JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 6 | May 2015

JONES DAY

Jones Day Attorney Spotlight: Dan McLoon

Businesses and organizations worldwide are facing a growing array of domestic and international laws and regulations that apply to the collection, use, and transfer of consumer and employee information; aggressive investigation and enforcement by regulators and data protection authorities; and private litigation over the use of information. In an effort to best assist clients with these issues, Jones Day has concentrated its longstanding interdisciplinary team of privacy and cybersecurity authorities into a formalized Cybersecurity, Privacy, & Data Protection Practice.

Dan McLoon, a partner based in Los Angeles, will lead the Cybersecurity, Privacy, & Data Protection Practice. Dan brings extensive trial and appellate experience to the practice, as well as more than 30 years of knowledge handling complex commercial litigation issues, data breaches, cybersecurity investigations, product liability cases, contract disputes, and accounting matters. He also has advised multiple companies on data security and consumer privacy compliance in both public and nonpublic matters. Dan looks forward to leading a dynamic practice group that advises clients on

EDITORIAL CONTACTS

Daniel J. McLoon, Los Angeles
Undine von Diemar, Munich
Mauricio Paez, New York
Jonathon Little, London
Kevin Lyles, Columbus
Paloma Bru, Madrid
Jay Johnson, Dallas
Olivier Haas, Paris
Adam Salter, Sydney
Anita Leung, Hong Kong

Editor-in-Chief: Anand Varadarajan

Practice Directory

HOT TOPICS IN THIS ISSUE

cutting-edge cybersecurity, data protection, and privacy issues in multiple jurisdictions around the world.

United States

Regulatory—Policy, Best Practices, and Standards

GAO Identifies Cybersecurity Challenges for Federal Government
On February 11, the U.S. Government Accountability Office ("GAO") released its biennial High Risk List, which is "intended to help inform the oversight agenda for the 114th Congress and to guide efforts of the administration and agencies to improve government performance and reduce waste and risks." In its report, the GAO suggested amending privacy laws to cover all "personally identifiable information collected, used and maintained by the federal government" and recommended that federal agencies improve their responses to data breaches involving personally identifiable information.

Insurance Group Publishes Global Cyber Governance Report
On April 27, the Zurich Insurance Group and the ESADEgeo-Center for Global Economy and Geopolitics jointly published a report on global cyber governance. According to the accompanying executive summary, "ideological differences and geopolitical tensions preclude strong and effective global governance institutions; and the current governance framework does not adequately reflect the global nature of cyberspace." The report calls for the private sector and policymakers to establish an effective global cyber governance framework, including a cyber alert system styled after the World Health Organization.

NIST Requests Public Comments on Framework for Big Data
On April 6, the National Institute of Standards and Technology ("NIST") published a draft Big Data Interoperability Framework that facilitates scientists' use of big data sets. The Framework was drafted by NIST's Big Data Public Working Group, which developed big data definitions, taxonomies, important requirements for privacy and security protections, a standard road map, and a proposed reference architecture. NIST requested comments on the draft by May 21.

NIST Seeks Comments on Potential Update to Electronic Authentication Guideline
On April 9, NIST requested public comments on whether it should update its Electronic Authentication Guideline published in August 2013. NIST released a statement indicating that an update to the guidelines may be necessary due to market innovation, changing federal requirements, and the current threat landscape, which increasingly targets remote authentication. Comments are due by May 22, 2015.

Regulatory—Retail

Major Retailers Report Millions in Expenses Relating to Data Breaches
In late February, two major retailers reported millions of dollars in gross expenses stemming from recent data breaches on their Form 8-K filings submitted with the Securities and Exchange Commission. One retailer claimed $252M in costs after hackers stole payment card data and personal information from shoppers, while the other retailer disclosed that it spent $33M responding to a data breach that compromised more than 50M payment cards.

Industry Group Expresses Concerns Regarding Privacy Bill of Rights
On February 26, the Direct Marketing Association, a large trade association focused on advancing and protecting data-driven marketing, sent a letter to the Secretary of Commerce that warned that President Obama's "privacy bill of rights" for U.S. consumers may "restrict legitimate business practices, undermine economic and job growth, and thwart innovation." On the following day, President Obama released a discussion draft of the Consumer Privacy Bill of Rights Act that is intended to "establish baseline protections

for individual privacy in the commercial arena."

Retail Industry Group Testifies Before House Committee on Cybersecurity
On March 18, the Senior Vice President of the National Retail Federation testified before the House Committee on Oversight and Government Reform. He called for policymakers to implement solutions to cybersecurity threats beyond information-sharing, including federal fraud protection for debit cards, a national data breach notification law, and more secure payment cards through pin-and-chip technology, adoption of end-to-end encryption, and competitive tokenization standards.

Payment Card Security Council Releases Updated Standards
On April 10, the Payment Card Industry Security Standards Council ("PCI SSC") issued an updated payment card production standard that will help better secure payment cards. The updated requirements secure the card production process from design through delivery and address various card production activities, including card manufacturing, chip embedding, data preparation, pre-personalization and card personalization, fulfillment, packaging, storage, and electronic PIN distribution. On April 15, the PCI SSC also published Version 3.1 of its data security standard, which addresses vulnerabilities within the Secure Sockets Layer encryption protocol that can put payment data at risk.

Regulatory—Defense, National Security, and Economic Espionage

Third Circuit Interprets "Authorization" Under Computer Fraud and Abuse Act
On February 5, the Third Circuit Court of Appeals affirmed the district court's grant of summary judgment in favor of a defendant that had been sued by a competitor for allegedly accessing the competitor's computer systems without authorization to download copyrighted materials in violation of the Computer Fraud and Abuse Act ("CFAA"). Because the defendant downloaded only publicly available materials and created trial accounts to the plaintiff's computer services, the court held that the defendant did not act without authorization within the meaning of the CFAA.

Grand Jury Indicts Individuals for Hacking Competitor's Computer System
On February 10, a federal grand jury in California indicted five individuals for violating the CFAA by hacking into a competitor's website. The indictment alleged that one of the defendants hired private investigators to monitor the activities of a competing company, and those private investigators in turn hired two hackers to infiltrate into the competitor's computer system.

Technology Companies Commit to Adopting Cybersecurity Framework Following White House Summit
On February 13, the White House issued a press statement in conjunction with its Summit on Cybersecurity and Consumer Protection at Stanford University. The White House confirmed that a number of companies committed to using the NIST Cybersecurity Framework.

