THE INVESTIGATIONS REVIEW OF THE AMERICAS 2018

Published by Global Investigations Review in association with:

Blake, Cassels & Graydon LLP
Campos Mello Advogados
D'Empaire Reyna Abogados
EY
Herbert Smith Freehills
Hogan Lovells
Kirkland & Ellis LLP
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados
Miller & Chevalier Chartered
Mitrani Caballero Ojam & Ruiz Moreno
Morrison & Foerster
Sidley Austin LLP
Sullivan & Cromwell LLP
Weil, Gotshal & Manges LLP

GIR
Global Investigations Review
www.globalinvestigationsreview.com

The Investigations Review of the Americas 2018

A Global Investigations Review Special Report

The Investigations Review of the Americas 2018

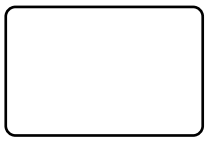
Senior co-publishing business development manager George Ingledew
Senior co-publishing manager Edward Perugia
edward.perugia@globalinvestigationsreview.com
Tel: +1 202 831 4658

Head of production Adam Myers
Editorial coordinator Iain Wilson
Chief subeditor Jonathan Allen
Production editor Caroline Herbert
Subeditor Simon Tyrie

Editor, Global Investigations Review David Vascott
Editor in chief David Samuels

Cover image credit: iStock.com/blackdovfx

Subscription details
To subscribe please contact:
Tel: +44 20 3780 4242
Fax: +44 20 7229 6910
subscriptions@globalinvestigationsreview.com



ISSN: 2056-6980

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

The Investigations Review of the Americas 2018

Published in association with:

Blake, Cassels & Graydon LLP

Campos Mello Advogados

D'Empaire Reyna Abogados

EY

Herbert Smith Freehills

Hogan Lovells

Kirkland & Ellis LLP

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

Miller & Chevalier Chartered

Mitrani Caballero Ojam & Ruiz Moreno

Morrison & Foerster

Sidley Austin LLP

Sullivan & Cromwell LLP

Weil, Gotshal & Manges LLP

Contents

Cross-border overviews

Enforcer overviews

Country chapters

Data privacy and transfers in cross-border investigations

John P Carlin, James M Koukios, David A Newman and Suhna N Pierce
Morrison & Foerster

The proliferation and expansion of different data protection regimes in jurisdictions around the world is making cross-border investigations increasingly challenging.

In particular, Department of Justice (DOJ) investigations of multinational companies for violations of the Foreign Corrupt Practices Act (FCPA), rate manipulation, US sanctions or export-control violations, or other cross-border economic crimes often require counsel representing the target company to assemble and review information from a web of complex corporate structures in different jurisdictions that implicate overlapping and at times inconsistent data privacy laws. In the course of such investigations, the DOJ will commonly request information about employees of the subject company – or about other third parties who have interacted with the subject company – that is housed in another jurisdiction. Moreover, the information requested may reside in emails sent or received by employees that work for affiliated entities in other countries. And, often, even when the subject company wishes to cooperate with the DOJ investigation, it may find itself constrained in its ability to divulge the requested information because of a non-US jurisdiction's laws, including data protection laws, employment laws, and laws that protect the secrecy of correspondence.

DOJ leadership has acknowledged this development while at the same time conveying a degree of scepticism towards companies' inability to disclose information on these grounds. In remarks given in March 2016, for example, the then-Assistant Attorney General in charge of the Criminal Division, Leslie Caldwell, noted that investigators were working to address 'myriad foreign data privacy regulations' in the course of investigating global white-collar criminal offences and suggested that in certain situations, 'non-cooperative companies make invalid assertions about particular data privacy laws in an effort to shield themselves from our investigations.'[1] In previous remarks, Caldwell had stated that the DOJ is 'looking closely – with an ever more sceptical eye – to ensure' that companies' invocations of data privacy laws as obstacles to sharing information are 'honest and not obstructionist.'[2]

