and issues raised by specific actual or potential acquisitions and investments.
- **Insurance.** Companies increasingly are concluding that cyber-, AI-, and privacy-specific insurance policies are essential. Our team has significant experience working inside the insurance industry and can review existing policies to assess coverages and exclusions.

REAL-WORLD EXPERIENCE

Our services are based on experience in the trenches of many of the country’s landmark cyber and privacy incidents (including many non-public incidents). Our lawyers have deep technical knowledge that allows them to translate complex technical findings into legal and business decision points. This has enabled us to provide a pragmatic approach to identifying and coordinating the key elements of effective incident response and overall data strategy.

Before joining Debevoise, partner Luke Dembosky served as Deputy Assistant Attorney General for National Security, managing the Justice Department’s work on all national security cyber incidents, including the cyber attack on Sony Pictures and the landmark breaches of Target, The Home Depot, Anthem and the U.S. Office of Personnel Management, among many others. At Debevoise, Luke co-chairs the cyber and privacy practice, acting for the firm’s clients on high-profile and high-stakes global and U.S. breach matters.

Our Team Leads

North America | United States

Luke Dembosky



Partner and Practice Leader, Washington, D.C.
ldembosky@debevoise.com • +1 202 383 8020

Luke Dembosky Co-Chairs the firm's global Data Strategy and Security practice. He advises companies on managing cyber risks, responding to cyber incidents, and handling related internal investigations and regulatory defense. Luke is ranked by *Chambers* among the top cyber incident response and crisis management attorneys. Luke joined Debevoise in March 2016 after serving as Deputy Assistant Attorney General for National Security at the U.S. Department of Justice, where he oversaw all national security cyber matters for the agency. His 14 years at DOJ included serving as DOJ's representative at the U.S. Embassy in Moscow, and as the senior DOJ official on the Target, Sony Pictures, Anthem, and OPM breaches, among many others.

Avi Gesser



Partner and Practice Leader, New York • agesser@debevoise.com • +1 212 909 6577

Avi Gesser is Co-Chair of the firm's Data Strategy & Security Group. His practice focuses on advising major companies on a wide range of cybersecurity, privacy and artificial intelligence matters. He has represented global financial services firms, private equity firms, insurance companies, hedge funds and media organizations in large-scale ransomware attacks, cyber breaches by nation-states, and regulatory investigations relating to the use of artificial intelligence. Mr. Gesser regularly advises boards and senior executives on governance, risk, and liability issues relating to cybersecurity and AI. Mr. Gesser is also a primary author of the firm's Data Blog and the architect of the Firm's Data Portal, an online tool that helps clients quickly assess and comply with their cyber breach notification obligations and tracks AI regulatory developments. He is recommended by *Chambers USA* as a leading lawyer for privacy and data security and in *The Legal 500*.

Erez Liebermann



Partner, New York • eliebermann@debevoise.com • +1 212 909 6224

Erez Liebermann is a litigation partner and a member of the firm's Data Strategy & Security Group. His practice focuses on advising major businesses on a wide range of complex, high-impact cyber-incident response matters and on data-related regulatory requirements. With decades of experience in data issues as a litigator, federal prosecutor and senior in-house counsel at a global insurance company, Mr. Liebermann regularly advises clients at the C-suite and board level on building strategies to reduce their data-related regulatory and reputational risks, and on navigating high-profile government investigations following data incidents. He is also widely acknowledged as a leading cybersecurity and data privacy professional and is ranked among the leading lawyers by *Chambers Global* (2024), *Chambers USA* (2024) and *The Legal 500* (2024). Clients note that he is "very talented" and "one of the most intelligent attorneys, [and] very practical and great to work with."

Charu A. Chandrasekhar



Partner, New York • cchandra@debevoise.com • +1 212 909 6774

Charu A. Chandrasekhar is a litigation partner based in the New York office and a member of the firm's White Collar & Regulatory Defense Group. Her practice focuses on securities enforcement and government investigations, including cybersecurity issues and internal investigations. Prior to joining the firm, Ms. Chandrasekhar served as an Assistant Regional Director in the SEC's Division of Enforcement and as the founding Chief of the Division's Retail Strategy Task Force. Ms. Chandrasekhar also served as a Senior Advisor and Senior Counsel in the Division of Enforcement's Market Abuse Unit.