Director of National Intelligence Testifies on Cyber Threats Facing America
On February 26, the Director of National Intelligence, testified before the Senate Armed Services Committee that cyber threats are "increasing in frequency, scale, sophistication and severity of impact." He identified "destructive cyber attacks carried out on US soil by nation state entities" and remarked that "economic espionage against US companies remains a major threat."

Director of FBI Discusses Cyber Threats In Budget Presentation
On March 12, the Director of the Federal Bureau of Investigation ("FBI") discussed cyber-based threats posed by "state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists" during his 2016 budget presentation before the Senate Appropriations Committee. The Director noted that the number of FBI investigations related to computer intrusions has increased by 80 percent since 2002, and that to counter this threat, the FBI requested a $10M budget increase to support its cyber efforts.

Privacy Watchdog Seeks Public Comment on U.S. Intelligence Surveillance Programs
On March 23, the Privacy and Civil Liberties Oversight Board issued a request for public comment on the privacy and civil liberties implications of the federal government's counterterrorism activities, including the government's internet surveillance and bulk telephone record collection activities.

President Obama Announces New Sanctions Program for Malicious Cyber Actors
On April 1, President Obama issued Executive Order 13964, in which he declared a national emergency relating to foreign "malicious cyber-enabled activities." The Order authorizes the Treasury to freeze the assets of malicious cyber actors, including those who harm or significantly compromise critical infrastructure and other major computer networks or cause significant "misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information."

Secretary of Homeland Security Discusses Cyber Cooperation with China's Minister of Public Security
On April 9, the Secretary of the Department of Homeland Security ("DHS") met with China's Minister of Public Security, Guo Shengkun, in an effort to increase law enforcement cooperation between the United States and China. The two agreed to increase information-sharing between the two countries in an effort to combat intellectual property theft and focus on "cross-border, cyber-enabled crime."

Department of Homeland Security Outlines Cybersecurity Efforts
On April 15, the National Protection and Programs Directorate ("NPPD")—a division of DHS—released written testimony for the Senate Committee on Appropriations regarding the NPPD's ongoing efforts to secure the nation's cyber-infrastructure. The testimony covered (i) EINSTEIN 3 Accelerated, which is a perimeter defense tool installed at certain ISPs to detect and block known cyber threats from affecting federal civilian personnel; (ii) risk assessments for critical infrastructure entities; and (iii) the National Cybersecurity & Communications Integration Center's efforts to share information and coordinate responses to cyber incidents.

Second Circuit Rules NSA's Bulk Data Collection Program Illegal
On May 7, the Court of Appeals for the Second Circuit ruled that the National Security Agency's ("NSA") bulk data collection program exceeded the scope of Congress's authorization in Section 215 of the Foreign Intelligence Surveillance Act of 1978. The court did not decide whether the NSA's program is constitutional.

Regulatory—Financial Services

NY Department Issues Update on Cybersecurity in the Banking Sector
On April 8, the New York State Department of Financial Services issued an Update on Cyber Security in the Banking Sector: Third Party Services Providers, which follows the Department's May 2014 report on Cyber Security in the Banking Sector. The Update surveys banking institutions' processes, policies, and procedures for assessing and safeguarding against the cybersecurity risks posed by third-party service providers. According to the Update, "banking organizations appear to be working to address the cybersecurity risks posed by third-party service providers, although progress varies depending on the size and type of institution."

Financial Lobbyists Speak Against Sunset Provisions of Cybersecurity Bills
On April 22, the Financial Services Roundtable ("FSR"), an advocacy organization representing leading financial service providers, published a statement against the inclusion of sunset provisions in the information-sharing cybersecurity bills currently being considered in Congress. FSR touted the proposed legislation as "provid[ing] a set of legal tools that will greatly enhance our nation's ability to battle cybercriminals."

Regulatory—Transportation

GAO Finds Significant Weaknesses in FAA's Cybersecurity Practices
On March 2, the Government Accountability Office ("GAO") publicly released a report to Congress entitled FAA Needs to Address Weaknesses in Air Traffic Control Systems. After assessing the Federal Aviation Administration's ("FAA") cybersecurity practices, the GAO found that despite steps taken to safeguard air traffic control systems, "significant security control weaknesses" threatened the FAA's ability ensure the "safe and uninterrupted operation of the nation's air traffic control system[.]"

Regulatory—Energy/Utilities

ICS-CERT Finds Energy Sector Reported Most Cyber Incidents in 2014
On March 13, the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT"), which works to reduce risks within and across all critical infrastructure sectors, reported that it received and responded to 245 incidents in FY 2014. ICS-CERT found that 32 percent of these incidents occurred in the energy sector, the highest percentage of any critical infrastructure sector, and approximately 55 percent of the incidents involved advanced persistent threats or sophisticated actors.

Regulatory—Health Care/HIPAA

DHHS Issues Guidance to Employers on HIPAA's Application to Workplace Wellness Programs
On April 16, the U.S. Department of Health and Human Services ("DHHS") issued a two-part informal guidance regarding the application of the Health Insurance Portability and Accountability Act ("HIPAA") to workplace wellness programs.

Litigation, Judicial Rulings, and Agency Enforcements

N.D. Cal. Court Holds Video Streaming Company Did Not Violate the VPPA
On March 31, a Northern District of California court dismissed a class action suit filed against a video streaming service, which alleged that the company violated the Video Privacy Protection Act ("VPPA") by allowing users' video history to be viewable on a social media platform. The court held that the video streaming service did not "knowingly" provide the social media company with users' video history, as required to prove a violation of the VPPA.

N.J. District Court Dismisses Data Breach Lawsuit Against Insurance Company
On March 31, a New Jersey District Court dismissed a putative class action against an insurance company, which stemmed from the theft of company laptops containing personal health information of the company's members. The court held that the plaintiffs lacked standing and failed to sufficiently allege economic harm, noting that an increased risk of identity theft due to a security breach is not sufficient to grant standing under Article III.

Consumers File Class Action for Privacy Violations Stemming from Facial Recognition Software
On April 1, a class action lawsuit was filed against a social media company for violating an Illinois statute regarding the collection and use of biometric data. The suit alleges that the social media company's tagging feature uses facial recognition software that collects biometric data and that the company does not meet the statutory requirements for informed consent for collection of this data. Plaintiff seeks to certify a class of all Illinois users whose biometric information was collected through the use of this facial recognition software.