Perhaps because of that scepticism, the DOJ has released guidance regarding cooperation in FCPA investigations – an area in which this issue commonly arises – which states that companies must specifically establish which data privacy laws actually prohibit transfers of requested information.[3] And companies are expected to 'work diligently to identify all available legal bases to provide' the requested information wherever possible.[4] (The DOJ has issued similar guidance in the context of export control and sanctions investigations.)[5]

In short, companies facing DOJ investigations cannot simply raise the spectre of 'foreign data privacy laws' to avoid requests to produce documents or other information – particularly if they wish to gain cooperation credit. At the same time, and as described below, many foreign laws do indeed impose onerous restrictions against the collection and transfer of personal information into the United States that must be analysed in connection with efforts to cooperate with a US investigation.

The proliferation of different data protection regimes

More than 100 countries around the world have data protection laws. Those laws all have common elements which require that individuals be afforded certain rights and that specific steps be taken before personal information can be collected and shared with third parties and outside of the country. The core principles are:

- Notice: individuals must be informed in advance about the types of personal information that a company will obtain, the ways in which a company will use that information, and to whom the company will disclose the information in order for the collection and use to be considered fair.
- Choice: a basic principle under privacy laws is that the individual at issue has a choice about whether or not his or her personal information is collected, used and shared (unless there is another valid legal basis for processing the information, as discussed below). An individual can agree to the collection of his or her personal information and specific uses and disclosures of it, if the individual has been provided sufficient information and the consent is voluntary.
- Limitations on sharing with third parties (including governments): having possession of personal information does not give a company licence to disclose the information to any third parties, or for any purposes, that it sees fit. The company can share the information with those recipients, and for those purposes, about which the individual has been informed, and it may need to execute a contract with the recipients to limit their use and further disclosure of the information.
- Limitations on cross-border transfers: privacy laws require special measures to transfer personal information outside the country's borders to recipients located in other jurisdictions that are regarded as having weaker privacy protections; such measures may include the individual's consent or an appropriate contract with the recipient.

European Union data privacy protections

The European Union and its member states impose strict data protection laws through a number of mechanisms, the first and foremost of which is Data Protection Directive 95/46 (the Directive). The Directive is designed to extend a high level of protection for all 'personal data,' which is defined to mean 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'

While member states are the bodies primarily responsible for enacting data protection laws, the Directive sets out several principles

that each member state is required to follow when implementing national legislation. One of those key obligations is making sure that there is a 'legal basis' or good reason to collect, use, or share personal information (which is generally referred to as 'processing' personal information). The following legal bases may potentially be used to justify an investigation:

- the processing is necessary for the company to comply with a legal obligation; this only refers to compliance with a European legal obligation and not to compliance with a US statute or regulation (but certain member states may have an obligation to comply with an order issued by a foreign court);
- the processing is necessary for the purposes of legitimate interests of the company or of a third party to whom the data are disclosed, except where the individual's interest in his or her fundamental rights and freedoms override those interests;
- the processing is necessary to perform a contract to which the individual is party (eg, the employment contract); or
- the individual has unambiguously consented to the processing.[6]

An even higher threshold applies where data concerns 'special categories', including data that reveal racial or ethnic origins, political opinions, religious or philosophical beliefs, health information, and trade union membership. Information relating to an individual's criminal history or to allegations of criminal activity is also considered to be sensitive data in EU countries. Under the Directive, a company that processes these types of information for purposes of an investigation can do so (i) if the processing is necessary to carry out specific obligations on the company under the member state's employment law; (ii) with the individual's explicit consent; or (iii) to establish, exercise or defend against a legal claim.[7]

Thus if a company needs to do an email review and the matter involves health information, the company may need to obtain explicit written consent from the individuals whose information is at issue, unless it is obligated to review this information under the employment law of the member state (which would be unlikely for a foreign company), or unless the review is necessary to establish, exercise, or defend a legal claim. The requirements to meet the condition of defending a legal claim may differ from one member state to another. For example, in the Netherlands there must be an actual legal proceeding in which the EU affiliate that controls the data is named as a party, and a voluntary disclosure to prevent a subpoena, investigation or legal proceeding will not constitute a valid basis. In contrast, in Italy the company can process sensitive personal information as part of an investigation (eg, into an employee's potentially criminal acts against the company) on the grounds of a legal claim that the company seeks to exercise or defend in the future.