Maura Kathleen Monaghan



Partner, New York • mkmonaghan@debevoise.com • +1 212 909 7459

Maura Kathleen Monaghan is a member of the firm's Litigation Department whose practice focuses on a wide range of complex commercial litigation, including regulatory and civil litigation matters involving data breaches. Ms. Monaghan is recognized as a "Litigation Star" by *Benchmark Litigation* and as one of the "Top 250 Women in Litigation" in the *IFLR Benchmark Litigation Guide*.

Jim Pastore



Partner, New York • jjpastore@debevoise.com • +1 212 909 6793

Jim Pastore is a litigation partner and a member of the firm's Cybersecurity & Data Privacy practice and Intellectual Property Litigation Group. His practice focuses on privacy and cybersecurity issues. Mr. Pastore is recognized by *Chambers USA* and *The Legal 500 US* for his cybersecurity work, and was included in *Benchmark Litigation's* Under 40 Hot List which recognizes attorneys under 40 with outstanding career accomplishments. *Chambers USA* (2024) also places Mr. Pastore in the top band for Incident Response. Mr. Pastore has also been named six consecutive times to *Cybersecurity Docket's* "Incident Response 50," a list of the best and brightest data breach response attorneys. Prior to rejoining Debevoise in 2014, Mr. Pastore served for five years as an Assistant United States Attorney in the Southern District of New York where he spent most of his time as a prosecutor with the Complex Frauds Unit and Computer Hacking and Intellectual Property Section.

Kristin A. Snyder



Partner, San Francisco • kasnyder@debevoise.com • +1 415 738 5718

Kristin Snyder is a litigation partner and member of the firm's White Collar & Regulatory Defense Group. Her practice focuses on securities-related cybersecurity, regulatory and enforcement matters, particularly for private investment firms and other asset managers. Ms. Snyder is recommended by *The Legal 500 US*. Prior to her role at Debevoise, Ms. Snyder served at the U.S. Securities & Exchange Commission (SEC) for 18 years, most recently serving as the Deputy Director of the Division of Examinations resident in its San Francisco Regional Office. In her role, she spearheaded the development of examination priorities for the national and international examination programs covering a spectrum of SEC registrants including investment advisers, investment companies, and broker-dealers.

David Sarratt



Partner, San Francisco • dsarratt@debevoise.com • +1 212 909 6864

David Sarratt is a partner in the firm's Litigation Department. He is a seasoned trial lawyer whose practice focuses on government enforcement actions, internal investigations and complex civil litigation for financial institutions and other clients. Mr. Sarratt has particular experience in matters relating to compliance with the Bank Secrecy Act and the Foreign Corrupt Practices Act, as well as with novel enforcement issues arising from new technologies.

Bruce E. Yannett



Partner, New York • beyannett@debevoise.com • +1 212 909 6495

Bruce Yannett is Chair of the White Collar & Regulatory Defense Practice Group and also served as Deputy Presiding Partner of the firm from July 2011 until June 2022. He focuses on white collar criminal defense, regulatory enforcement and internal investigations. He represents a broad range of companies, financial institutions and their executives in matters involving securities fraud, accounting fraud, foreign bribery, cybersecurity, insider trading, and money laundering. He has extensive experience representing corporations and individuals outside the United States in responding to inquiries and investigations. Mr. Yannett's practice also encompasses complex litigation, including derivative cases, shareholder actions and commercial disputes.

Matthew Kelly



Counsel, New York • makelly@debevoise.com • +1 212 909 6990

Matthew Kelly is a counsel and a member of the Data Strategy & Security Group. His practice focuses on advising the firm's growing number of clients on matters related to AI governance, compliance and risk management, and on data privacy. Mr. Kelly has extensive experience advising public companies, and companies across the financial services sector, on internal investigations and regulatory matters involving data strategy, governance and compliance. He has advised clients on the usage of quantitative modeling tools and data-driven operations, and on the design and implementation of post-Dodd-Frank model governance frameworks. Mr. Kelly has also led multiple advisory and regulatory matters related to algorithmic trading and data governance for broker-dealer and investment advisory clients, including SEC, FINRA, and New York Attorney General investigations. Mr. Kelly is ranked as Up and Coming by Chambers for Privacy and Data Security and is recognized by *The Legal 500 US* for Cyber Law.