FTC Announces Settlement with Companies Falsely Claiming Safe Harbor Compliance

On April 13, the Federal Trade Commission ("FTC") announced that two companies agreed to settle charges that they falsely claimed to be in compliance with the requirements of the U.S.-EU Safe Harbor Framework and U.S.-Swiss Safe Harbor Framework (source document continued). According to the complaints, the companies' websites falsely stated that they were certified under the two frameworks, and one of the companies also allegedly deceived customers about its dispute resolution procedures and its participation in the TRUSTe Privacy program.

California District Court Finds Professional Networking Site Not a Consumer Reporting Agency
On April 14, a Northern District of California court dismissed a class action against a professional networking website, holding that the site's search service was not a "consumer report" under the Fair Credit Reporting Act ("FCRA"). The plaintiffs argued that the site's reference search service, which provided prospective employers with the names of people who might know a candidate, constituted a "consumer report" under the FCRA. The court rejected these arguments, stating that the website is not a "consumer reporting agency under the FCRA," and that the reference search results themselves did not provide information about the candidate that rose to the level of a consumer report.

FTC Announces Settlement with Debt Brokers Over Information Disclosure
On April 21, the FTC announced that two debt brokers agreed to settle charges that they posted sensitive consumer information online in unencrypted documents that were accessible to anyone with an internet connection. The information posted by the data brokers without the consumer's knowledge or consent included the consumer's name, birth date, geographic location, email address, bank account and routing number, and driver's license.

Legislative—Federal

FTC Offers Testimony on Proposed Data Security Legislation
On March 18, the FTC Consumer Protection Director testified before the House Energy and Commerce Committee on proposed data security legislation. She testified that the FTC supports the bill's provisions requiring reasonable data security standards for companies, consumer notification of data breaches, and FTC penalties and enforcement against common carriers and nonprofits. However, she criticized the bill's narrow definition of "protected personal information," the failure to address connected device functionality, and the omission of rulemaking authority under the Administrative Procedure Act.

House Committee Holds Hearing and Releases Draft Changes to FERPA
On February 12, the House Education and Workforce Committee conducted a hearing on improvement of existing federal student privacy law. The committee heard testimony from industry, academics, advocacy, and school practitioners on how Congress should update the 1974 Family Educational Rights and Privacy Act ("FERPA"). On April 6, the Education and Workforce Committee issued a discussion draft of the proposed amendments to FERPA, which included revisions to the definition of a student's "educational record" and a ban on using such information for marketing or advertising.

President Signs Cybersecurity Threat-Sharing Executive Order
On February 13, at the White House's Summit on Cybersecurity and Consumer Protection, President Obama signed an executive order boosting cybersecurity information-sharing efforts between the private sector and the federal government. The new executive order urges companies in the private sector to create Information Sharing and Analysis Organizations ("ISAOs") for data exchange and collaboration across regions or in response to a specific emerging cybersecurity threat. DHS is responsible for developing a common set of voluntary standards for ISAOs, and lawmakers and representatives from DHS weighed the merits of the President's executive order at a February 25 hearing.

President Issues Consumer Privacy Bill of Rights Discussion Draft
On February 27, President Obama released a discussion draft of the Consumer Privacy Bill

of Rights Act. The bill develops baseline protections for individual privacy in the commercial context and promotes implementation of privacy protections through codes of conduct developed by stakeholders in various industries and enforced by the FTC.

House Committee Approves Data Security and Breach Notification Act
On March 12, Energy and Commerce Committee Vice Chairman Marsha Blackburn (R-TN) and Representative Peter Welch (D-VT) unveiled the Data Security and Breach Notification Act. The bill requires a wide range of entities that collect and maintain consumers' personal information to secure that data and provide notice within 30 days of determining the scope of a breach and restoring their systems. The Energy and Commerce Committee voted to advance an amended version of the bill on April 14.

FCC Working Group Issues Cybersecurity Measures for Communications Sector
On March 18, the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council's Working Group 4 ("WG4") issued its Cybersecurity Risk Management and Best Practices Working Group 4: Final Report. The WG4, which consists of members of the communications sector, was established to help communications providers implement the Cybersecurity Framework released by NIST. The group's Final Report contains the first-ever cybersecurity measures for the communications industry, and it includes separate reports tailored to five segments of the industry: broadcast, cable, satellite, wireless, and wireline services.

House Passes Bill to Amend Gramm-Leach-Bliley Act Annual Privacy Notice Requirement
On April 13, the House passed a bill to relieve the Gramm-Leach-Bliley Act requirement that financial institutions send customers annual privacy notices explaining information-sharing practices when the bank's privacy policy remains the same. The bill seeks to eliminate confusion among bank customers and reduce costs for financial institutions. The Senate received the legislation on April 14 and referred it to the Committee on Banking, Housing, and Urban Affairs.

Congressional Committees Approve Various Cyber Threat Information-Sharing Measures
On April 13, the House Intelligence Committee recommended passing the Protecting Cyber Networks Act (H.R. 1560), a bill authorizing corporate cyber threat information-sharing. The Committee reported that the bill "enables private companies to monitor their networks and voluntarily share cyber threat indicators with one another and with the federal government, all while providing strong protections for privacy and civil liberties." On April 15, the Senate Intelligence Committee issued its report approving the Cybersecurity Information Sharing Act of 2015 (S. 754). The Committee reported that the bill "provides positive legal authority" for private companies to monitor and defend their networks and customer-authorized networks for cybersecurity purposes, and to share information with other companies and the government. In addition, the bill "creates narrowly tailored liability protection to incentivize companies' efforts to identify cybersecurity threats and share information about them." On April 17, the House Homeland Security Committee recommended adopting the National Cybersecurity Protection Advancement Act of 2015 (H.R. 1731), which authorizes and "provides liability protections for private entities that conduct network awareness or voluntar[ily] sha[r]e cyber threat information with [] another private entity or the [National Cybersecurity and Communications Integration Center]."

Legislative—States

Connecticut Attorney General Announces Formation of Privacy and Data Security Department
On March 11, the Connecticut Attorney General announced the formation of a permanent Privacy and Data Security Department within his office. The specialized department follows on the heels of a Privacy Task Force appointed by the Attorney General in 2011 and is intended to "continue and expand upon the Task Force's work by dedicating staff to

work exclusively on privacy-related matters."

State Attorneys General Focus on Privacy and Data Security at Annual Meeting for Southern Region
From March 12 through 13, state attorneys general for the Southern Region of the National Association of Attorneys General ("NAAG") held their 2015 NAAG Southern Region Meeting in Point Clear, Alabama. The meeting was titled "The Surge in Data Breaches: Challenges for Attorneys General" and focused on data security issues with panels such as "Anatomy of a Data Breach" and "Big Data and Privacy—Striking a Balance."