In addition to having to have a legal basis for each act of processing, the Directive imposes restrictions against sharing personal information outside the European Economic Area (EEA). The European Commission (EC) has determined that a handful of countries provide 'adequate' levels of protection for personal data, which means data can be transferred on to those countries without additional mechanisms in place. But the United States has not been deemed to provide adequate protection to personal information. As such, organisations operating in an EEA country are constrained in their ability to transfer personal data into the United States (eg, by moving it to an affiliate or parent company that is based in the United States).

In the absence of an adequacy determination, there are effectively five mechanisms for transferring personal information from an EEA affiliate to a parent company in the United States:

- the US company has been certified to the US-EU Privacy Shield;
- the individual whom the data concerns has given his or her unambiguous consent;
- the transfer is necessary for the performance of a contract with, or concluded in the interests of, an individual;
- the European company and the US company have entered into a form agreement called the Standard Contractual Clauses that have been approved by the EC; or
- a group of affiliated companies have agreed to be bound by an approved set of binding corporate rules (BCRs), which has been approved by the EU data protection authorities.

Thus companies need to put in place a mechanism to share the information between the entity in the EU and the affiliated company in the US. Those mechanisms would not enable the EU entity or its US affiliate to share the information with the DOJ. A discrete mechanism would be needed to further share the information with the DOJ, such as obtaining the individual's consent to the disclosure.

As of 25 May 2018, the General Data Protection Regulation (GDPR) will take effect, replacing the Directive.[8] The GDPR contains data transfer restrictions that are equivalent to the Directive. The GDPR will apply directly in countries in the EEA, meaning there will be no need for those countries to implement the rules into their national legislation as has been the case for the Directive. Under the GDPR, some requirements will be more demanding than their counterparts under the Directive. For example, article 13 of the GDPR specifies a more extensive list of information that should be provided to the individuals regarding processing of their personal information than what is required under current law to comply with notice principles. Additionally, the GDPR will require companies to conduct 'data protection impact assessments' where processing 'is likely to result in a high risk' for the rights of individuals, having regard to the 'nature, scope, context and purposes of the processing'. It remains to be seen whether investigations would be considered a type of processing likely to result in high risk to the rights of individuals.

Additional development: UK data privacy restrictions in the shadow of 'Brexit'

If the UK were to leave the EU entirely under Brexit, it would no longer be subject to the GDPR. On 21 June 2017, however, as part of the Queen's Speech (which traditionally sets out the agenda for the next parliamentary year), the UK government announced plans for 'a new law' – namely, a new UK Data Protection Bill – that will 'ensure that the United Kingdom retains its world-class regime protecting personal data.'

The UK Data Protection Bill would serve as a successor to the UK's current Data Protection Act 1998. An accompanying document to the Queen's Speech describing the government's plans stated that the bill would create a new framework to balance users' and businesses' freedom and security online. The document further explained that the legislation's key features would include:

- making the UK's data protection framework suitable for the new digital age, allowing citizens to better control their data;
- implementing the EU General Data Protection Regulation (GDPR) in order to meet the UK's obligations while it is an EU member state and help put the UK in the best position to maintain its ability to share data with other EU member states and internationally, after it leaves the EU;
- modernising and updating the regime for data processing by law enforcement agencies, covering both domestic processing and cross-border transfers of personal data; and

- updating the powers and sanctions available to the UK's Information Commissioner.

While it remains possible that the Queen's Speech – which, of course, covers a broad array of topics beyond data protection – could get voted down or amended, it is generally not expected that the proposals regarding data protection will radically differ from those made in the Queen's Speech. The speech thus provides further confirmation that the UK will implement the GDPR in May 2018 (when the UK will still be an EU member state) and echoes the Information Commissioner's previous comments to the effect that the UK must seek to keep up with the EU data protection regime even after Brexit. That said, it remains to be seen how closely the proposed Data Protection Bill will track the requirements of the GDPR and so legislative developments in the coming year on this topic bear close watching.