Johanna Skrzypczyk



Counsel, New York • jnskrzypczyk@debevoise.com • +1 212 909 6291

Johanna Skrzypczyk is a counsel in the Data Strategy and Security practice of Debevoise & Plimpton LLP. Her practice focuses on advising AI matters and privacy-oriented work, particularly related to the California Consumer Privacy Act. Prior to joining Debevoise, Ms. Skrzypczyk served as Assistant Attorney General in the Bureau of Internet and Technology at the New York Attorney General's Office. In this role, she helped draft the amendments to New York's data breach law (known as the SHIELD Act), investigated, litigated, and negotiated the landmark settlement of an action against a national corporation regarding credential stuffing, one of the very few regulatory actions to address this widespread type of cyberattack, and co-led an initiative involving potential discriminatory impacts of AI. Ms. Skrzypczyk also worked on matters involving consumer privacy, data security and virtual markets. Ms. Skrzypczyk was recognized by *The Legal 500 US* in the Cyber Law category.

Christopher S. Ford



Counsel, San Francisco • csford@debevoise.com • +1 212 909 6881

Christopher S. Ford is a counsel in the Litigation Department who is a member of the firm's Intellectual Property Litigation group and Cybersecurity & Data Privacy practice. His practice focuses on trademark, cybersecurity, and data privacy issues. His cybersecurity and data privacy practice includes advising clients on incident preparation and response, as well as related criminal and civil litigation and regulatory investigations. His recent matters include managing responses to corporate data breaches, ransomware incidents, and other data security issues, as well as assisting a wide range of the firm's clients in managing their cybersecurity and related supply chain risks.

Kim T. Le



Counsel, San Francisco • kle@debevoise.com • +1 415 738 5706

Kim T. Le is a corporate counsel and a member of the firm's Healthcare & Life Sciences Group. She is also active in the firm's Data Strategy & Security practice. As a leading practitioner on privacy, data security and cyber-security issues, Ms. Le provides expertise in data breach reporting, including covered entity and business associate obligations under the HIPAA breach notification rule and audit response. Further, Ms. Le counsels clients regarding privacy and security preparedness, routinely redesigning compliance programs for provider organizations, hybrid entities, service vendors and technology companies to improve operational effectiveness and decrease compliance risk.

Tigist Kassahun



Counsel, Washington, D.C. • tkassahu@debevoise.com • +1 202 383 8052

Tigist Kassahun is a corporate counsel and a member of the firm's Intellectual Property and Mergers & Acquisitions Groups, as well as a frequent collaborator with the firm's Data Strategy & Security practice. Ms. Kassahun is experienced in leading intellectual property and technology transactions and advising clients on related matters, including intellectual property protection, data privacy and cybersecurity. She regularly represents a broad range of clients across the technology, financial services, arts, telecommunications, private equity, entertainment, healthcare and insurance industries.

Mengyi Xu



Associate, New York • mxu@debevoise.com • +1 212 909 6826

Mengyi Xu is an associate in the Litigation Department and a Certified Information Privacy Professional (CIPP/US). As a member of the firm's interdisciplinary Data Strategy & Security practice, she helps clients navigate complex data-driven challenges, including issues related to cybersecurity, data privacy, and data and AI governance. Mengyi's cybersecurity and data privacy practice focuses on incident preparation and response, regulatory compliance, and risk management.

Europe | United Kingdom

Jane Shvets



Partner, London & New York • jshvets@debevoise.com • +44 20 7786 9163/+1 212 909 6000

Jane Shvets is a partner who splits her time between our London and New York offices, and who plays a leading role in our Cybersecurity & Data Privacy and White Collar practices. Ms. Shvets has significant expertise in global compliance advice, with a particular emphasis on EU data protection and data transfer issues and managing cross-border data flows associated with complex multinational litigation and investigations as well as foreign corrupt practices legislation. She is the co-author of multiple publications on implications for cross-border data flows of Brexit, the upcoming General Data Protection Regulation (GDPR), the EU-U.S. Privacy Shield, and other developments in the law. Ms. Shvets is a native Russian speaker and is proficient in Ukrainian.

Karolos Seeger



Partner, London • kseeger@debevoise.com • +44 20 7786 9042

Karolos Seeger is a partner in the firm's White Collar & Regulatory Defense Group and International Dispute Resolution Group, based in the London office. His practice focuses on white collar crime and internal investigations, in particular regarding compliance with corrupt practices legislation, conducting compliance assessments and creating and implementing appropriate compliance programs and procedures. He also focuses on cybersecurity and European data protection matters, as well as complex litigation and international arbitration. Mr. Seeger is a Solicitor-Advocate (Higher Rights of Audience). He is admitted to practice law in England and Wales (2000) and is an accredited Mediator with ADR Chambers. He is fluent in German and Greek and speaks French.