Maryland Legislature Passes Bill to Establish Cybersecurity Council
On April 13, the Maryland Legislature passed legislation creating the Maryland Cybersecurity Council. The Council, comprising various public and private officials, will work with federal agencies, private businesses, and experts to assess cybersecurity risks in the state and to support the adoption and implementation of cybersecurity standards and technologies.

Connecticut to Study Cybersecurity Issues Facing the State
On April 16, the Connecticut General Assembly approved legislation that directs the Department of Administrative Services and the Department of Emergency Services and Public Protection to conduct a study examining cybersecurity issues facing the state.

Texas House Seeks to Criminalize Computer System Breaches
On April 17, the Texas House passed a law making it a felony to breach a computer system owned by the government or a commercial entity. In order to violate the provision, a person would have to act with the intent to obtain or use a file, data, or proprietary information stored in the system to defraud another individual or damage property.

Four States Amend Data Breach Notification Statutes
Montana, Wyoming, North Dakota, and Washington all recently passed laws amending various aspects of their respective data breach notification laws. On February 27, Montana altered its data breach statute to require breach notification to the Montana attorney general. The change also broadens the definition of "personal information" to include medical record information, taxpayer identification numbers, and identity protection personal identification numbers. On March 2, Wyoming amended its data breach statute to require owners or licensors of personal information to provide "clear and conspicuous" notice of a data breach to consumers and to expand the definition of "personally identifying information" to include unique biometric data or individual taxpayer identification numbers. On April 13, the North Dakota governor signed into law an amendment stating that any individual or business that owns or licenses computerized personal information must disclose a breach of its security system to the North Dakota attorney general if more than 250 individuals are affected. On April 23, Washington's governor signed into law several amendments to Washington's data breach notification law, including mandatory notification to the state attorney general when 500 residents are affected, a 45-day deadline for notification, updated content requirements for notifications, and a safe harbor for personal information that is adequately secured.

[Return to Top]

Canada

Regulator Issues First Fine Under Canada's Anti-Spam Legislation
On March 5, Canada's federal spam regulator, the Radio-television and Telecommunications Commission, imposed the first fine under Canada's Anti-Spam Legislation. The C$1.1M (US$880,000) penalty was levied on a Quebec City-based training marketer, which allegedly sent commercial electronic messages without the

recipient's consent and without a functioning unsubscribe mechanism.

Canadian Privacy Commissioner Finds Privacy Act Violation by Federal Department
On March 16, the Office of the Privacy Commissioner of Canada ruled that a federal department responsible for helping Canadians maintain and improve their health violated federal privacy law by disclosing the names of participants in a program that provided access to medical marijuana.

British Columbian Privacy Commissioner Rules Canadian Municipality Violated Employee Privacy
On March 30, British Columbia's Information and Privacy Commissioner released an investigative report finding that a municipality should disable some features of its employee monitoring software, which allowed the employer to log keystrokes, obtain automated screenshots, and continuously track computer program activity, because the usage violated the privacy rights of employees under the provincial Freedom of Information and Privacy Protection Act. The report also recommended that the municipality destroy all data collected by the software.

Canadian Privacy Commissioner Rules Advertising Campaign Raises Privacy Concerns
On April 7, the Office of the Privacy Commissioner of Canada released a report finding that a large telecommunications company had violated the Personal Information Protection and Electronic Documents Act when it tracked its customers' browsing habits, application usage, and television viewing and calling patterns as part of a relevant advertising program without consent. According to the Office of the Privacy Commissioner of Canada, the company subsequently withdrew the targeted advertising campaign.

Canada Becomes Member of APEC Privacy Rules Initiative
On April 15, the Asia-Pacific Economic Cooperation's ("APEC") Electronic Commerce Steering Group announced that Canada was accepted as the fourth member of the APEC's Cross-Border Privacy Rules System, joining the U.S., Mexico, and Japan. The privacy regime is designed to boost the protection of consumer data from security threats as data is transmitted around the Asia-Pacific region while cutting compliance costs for businesses.

The following Jones Day attorneys contributed to the United States and Canada sections: Steven Gersten, Jay Johnson, Sam Lam, Colin Leary, Gabriel Ledeen, Tyson Lies, Chiji Offor, Mauricio Paez, Nicole Perry, Scott Poteet, Jessica Sawyer, and Anand Varadarajan.

[Return to Top]

Latin America

Argentina

New Sanctions Regulation for Do Not Call Registry Law
On February 19, the Argentinean Data Protection Authority ("DPA") enacted a new sanctions regulation (source document in Spanish) implementing fines for the recently approved Do Not Call Registry Law (source document in Spanish). The new sanctions schedule ranges from 1,000 Argentinean pesos to 100,000 Argentinean pesos (US$100–$11,500) depending on the severity of the violation. Actions drawing higher penalties include (i) failure to renew the annual registration of a personal database at the DPA; (ii) processing personal information without the DPA registration; and (iii) disregarding the Do Not Call Registry in a marketing campaign.

Argentina Creates New Closed-Circuit Television Regulations
On February 24, the Argentinean DPA enacted a new closed-circuit television ("CCTV")

regulation (source document in Spanish) addressing the public and private use of video cameras for video surveillance. The regulation requires notice and consent provisions and public disclosure of data protection rights. In addition, the regulation mandates that the collection of personal data by CCTV cannot be inconsistent with the purposes for which the data was initially collected.

Brazil

Right To Be Forgotten Bill Awaits Legislative Review
On March 12, the Consumer Defense Commission finalized its draft Right To Be Forgotten bill (source document in Portuguese), which would require search engines to remove links to outdated or irrelevant information after the request of a citizen. The House of Representatives and Senate must pass the proposed legislation, and the President must approve the bill before it becomes official.

Ministry of Justice Extends Public Debates on Internet Civil Framework and Draft Data Protection Bill
On March 31, the Brazilian Ministry of Justice extended the term of the public debate on the regulations governing the Internet Civil Framework until April 30 (source document in Portuguese). Topics requiring further clarification include exceptions to the network neutrality principle, retention of logs by connection providers and service providers, and online privacy. Similarly, public debate on the draft data protection law (source document in Portuguese and English) has also been extended until April 30.