Data protection regimes in Asia, Latin America and Africa

There is so much focus on Europe that companies often forget about some of the obligations in Asia, Latin America and Africa. The number of jurisdictions in these regions that have data privacy laws continues to increase. Such laws tend to have a number of common elements, including with respect to notice, choice, data security, the right of the individual to access and correct personal information relating to him or her, and data integrity and retention. In general – consistent with privacy regimes throughout the world – these laws require that individuals be told what personal information is collected, why it is collected, and with whom it is shared. The laws also require consent mechanisms, though they vary by country. Some countries in the Asia-Pacific region, such as South Korea and Hong Kong, require affirmative opt-in consent for at least some uses of data, while in other countries, such as New Zealand, there is less of an emphasis on consent. In Latin America, all relevant privacy laws include choice requirements, though some countries, such as Colombia, have a much stronger emphasis on affirmative consent than others.

Much like other privacy regimes, these laws also require organisations that collect, use and disclose personal information to take reasonable precautions to protect that information from loss, misuse, unauthorised access, disclosure, alteration and destruction. With respect to access and correction rights, however, many countries in Asia either do not specify specific time frames for honouring access or correction requests, or provide a manageable time frame similar to those found in European countries. By contrast, many Latin American privacy laws impose very short time frames for responding to access and correction requests. Finally, these privacy laws generally require that organisations that collect personal information ensure that their records are accurate, complete and kept up to date for the purposes for which the information will be used and also that they retain the personal information only for the period of time required to achieve the purpose of the processing.

With regard to cross-border transfers, a number of these countries restrict the transfer of personal information to countries that do not adequately protect personal information. In most cases in the Asia-Pacific region, however, data protection authorities have not provided guidance on what countries provide adequate protections; companies can mitigate uncertainty by implementing mechanisms such as contractual agreements to facilitate cross-border transfers without running afoul of these rules. By contrast, in the Latin American region, privacy laws rely more heavily on consent for cross-border transfers. In Africa and the Middle East, there are 18 countries, plus areas within the United Arab Emirates and Qatar, that have enacted comprehensive privacy laws, almost all of which include cross-border limitations. These laws do for the most part provide that a company can transfer data to another country if it is a contractual necessity (though not merely based on the legitimate interest of the company).

Beyond data protection regimes: employment and correspondence secrecy laws

Outside of the United States, several other types of laws may affect a company's ability to conduct an internal investigation in a given jurisdiction, most notably employment laws and correspondence secrecy laws. As with data protection laws, these laws have nuances in their formulation and interpretation so that the operative rules differ from country to country.

Many countries have laws protecting the secrecy of correspondence. This right may be established by a country's constitution or provided by the civil or criminal code or by telecommunications law. Such provisions guarantee the secrecy of closed correspondence and require consent of the parties to such a communication in order to access its contents. While originally envisioned to protect sealed letters, in many countries the secrecy of correspondence is held inviolable not only for written correspondence but also extends to telephone calls, emails and other electronic communications. Correspondence secrecy rules will typically become an issue if the company permits its employees to make incidental personal use of company computer systems. Where such personal use is allowed, there is potential for the company to access employees' private communications in the course of collecting and reviewing emails and other documents for the investigation. As a result, the collection and review generally can proceed only with the employee's informed consent, which may be withdrawn at any time.

Furthermore, employment laws in many countries regulate the manner and extent of control that an employer can exercise in relation to its workers. In the context of an internal investigation, a company is obligated, in some countries, to provide a specific notice to applicable employees to inform them about the pending investigation. This notice is in addition to any general privacy notice that the employer may have provided its employees. The specific notice must be provided to an employee under investigation informing him or her of the allegations or suspicions at issue and providing the employee an opportunity to address those allegations. Generally, the specific notice should be provided prior to any data collection, although some countries allow for delaying the notice until there is no longer a risk of the employee destroying evidence. Employment laws, in combination with data protection laws, also require a company to minimise the intrusion that an internal investigation has into employees' private affairs. Thus, where private correspondence is encountered during document review, it should be not be reviewed and should be disregarded, even if the employee has consented to the investigation accessing private correspondence. In some countries, it is recommended practice to give the employee the option to be present when his or her emails or other documents are being reviewed, so that the employee can indicate which ones are private in nature and should be discarded.