Robert Maddox



Counsel, London • rmaddox@debevoise.com • +44 20 7786 5407

Robert Maddox is a member of our Cybersecurity & Data Privacy practice as well as our White Collar & Regulatory Defense and International Dispute Resolution Groups. His practice focuses on complex multi-jurisdictional investigations, disputes and cybersecurity matters. Prior to entering private practice, Robert interned on the defense team of Thomas Lubanga Dyilo, the first individual to stand trial before the International Criminal Court in The Hague. Robert advises clients on cybersecurity and data protection issues in the EU, including financial services reporting obligations. He publishes and speaks on these topics frequently. Robert's recent articles have been featured in *Strategic Risk* and *Global Reinsurance* and his views on the incoming EU General Data Protection Regulation were featured by *The Deal*.

Europe | France

Alexandre Bisch



Counsel, Paris • abisch@debevoise.com • +33 1 40 73 13 37

Alexandre Bisch is a counsel in the Paris office and a member of the firm's Litigation Department. Mr. Bisch focuses on white collar criminal defence and commercial litigation. He advises and represents companies and their executives in matters involving criminal, regulatory and internal investigations. He also represents clients on a variety of civil and commercial disputes, including domestic and international litigations and enforcement of foreign judgments and arbitral awards.

Fanny Gauthier



Associate, Paris • fgauthier@debevoise.com • +33 1 40 73 12 90

Fanny Gauthier is a member of our International Dispute Resolution Group, as well as the firm's Cybersecurity & Data Privacy practice. Based in our Paris office, her practice focuses on complex domestic and international litigation. Prior to joining the firm last year, Ms. Gauthier trained as an intern in a Paris-based boutique firm specializing in arbitration and in the London office of a leading international law firm. She also interned with the Presidency of the French Supreme Court for civil and commercial matters, and in the financial law team of the Caisse des Dépôts et Consignations, a major public investment group. Ms. Gauthier is a native French speaker, fluent in English and proficient in Spanish.

Asia | Shanghai

Philip Rohlik



Counsel, Shanghai • prohlik@debevoise.com • +86 21 5047 0788

Philip Rohlik is a member of the firm's Litigation Group and leads our dispute resolution team in Shanghai. His practice focuses on international investigations, securities law and dispute resolution. It has included representation of U.S. and multinational companies in complex litigation and investigations, with a particular focus on Asia, including regularly counseling clients on relevant data protection and networks securities regulations in China. Mr. Rohlik also regularly advises corporate clients on regulatory issues arising in the course of their business around the globe or in connection with M&A transactions. Mr. Rohlik is admitted to practice law in New York and the United States District Court for the Southern District of New York, and is a solicitor admitted to appear before the High Court of Hong Kong.

New York

66 Hudson Boulevard
New York, NY 10001
Tel: +1 212 909 6000
Fax: +1 212 909 6836

Washington, D.C.

801 Pennsylvania Avenue N.W.
Washington, D.C. 20004
Tel: +1 202 383 8000
Fax: +1 202 383 8118

San Francisco

650 California St
San Francisco, CA 94108
Tel: +1 415-738-5700
Fax: +1 415 644 5628

London

65 Gresham Street
London
EC2V 7NQ
Tel: +44 20 7786 9000
Fax: +44 20 7588 4180

Paris

103 rue de Grenelle
75007 Paris
Tel: +33 1 40 73 12 12
Fax: +33 1 47 20 50 82

Frankfurt

Taunustor 1 (TaunusTurm)
60310 Frankfurt am Main
Tel: +49 69 2097 5000
Fax: +49 69 2097 5555

Debevoise & Plimpton (Luxembourg) SCS

Inscrit au Barreau de Luxembourg
4a, rue Albert Borschette
L-1246 Luxembourg
+352 28 5795 33 00

Hong Kong

21/F AIA Central
1 Connaught Road Central
Hong Kong
Tel: +852 2160 9800
Fax: +852 2810 9828

Shanghai

13/F, Tower 1
Jing'an Kerry Centre
1515 Nanjing Road West
Shanghai 200040
Tel: +86 21 5047 1800
Fax: +86 21 5047 1600

debevoisedata.com
privacy
security
protection