Honduras

Institute for Access of Public Information Promotes Draft Bill for Protection of Confidential Data
On March 3, the Institute for Access to Public Information ("IAIP") began a public consultation (source document in Spanish) on draft legislation covering the protection of confidential data in Honduras. The IAIP sought technical insights from international experts, government sectors, private companies, academics, and civilians to strengthen the draft bill and promote its importance. The draft bill will be submitted to the National Congress of Honduras in the coming months.

Mexico

Executive Branch to Publish New Transparency Law
On April 16, the Mexican House of Representatives approved the General Law on Transparency and Access to Public Information (source document in Spanish) and submitted it to the Executive Branch for official publication in Mexico's Federal Official Gazette. In addition to setting the rules for the National System for Transparency, Information Access, and Personal Data Protection, the new legislation imposes transparency obligations on political parties, public trusts and funds, and entities managing public funds.

Paraguay

House of Representatives Rejects Bill to Retain Personal Data
On March 12, the Paraguayan House of Representatives rejected the internet traffic data retention bill (source document in Spanish) known as Pyrawebs. The Pyrawebs bill would have required internet service providers to store internet traffic data for one year in databases accessible to authorities for criminal investigation purposes. The Paraguayan Senate has 120 days to reexamine the legislation.

Peru

Peruvian Data Protection Authority Hosts XIII Ibero-American Congress on Data Protection
On May 6–8, the Peruvian National Authority on Personal Data Protection hosted the XIII Ibero-American Congress on Data Protection (source document in Spanish), which included the participation of data protection authorities, academics, and experts from all over Latin America. Topics included the privacy of minors, data protection in health services, privacy in the workplace, criminal activity on privacy matters, and credit bureaus.

The following Jones Day attorneys contributed to the Latin America section: Guillermo Larrea and Virginia Uelze.

[Return to Top]

Europe, Middle East, and Africa

European Union

UN Human Rights Councils Creates Special Rapporteur to Investigate and Report on Privacy Rights
On March 24, the United Nations Human Rights Council passed a landmark resolution appointing a Special Rapporteur on the right to privacy for an initial period of three years. The resolution, spearheaded by Brazil and Germany, directs the Special Rapporteur "to gather relevant information, including on international and national frameworks, national practices and experience, to study trends, developments and challenges in relation to the right to privacy and to make recommendations to ensure its promotion and protection[.]" The Special Rapporteur is expected to be appointed in June.

Global Privacy Enforcement Network Releases 2014 Annual Report
On April 1, the Global Privacy Enforcement Network released its first annual report showing increased size and participation in the network. Specific developments include: substantial enhancements to the online cooperation platform; new network members from Africa, Asia, and Latin America; successful teleconferences in the Atlantic and Pacific regions; and a major cooperative sweep of the privacy practices of more than 1,200 apps.

European Court of Justice

ECJ Hears Arguments in Safe Harbor Case
On March 24, the European Court of Justice ("ECJ") held an oral hearing in *Schrems v. Data Protection Commissioner*. The case involves a privacy activist challenging the Irish Data Protection Commissioner's decision not to investigate claims about improper data transfers to the U.S. by a social media website. Referred to the ECJ by the High Court of Ireland, the case raises questions of whether a national data protection authority is bound by the Commission's prior Safe Harbor decision or whether the national authority must investigate the data practices of the third country. An opinion is expected in June.

Article 29 Working Party

Article 29 Working Party Releases Cookie Sweep Combined Analysis Report
On February 3, the Article 29 Working Party published the Cookie Sweep Combined Analysis Report, which presents the consolidated analyses of privacy and telecommunications authorities in Denmark, Slovenia, France, Greece, the Netherlands, the United Kingdom, Czech Republic, and Spain regarding the use of cookies on popular websites. The report covers 478 e-commerce, media, and public service websites; disclosures to users on installed cookies; and procedures in place to obtain user consent. The Article 29 Working Party concluded that, while most sites inform users about cookies, additional efforts are necessary to obtain the proper user consent.

Article 29 Working Party Issues Statement on Automatic Interstate Exchanges of

Personal Data for Tax Purposes
On February 4, the Article 29 Working Party released a statement discussing the mechanisms for automatic interstate exchanges of personal data for tax purposes and the impact on privacy and data protection. The statement requests involved national governments and EU institutions involved to ensure appropriate and consistent safeguards for data protection. In particular, the Article 29 Working Party (i) touted adherence to the principles of purpose limitation and necessity; (ii) discussed increased risks and liability under EU data protection laws; and (iii) confirmed its approach on granting additional guidance to increase data protection safeguards in this area.

Article 29 Working Party Sends Letter to Commissioner on Safe Harbor and Surveillance
On February 5, the Article 29 Working Party published a letter to the Commissioner for Justice, Consumers and Gender Equality expressing concerns about the "massive, indiscriminate and disproportionate access" to EU personal data by U.S. authorities. The Working Party emphasized the EU Commission's 13 recommendations on Safe Harbor and reiterated its own recommendations, including that EU data subjects be granted the same data protection rights as those in the U.S. The Working Party also discussed surveillance solutions for other transfer instruments (standard contractual clauses and binding corporate rules) and concluded by requesting an international agreement against "indiscriminate surveillance."

Article 29 Working Party Publishes Letter on Passenger Name Records in Mexico
On February 6, the Article 29 Working Party sent a letter to the Commissioner for Migration, Home Affairs and Citizenship regarding the Mexican government's requirement to transfer the passenger name records of all passengers flying from the European Union to Mexico. Noting no legal authority for this transfer and the need to adequately safeguard this data, the Working Party suggested a solution based on the European Charter of Fundamental Rights and the EU Data Protection Directive 95/46/EC.

Article 29 Working Party Raises Concerns Regarding Draft General Data Protection Regulation
On March 17, the Article 29 Working Party issued a press release raising concerns about the Justice and Home Affairs Council's consensus draft General Data Protection Regulation. The Working Party stated that under the regulation, "it will be possible for a data controller to further process data even if the purpose is incompatible with the original one as long as the controller has an overriding interest in this processing." To prevent this, the Working Party called upon Member States to modify the regulation's wording to safeguard the "fundamental right to data protection."

Article 29 Working Party Comments on EU Passenger Name Records
On March 19, the Article 29 Working Party sent a letter to the Chairman of the Committee on Civil Liberties, Justice and Home Affairs on the EU Passenger Name Records ("EU PNR") system pushed forward by the EU Council and the EU Parliament. In the letter, the Article 29 Working Party stated that any EU PNR system must respect the privacy and protection of personal data, and it recommended further justification for the EU PNR scheme, a detailed evaluation of its efficiency, and a sunset clause.