Additional development to watch: DOJ requests Supreme Court review of the Second Circuit's ruling in US v Microsoft

In the past year, one of the most closely watched issues with respect

to the scope of US privacy and data security law has been the enforceability of warrants issued pursuant to the Stored Communications Act (SCA), 18 USC section 2701 et seq., seeking data stored outside the United States. In *Microsoft v United States*, 829 F.3d 197 (2d. Cir. 2016), the US Court of Appeals for the Second Circuit considered a challenge from Microsoft to the enforceability of an SCA warrant seeking content information with respect to an email account stored by the Company in Dublin. Microsoft had moved to quash the warrant on the grounds that the SCA, and therefore the warrant, did not authorise a search and seizure outside of the territory of the United States.

In a closely watched ruling, the Second Circuit ultimately agreed with Microsoft. Whereas the US government had argued that the analysis should turn on the fact that Microsoft technicians sitting at their desks in the United States had the physical and technological capability to access the emails stored on servers outside of the United States, the Second Circuit disagreed, reasoning that, even if Microsoft accessed the emails from a US workstation, the actual seizure of the emails would occur on a server outside of the United States. The court went on to hold on statutory grounds that the SCA warrant cannot authorise such a seizure because the statute only permits searches and seizures that occur within the United States.

Since the *Microsoft* ruling came down, a number of lower courts in other circuits have reached a different result. For example, a federal magistrate judge in the Eastern District of Pennsylvania ruled for the Department of Justice and ordered Google, Inc to comply with two search warrants for foreign-stored user data. *In re Search Warrant*, No. 16-960-M-01 to Google (E.D. Pa. 3 February 2017). Then, a few months later, a federal judge in California declined to apply the reasoning of the *Microsoft* case in another SCA case involving Google. *In re Google*, No. 16-mc-80263-LB (N.D. Ca. 19 April 2017).

On 23 June, having unsuccessfully sought en banc review from the full Second Circuit, the DOJ took an important action in an effort to resolve the current uncertainties when it sought Supreme Court review of the Second Circuit's *Microsoft* decision. In the petition for certiorari, the acting solicitor general argued that the Second Circuit reached an 'unprecedented holding' that was grounded in the flawed premise that the production of information 'the provider can access domestically with the click of a computer mouse' nevertheless constitutes an extraterritorial application of the SCA. The Supreme Court is likely to act on the petition in the autumn of 2017, potentially paving the way for the issue to be resolved in the first half of 2018. Because the issue is one of statutory interpretation, there is also the possibility that it could ultimately be addressed through the passage of new legislation in Congress.

Conclusion

In light of the complex and often inconsistent data privacy frameworks that regulate multinational companies – along with the DOJ's repeated scepticism toward generalised refusals to comply with a US investigation on data privacy grounds – it is imperative that those conducting cross-border investigations have a firm grasp of the specific requirements applicable to their circumstances. A series of ongoing litigation matters and other events may result in significant changes to the landscape over the next year – including the outcome of the Privacy Shield litigation in the EU, the fate of the Second Circuit's *Microsoft* ruling in the Supreme Court, and the evolution of UK data privacy protection laws against the backdrop of Brexit. These developments bear close monitoring not only by attorneys principally engaged in data privacy work but also by those who counsel clients regarding cross-border investigations.

Notes

1 'Assistant Attorney General Leslie R Caldwell Speaks at American Bar Association's 30th Annual National Institute on White Collar Crime,' 4 March 2016, www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-american-bar-association-s-30th.

2 'Remarks by Assistant Attorney General for the Criminal Division Leslie R Caldwell at the 22nd Annual Ethics and Compliance Conference,' 1 October 2014, www.justice.gov/opa/speech/remarks-assistant-attorney-general-criminal-division-leslie-r-caldwell-22nd-annual-ethics.