European Data Protection Supervisor

New European Data Protection Supervisor Presents 2015–2019 Strategy
On March 2, the new European Data Protection Supervisor ("EDPS") presented a five-year plan with three strategic objectives and 10 actions, including a special focus on data protection in the digital age, global partnerships, and the implementation of up-to-date data protection rules.

EDPS Speaks on Global Privacy Issues at Two Events in Washington, D.C.
On March 10, the EDPS spoke at the Council of Foreign Relations and at the Annual Dinner for the Center for Democracy and Technology. At the council, he commented on

his strategy for implementing the General Data Protection Regulation, stressing the adjustment of data protection to the digital environment, global partnerships to face challenges posed by new technologies, and a new deal on data protection and transatlantic data flows. At the dinner, the EDPS insisted on the need to develop global privacy rules and the importance of making privacy simple, user-friendly, and readable.

European Network and Information Security Agency

ENISA Updates Recommendations on Baseline Capabilities for CERTs
In December 2014, the European Network and Information Security Agency ("ENISA") provided updates for computer emergency rescue teams ("CERTs") fulfilling baseline capabilities. According to the report, a coordinated approach that includes enhanced information-sharing and cooperative incident response is needed to effectively respond to threats and attacks against information infrastructure at the European level.

ENISA Proposes Standards for Electronic IDs and Trust Service Providers
In December 2014, ENISA released a paper covering standards for electronic IDs and trust service providers. The paper reviews major EU initiatives and ENISA recommendations in this area, and discusses concrete standardization activities associated with electronic IDs and trust service providers. The report concludes with a proposal for a standard on cryptographic suites for electronic signatures and infrastructures put forward by ENISA and related to the ETSI TS 113 312 standard.

ENISA Publishes Study on Cybersecurity for Smart Homes
On February 9, ENISA issued a report titled Threat Landscape and Good Practice, Guide for Smart Home and Converged Media. The report provides an overview of the current state of cybersecurity for smart homes and identifies commonly used assets, exposure of these assets to cyber threats, threat agents, vulnerabilities and risks, and available good practices.

ENISA Issues Report on Certification Schemes for ICS/SCADA Professionals
On February 19, ENISA published a report on good practices and recommendations for developing harmonized certification schemes for Industrial Control Systems and Supervisory Control and Data Acquisition ("ICS/SCADA") professionals. The report relies on expert interviews and online surveys to identify existing challenges and propose guidelines for creating certification schemes for these cybersecurity professionals.

ENISA Releases Study on Methodologies for Identifying Critical Information Infrastructure Assets and Services
On February 23, ENISA published a study addressing the identification of critical information infrastructures in communication networks. The study provides an overview of the current state of European networks and suggests possible improvements in anticipation of future threat landscapes and challenges.

ENISA Issues Guide Relating to Security Framework for Governmental Cloud Computing
On February 26, ENISA published a guide proposing steps that public administrations should take to deploy cloud computing, providing guidance from pre-procurement until finalization and termination of a cloud contract. Although largely based on four national governmental cloud models (Estonia, Greece, Spain, and the UK), the guide also includes annex case studies, interviews, and a decision tree/questionnaire template that can be used by administrations for cloud-related projects.

ENISA Publishes Auditing Framework for Trust Service Providers
On April 2, ENISA issued a report providing an overview of trust service provider ("TSP") audits. The report, aimed at TSPs performing audits and external auditors assessing TSPs, discusses the standards applicable to the auditors, the methodology of auditing TSPs, TSP documentation, and implementation of TSP services.

ENISA Issues Guidelines for Supervising Electronic Communication Providers
On April 9, ENISA published a framework for authorities supervising the electronic communications sector under Article 13a of the Framework Directive and Article 4 of the E-Privacy Directive. The framework includes 26 security objectives, grouped in seven domains and in three sophistication levels (basic, industry-standard, and state-of-the-art). For each security objective, the framework lists relevant security measures and required evidence to ensure that the measures are applied.

Belgium

Belgian Privacy Commission Issues Recommendation on Cookie Use
On February 4, the Belgian Privacy Commission adopted a recommendation (source document in French) on the use of cookies. This recommendation builds on previous opinions of the Article 29 Working Party and addresses relevant definitions, legal principles, and recommendations per type of actor.

Belgium Passes Legislation on Processing Personal Data for Belgian Passports and Travel Documents
On February 10, Belgium enacted a law (source document in French and Dutch) that regulates the automated processing of personal data related to Belgian passports and travel documents, including their production, billing, indemnification, and replacement. For each purpose identified, the law explains which data can be collected, how long it can be retained, and by whom it can be processed.

Belgian Privacy Commission Discusses EU Expert Database
On February 25, the Belgian Privacy Commission issued an opinion (source document in French) establishing the conditions for using the EU database of experts, called the "EU-Goalkeeper Registrar."

Belgian Privacy Commission Publishes Opinion on Cloud Use by Hospitals
On February 25, the Belgian Privacy Commission published an opinion (source document in French) on cloud computing in a hospital setting and requested that such use be conditioned on the establishment of an evaluation tool and the removal of restrictions on the types of cloud services chosen.

Belgium Exempts Social Inspectors from Privacy Law Compliance
On March 11, Belgium adopted a Royal Decree (source document in French and Dutch) that exempts social inspectors from complying with certain privacy law obligations.

Belgian Privacy Commission Investigates Social Media Company's Compliance with Data Protection Law
Following a draft academic report published on March 31, the Belgian Privacy Commission announced that it is assessing a social media company's compliance with Belgian data protection law. Among other topics, the report discusses the privacy implications of the company's privacy policies, contract terms, sharing of user data, location tracking, and use of user-generated content.

France

La Quadrature du Net Challenges Decree on Military Programming Act
On February 18, La Quadrature du Net (a French association for data protection and public freedoms) requested that the French Council of State (source document in French) challenge the implementation decree of the Military Programming Act, passed on December 28, 2014. The Act enables authorities to access connection data of web users in procedures related to terrorism and cyber criminality.

CNIL Releases BYOD Guidelines
On February 19, the French Data Protection Authority ("CNIL") issued guidelines (source

document in French) relating to the use of personal devices by employees ("Bring your Own Device" or "BYOD"). These guidelines discuss key principles for data protection compliance and seek to apply the same security and device management procedures that exist for company equipment to employee-owned devices when used for work purposes.

French Government Publishes Decree to Delist Terrorism-Related Websites from Search Engines
On March 4, the French government adopted Decree 2015-253 (source document in French), which enables delisting of websites promoting terrorist actions and websites related to child pornography from internet search results.

CNIL Streamlines International Transfers of Personal Data
On March 24, CNIL announced a simplified process for the entities of a corporate group to register personal data transfers outside of the EU on the basis of binding corporate rules ("BCRs"). Once the BCRs are approved at a business group level, CNIL will issue a single authorization that the business group entities will be able to reference in their filings rather than request new and individual authorizations of data transfers.

French Government Publishes Decree on Security of Essential Operators' Information Systems
On March 27, the French government enacted Decree 2015-351 (source document in French), which provides additional details relating to the cybersecurity framework applicable to essential operators. Forthcoming ministerial orders will establish the criteria enabling the essential operators to identify information systems subject to the cybersecurity framework, rules relating to information security, and the incident reporting procedures.

French Government Publishes Decree on TSPs for National Security Providers
On March 27, the French government adopted Decree 2015-350 (source document in French) to set up a qualification procedure for products and service providers needed by essential operators. The qualification procedure is intended for persons who need to qualify security products and services for national security purposes.

CNIL Releases Guidelines on HTTPS Traffic Analysis
On March 31, CNIL issued guidelines (source document in French) for data protection compliance on analysis procedures relating to online communications encrypted with the https protocol.

CNIL Releases 2014 Annual Report
On April 16, CNIL issued its annual report for 2014 (source document in French). According to the report, the number of privacy-related complaints rose from the previous year, including complaints concerning e-reputation issues (39 percent rise), e-commerce (16 percent rise), banks (12 percent), and public liberties and local administration (11 percent). CNIL also noted that it has received 200 complaints relating to delisting from web search engines since the May 2014 ECJ decision relating to the Right To Be Forgotten.

Germany

Bavarian DPO Examines Data Protection Standards of Smart Televisions
On February 27, the Bavarian Data Protection Officer ("DPO") issued a press release on the results of its examination of smart televisions of 13 manufacturers who represent a 90 percent market share in Germany. Although detailed results of the examination were not published, the report notes that manufacturers rarely implement basic data protection principles and do not enable anonymous use.

German Federal Government Introduces Research and Development Program on Cybersecurity
On March 11, the German federal government presented its plan (source document in

German) to promote research and development regarding IT security. With a budget of €180M until 2020, the government plans to promote particular encryption technologies to protect personal data and communication services. The plan focuses on four areas: new technologies, secure and trustworthy information and communication systems, application areas of IT security, and privacy and protection of data.

Hamburg's DPO Aims to Restrict Internet Search Engine's Combination of User Data
On April 8, the Hamburg DPO denied an internet search engine's appeal of a September 2014 decision in which the DPO ordered the search engine to either restrict the combination of user data from its various services or to obtain additional consent from the users. According to the DPO, the search engine already announced that it will materially change its services in order to meet these data protection requirements.

German Ministry of Justice Presents Guidelines on Planned Data Retention Act
On April 15, 2015 the German Minister of Justice presented guidelines (source document in German) for the implementation of retention obligations and maximum storage periods for traffic data (*Leitlinien zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten*). The new proposal sets telecommunications traffic data retention at 10 weeks and location data from cell phones at four weeks. The content of the communication, websites accessed, and email data would be excluded from the retention obligation. Furthermore, access to the data would be limited to cases of severe crimes and would require court approval.

Spain

Spanish Data Protection Agency Adopts Resolution on Right to be Forgotten
In March, the Spanish DPA (*Agencia Española de Protección de Datos*) adopted a resolution on the Right To Be Forgotten. Under the resolution, internet search engines must remove the search results of individuals who request to have their information removed from these results.

The Netherlands

Dutch Data Protection Authority Issues Opinion on Revisions to Data Retention Act
On February 16, 2015, the Dutch Data Protection Authority ("DDPA") issued advice on draft legislation to amend the existing data retention obligations regarding telephone and internet communications data. The draft bill followed the April 2014 ECJ decision nullifying the European Data Retention Directive. In its statement, the DDPA did not recommend presenting the bill to the Dutch Parliament because the draft legislation still maintains the obligation to retain telecommunications data and does not adequately substantiate the retention of this data.

DDPA Signs Memorandum of Understanding with U.S. Counterpart on Privacy Enforcement
On March 9, the DDPA and the U.S. Federal Trade Commission signed a Memorandum of Understanding to improve information-sharing and enforcement cooperation on privacy and data security matters. In addition to describing the Agreement's objective of mutual assistance in enforcing certain "Covered Privacy Violations," the Agreement sets forth guidelines for handling and storing shared information.

Dutch Government Amends Cookie Regulations
On March 11, the Dutch government enacted an amended version of the cookie legislation (source document in Dutch). The amendments introduce a number of exceptions to the requirement to obtain the user's consent prior to using cookies, including an exception if the cookie is used to obtain information about the quality of the service provided or if the cookie has no impact on the privacy of the user involved. Also, under the amendments,

the government cannot require the user to accept cookies before giving access to the site. However, cookies used to load user profiles or track users on the internet still require consent.

United Kingdom

UK Amends Law to Facilitate Actions Against Nuisance Calls and Spam
On February 24, the UK government updated its rules relating to nuisance calls and spam. While the prior rules mandated proof that such calls or spam caused "substantial damage or substantial distress," the new rules require only a showing that the calls or spam are a serious breach of law. This reduces the burden of proof before the Information Commissioner can impose a monetary penalty of up to £500,000.

UK Information Commissioner Fines Personal Injury Claims Company £80,000 for Unsolicited Calls
On March 26, the Information Commissioner fined a personal injuries claims management company for making direct marketing calls to individuals without their consent. Many of the affected individuals had registered with the Telephone Preference Service so that they would not receive such marketing calls.

The following Jones Day attorneys contributed to the Europe sections: Paloma Bru, Marianna Consiglio, Undine von Diemar, Olivier Haas, Olaf Hohlefelder, Bastiaan Kout, Jonathon Little, Afra Mantoni, Laurent De Muyter, Selma Olthof, and Elizabeth Robertson.

[Return to Top]

Asia

People's Republic of China

State Agency Promulgates Requirements for Collecting Consumer Information
On March 15, the State Administration for Industry and Commerce's Measures for Punishments against Infringements on Consumers Right and Interests (source document in Chinese) became effective. The measures aim to protect the personal information of general consumers by setting forth requirements for collecting consumers' personal information and sending commercial information to consumers. The measures also define various penalties for violations of these requirements.