3 US Dep't of Justice, 'The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance,' at 6, 5 April 2016, www.justice.gov/archives/opa/blog-entry/file/838386/download.

4 Id.

5 US Dep't of Justice, 'Guidance Regarding Voluntary Self-Disclosures, Cooperation, and Remediation in Export Control and Sanctions Investigations involving Business Organizations' at 6, 12 October 2016.

6 See Directive 95/46/EC article 7. Article 7 provides additional legal bases for processing personal information, but these are unlikely to be relevant to an investigation.

7 See Directive 95/46/EC article 8. Article 8 also provides further conditions for processing sensitive personal information, but these are unlikely to be useful for an investigation. Beyond the conditions for processing sensitive personal data provided by the Directive, member state data protection laws may specify additional grounds for collection and use of sensitive personal data, some of which may be relevant to investigations.

8 See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

John P Carlin
Morrison & Foerster

John P Carlin, chair of Morrison & Foerster's global risk and crisis management team, advises industry-leading organisations in sensitive cyber and other national security matters, white-collar investigations, and government enforcement actions. He has served as a top-level official in both Republican and Democratic administrations, most recently as Assistant Attorney General for National Security, the DOJ's highest-ranking national security lawyer. In this capacity, for which he was nominated by the President and overwhelmingly confirmed by the Senate on a bipartisan basis, John oversaw nearly 400 employees responsible for protecting the nation against terrorism, espionage, and cyber and other national security threats.

Prior to assuming his role in the NSD, he served as Chief of Staff and Senior Counsel to Robert S Mueller, III, former director of the FBI, where he helped lead the FBI's evolution to meet growing and changing national security threats, including cyber threats. John also held positions as National Coordinator of the DOJ's Computer Hacking and Intellectual Property Program and Assistant United States Attorney for the District of Columbia, where he prosecuted cyber, fraud, and public corruption matters, among others, trying more than 40 cases to verdict.

John has been featured or cited as a leading authority on cyber and economic espionage matters by numerous major media outlets, including *The New York Times*, *The Washington Post*, *The Wall Street Journal*, *The Los Angeles Times*, *USA Today*, CBS's *60 Minutes*, NBC's *Meet the Press*, PBS's *Charlie Rose* and *Newshour*, ABC's *Nightline* and *Good Morning America*, NPR, CNN, and *Vanity Fair*, among others.

James M Koukios
Morrison & Foerster

James M Koukios is an experienced trial attorney and focuses his practice on white-collar crime and related matters, including internal corporate investigations and government enforcement actions. He has tried over 20 federal jury cases, including two landmark FCPA-related trials, *United States v Esquenazi* and *United States v Duperval*. For his work on these matters, he received the Assistant Attorney General's Distinguished Service Award. James was also a lead prosecutor in the defence procurement fraud case that served as the basis for the 2016 film *War Dogs*, and was featured on a 2017 episode of CNBC's *American Greed* to discuss the high-profile prosecution of Efraim Diveroli and his company AEY Inc.

Prior to joining Morrison & Foerster, James served as the Senior Deputy Chief of the Fraud Section in the Criminal Division of the DOJ. In that role, he supervised investigations, prosecutions and resolutions in the Fraud Section's FCPA, Health Care Fraud, and Securities and Financial Fraud Units. He was also a key contributor in drafting the DOJ and SEC joint publication, *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, which followed a series of consultations with business and compliance leaders.

Along with his role as Senior Deputy Chief, James has also held numerous government positions, including Assistant Chief in the Fraud Section's FCPA Unit, Special Counsel to former FBI Director Robert S Mueller, III, and as an Assistant US Attorney in the Southern District of Florida.

David A Newman
Morrison & Foerster

David A Newman represents clients in a wide variety of national security and global risk and crisis management issues. He has extensive experience in national security law, crisis management, and government regulation.