Hong Kong

Privacy Commissioner Responds to Ombudsman Investigation Reports
On March 24, the Office of the Privacy Commissioner for Personal Data ("PCPD") published a media statement responding to the Office of Ombudsman's investigative report on the Education Bureau's Nondisclosure of Teachers' Registration Status and its investigation into the Recovery of Debts under the Non-Means-Tested Loan Scheme. The PCPD commented that the Education Bureau should apply the Personal Data (Privacy) Ordinance when determining whether or not to disclose individual teachers' personal data and the exact personal data to be disclosed. The PCPD also rejected the Ombudsman's proposal that the Working Family and Student Financial Assistance Agency should forward the borrower's default data to an outside consumer credit agency because of the potential privacy ramifications when borrower data is sent to agencies operating outside of Hong Kong.

PCPD Publishes New Guidance on Responsible Use of Drones
On March 31, the PCPD published Guidance on CCTV Surveillance and Use of Drones, which sets forth guidance for the responsible use of drones (unmanned aircraft systems). The guidelines state that any intrusion on privacy caused by drones must be proportional to the benefit derived from their use.

Japan

Cabinet Submits Bill to Amend Personal Information Protection Act
On March 10, the Cabinet submitted a bill to amend the Personal Information Protection Act (source document in Japanese) to the Diet. The major changes proposed by the amendments include (i) the establishment of a privacy commissioner; (ii) expanding the definition of the personal information; (iii) new rules on utilizing anonymous personal data; (iv) applicability of the Act to foreign entities; and (v) new regulations on the extraterritorial transfer of the personal data.

Cabinet Submits Bill to Amend My Numbers Act
On March 10, the Cabinet submitted a bill (source document in Japanese) to amend the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure to the Diet. The bill would expand the application of individual ID numbers ("My Numbers") from the limited administrative purposes of taxation and social security. Under the proposal, My Numbers would be used for bank accounts and for municipal governments to manage individual immunization and health records.

Taiwan

Ministry of Justice Interprets Personal Information Act
On January 15, the Ministry of Justice issued a letter (source document in Chinese) defining situations under Paragraph 1 of Article 15 of the Personal Information Act in which a government agency may collect an individual's personal information without consent. The Ministry explained how a police officer may legally collect the fingerprint of an unconscious patient whose identity is otherwise unknown to health care providers.

The following Jones Day attorneys contributed to the Asia sections: Li-Jung Huang, Anita Leung, Michiru Takahashi, and Richard Zeng.

[Return to Top]

Australia

Information Commissioner Updates Privacy Principles Guidelines
On April 1, the Office of the Australian Information Commissioner updated the Australian Privacy Principles ("APP") Guidelines. The updated APP Guidelines clarify when entities will be considered to be doing business in Australia—a key component in determining whether APP compliance is required for the entity. The revisions also discuss the circumstances under which providing personal information to an overseas contractor would deviate from the APP Guidelines.

Australia Passes Data Retention Bill
On April 13, Australia officially enacted the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth). The legislation requires telecommunications service providers to retain and secure telecommunications data (not content) for two years and sets forth restrictions on agencies that may access the stored data.

The following Jones Day attorneys contributed to the Australia section: Adam Salter and Nicola Walker.

[Return to Top]

Jones Day Cybersecurity, Privacy, and Data Protection Lawyers

Emmanuel G. Baud	Jean-Paul Boulee	Wolfgang G. Büchner	Shawn Cleveland

Paris

James A. Cox
Dallas

Joshua L. Fuchs
Houston

Elena Kaplan
Atlanta

Anita Leung
Hong Kong

Todd McClelland
Atlanta

Janine Cone Metcalf
Atlanta

Chaka M. Patterson
Chicago

Gregory P. Silberman
Silicon Valley

Michael W. Vella
Shanghai

Paloma Bru
Madrid

Christopher J. Lopata
New York

Michael G. Morgan
Los Angeles

Po-Chien Chen
Taipei

Adrian Garcia
Dallas

Javier Gutiérrez Ponce
Madrid

Nandini Iyer
Silicon Valley

Susan M. O'Connor
New York

Jessica M. Sawyer
Los Angeles

Natalie A. Williams
Atlanta

Atlanta

Walter W. Davis
Atlanta

Karen P. Hewitt
San Diego

Jeffrey L. Kapp
Cleveland

Jonathon Little
London

Jason McDonell
San Francisco

Caroline N. Mitchell
San Francisco

Jeff Rabkin
San Francisco

Cristiana Spontoni
Brussels

Undine von Diemar
Munich

Amanda B. Childs
Dallas

Margaret I. Lyle
Dallas

Sergei Volfson
Moscow

Nigel Chin
Singapore

Steven G. Gersten
Dallas

Aaron M. Healey
Columbus

Bastiaan K. Kout
Amsterdam

Nicole M. Perry
Houston

Raquel Travesí
Madrid

Marc L. Swartzbaugh
Cleveland

Munich

Scott A. Edelstein
Washington/Los Angeles

John E. Iole
Pittsburgh

J. Todd Kennard
Columbus

Kevin D. Lyles
Columbus

Carmen G. McLean
Washington

Matthew D. Orwig
Dallas/Houston

Elizabeth A. Robertson
London

Michiru Takahashi
Tokyo

Toru Yamada
Tokyo

Jay Johnson
Dallas

Stefano Macchi di Cellere
Milan/London

Olivier Haas
Paris

Christopher S. Cogburn
Atlanta

Bart Green
Irvine

Elaine Ho
Singapore

Colin Leary
San Francisco

Scott B. Poteet
Dallas

Virginia Uelze
São Paulo

Dallas/Houston

Timothy P. Fraelich
Cleveland

Robert W. Kantner
Dallas

Ted-Philip Kroke
Frankfurt

John M. Majoras
Columbus/Washington

Daniel J. McLoon
Los Angeles

Mauricio F. Paez
New York

Adam Salter
Sydney

Rhys Thomas
London

Sidney R. Brown
Atlanta

Guillermo E. Larrea
Mexico City

Georg Mikes
Frankfurt

David L. Odom
Dallas

Laurent De Muyter
Brussels

Joshua Grossman
New York

Nancy L. Hoffman
New York

Gabriel Ledeen
San Francisco

Brandy Hutton Ranjan
Columbus

Anand Varadarajan
Dallas

Follow us on:

Jones Day is a legal institution with 2,400 lawyers on five continents. We are One Firm Worldwide℠.