Prior to joining Morrison & Foerster, David held several key posts at the White House, serving as Special Assistant and Associate Counsel to President Barack Obama and on the staff of the National Security Council. Throughout his tenure at the White House, David played a central role in coordinating the Administration's responses to domestic and international crises. He regularly advised the President and other senior administration officials on a range of complex matters affecting the federal government, overseeing a broad portfolio that spanned national security priorities, crisis response and preparedness planning, new data and technology initiatives, criminal justice reform, and civil rights litigation.

Previously, David was counsel to the Assistant Attorney General for National Security at the DOJ, where he helped manage the DOJ National Security Division and counselled senior officials at DOJ and across the government on a wide array of matters – from high-profile terrorism investigations and litigation involving government surveillance programmes to reviews of data privacy policies and matters before the Committee on Foreign Investment in the United States. David also regularly coordinated White House briefings and responses to congressional inquiries involving sensitive national security programmes and worked closely with the Intelligence Community and the US military to support counterterrorism operations.

Suhna N Pierce
Morrison & Foerster

Suhna N Pierce has a rare combination of technical and legal competency. With extensive experience in the information technology industry providing infrastructure engineering and support services, she has deep knowledge of the technologies and processes used in enterprise settings. As an attorney, Suhna brings practical insight into the data security matters that the firm's clients handle on a daily basis. She has worked with companies responding to regulatory inquiries regarding their privacy and data security practices, including Federal Trade Commission investigations following data security incidents.

Suhna also advises clients on complying with US and foreign privacy and data protection laws. She has helped clients develop

privacy policies for website visitors and privacy notices for employees and customers; establish contracts relating to cross-border data transfer and protection obligations; and carry out registrations with data protection regulators. She has assisted clients with completing multi-jurisdictional surveys of privacy obligations, such as comparing different countries' requirements for marketing communications. Ms Pierce also has experience advising clients on privacy issues related to Foreign Corrupt Practices Act compliance programmes.

Prior to her legal career, she worked as an IT systems engineer in a variety of environments, including Fortune 500 corporations, an IT consulting company, and a not-for-profit organisation.

Morrison & Foerster (SF Office: HQ)
425 Market Street
San Francisco, CA 94105-2482

Morrison & Foerster (DC Office: Carlin, Koukios)
2000 Pennsylvania Avenue, Northwest
Washington, DC 20006-1888

Morrison & Foerster (NY Office: Carlin, Newman, Pierce)
250 West 55th Street
New York, NY 10019-9601

Tel: +1 415 268 7000

John P Carlin
jcarlin@mofo.com

James M Koukios
jkoukios@mofo.com

David A Newman
dnewman@mofo.com

Suhna N Pierce
spierce@mofo.com

www.mofo.com

With a team comprised of former federal prosecutors and regulators, veteran defence lawyers and seasoned foreign counsel, Morrison & Foerster has significant experience handling investigations and compliance matters on six continents and in more than 65 countries worldwide. Our investigations team understands how regulators think and can anticipate their next move. We approach each engagement from the client's perspective, drawing on our collective experience to offer practical advice that balances risk with the reality of running a business. Our clients frequently seek our advice on the many US and foreign laws regulating international business transactions including the FCPA, UK Bribery Act, Sarbanes-Oxley, the whistleblower provisions of the Dodd-Frank Act, international trade, export control and sanctions laws, anti-money laundering laws, and the Bank Secrecy Act, among others.

Our privacy and data security team, which consists of more than 60 experienced lawyers across the US, Europe and Asia, provides seamless, integrated service and is familiar with the data protection laws in every jurisdiction in which they exist. Our team includes locally qualified lawyers who are not only well-versed in international privacy laws, but also in interactions with the relevant data protection authorities. Because of our vast experience in international privacy and data security compliance, we are uniquely suited to help global organisations respond to global data security breaches and investigations, and have represented multinational clients in numerous investigations relating to data protection authority inquiries in Japan, Hong Kong, South Korea, France, Germany, the UK, Ireland, the Netherlands, Luxembourg, Canada, Australia and Russia, as well as authorities in the United States including the Federal Trade Commission and state attorneys general.

Strategic Research Sponsor of the
ABA Section of International Law

Law
Business
Research

ISSN 2056-6980