JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 11 | September 2016 JONES DAY

Jones Day Attorney Spotlight: Jörg Hladjk

Multinational companies have faced new developments over the past year in the area of EU data protection law, from the invalidation of the U.S.-EU Safe Harbor framework and uncertainty for international data transfers based on EU data transfer agreements, to the adoption of the EU's General Data Protection Regulation ("GDPR"), and most recently the EU-U.S. Privacy Shield. Ongoing enforcement activity by the EU data protection authorities, the imminent adoption of the EU Cybersecurity Directive, and numerous guidelines issued on a range of compliance issues will further shape the legal landscape.

Jörg Hladjk is a key member of the Firm's Cybersecurity, Privacy & Data Protection Practice and leads this practice in Brussels—the legislative hub in Europe for data protection and cybersecurity and where the European Data Protection Board will hear cross-border EU data protection cases under the GDPR. Jörg has well-established contacts with the European Commission, the European Data Protection Supervisor, and EU data protection authorities, and he counsels multinational clients across various industry sectors on all aspects of global and European cybersecurity and data

EDITORIAL CONTACTS

Daniel J. McLoon
Los Angeles

Mauricio F. Paez
New York

Jonathon Little
London

Kevin D. Lyles
Columbus

Todd S. McClelland
Atlanta

Jeff Rabkin
San Francisco

Adam Salter
Sydney

Michiru Takahashi
Tokyo

Undine von Diemar
Munich

Paloma Bru
Madrid

Olivier Haas
Paris

Jörg Hladjk
Brussels

Jay Johnson
Dallas

Editor-in-Chief: Anand Varadarajan

Practice Directory

HOT TOPICS IN THIS ISSUE

protection laws.

With more than 11 years of experience in this field, Jörg advises on a wide range of activities: global and pan-European compliance strategies for international data transfers, including the implementation of EU Standard Contractual Clauses and Binding Corporate Rules; managing notification procedures with national data protection authorities across the EU; developing data protection compliance programs; and assisting clients with data security breaches.

Jörg's broad-ranging experience reinforces our efforts to provide clients with the best guidance in Europe's dynamic and rapidly changing data protection landscape, where noncompliance comes with heavy sanctions.

United States

Regulatory—Policy, Best Practices, and Standards

New York Attorney General Announces Record Data Breach Notifications for 2016
On May 4, the New York Attorney General announced that his office has received a more than 40 percent increase in data breach notifications involving New Yorkers in 2016 as compared to 2015. The office is on pace to receive well over 1,000 notices for the year, a new record.

Survey Finds Government Unable to Adequately Detect Cyber Attacks
On May 18, the International Information System Security Certification Consortium and KPMG released The State of Cybersecurity from the Federal Cyber Executive Perspective. According to a survey of 54 officials and executives from the Department of Defense, government intelligence agencies, and civilian intelligence agencies, 59 percent found that their agencies struggle to understand how cyber attackers could potentially breach their systems, and 65 percent disagreed that the federal government as a whole could detect ongoing cyber attacks.

Regulatory—Critical Infrastructure

NIST Refines Cybersecurity Framework
On June 9, NIST announced minor updates to its Cybersecurity Framework based on user feedback. NIST noted that the updated draft will ensure that document references are current, clarify the framework's Implementation tiers, and add guidance relating to supply chain risk management.

NIST Partners with Baldridge Program

China Considers Second Draft of Cybersecurity Law

Australia Releases Guide to Big Data and Australian Privacy Principles

RECENT AND PENDING SPEAKING ENGAGEMENTS

For more information on Jones Day speaking engagements, please contact one of the editorial contacts listed above.

Medical Devices: Cybersecurity, Privacy, and HIPAA, ABA Third Medical Device & Healthcare Technology Compliance Institute (October 13-15). **Jones Day Speaker:** Mauricio Paez

Outsourcing, IT and Data Protection VAB Seminar: Foreign Banks in Germany—New Challenges and New Chances, Frankfurt (October 6). **Jones Day Speakers:** Undine von Diemar, Ted Kroke

EU Privacy Laws and Implications for Implementing Health & Safety Programs European Union Health, Safety & Environment Forum, Dublin (September 28-29). **Jones Day Speaker:** Undine von Diemar

The Debate Between Security and Privacy Continues: Where Do We Draw the Line?, ALM cyberSecure 2016, New York (September 27). **Jones Day Speaker:** Mauricio Paez

International Data Transfers: Accessing Your Organizations Adequacy, ALM cybersecure 2016, New York (September 27). **Jones Day Speaker:** Mauricio Paez

Cybersecurity and Insurance in the Age of Digital Vulnerability: What In-House Counsel Need To Know, Association of Corporate Counsel, San Diego (September 21). **Jones Day Speakers:** Jeff Rabkin, Richard DeNatale

What to Do When: You Get Hacked, Jones Day MCLE presentation (September 8). **Jones Day Speakers:** Jeff Rabkin, Greg Silberman, Richard DeNatale

Eliminating the Weakest Link: Cybersecurity Ethics and Risk Mitigation for Lawyers, Jones Day CLE Breakfast Club, Houston (September 15). **Jones Day Speakers:** Nicole Perry, Jason Varnado

On July 12, NIST issued a press release stating that it is partnering with Baldridge Program to develop a Baldridge-based assessment tool aligned to NIST's Cybersecurity Framework. According to the Baldridge Program director, the tool "will enable an evaluation of not only the robustness, but also of the effectiveness and maturity of the cybersecurity risk management programs of organizations of all kinds."

Regulatory—Defense and National Security

U.S. and India Enhance Cybersecurity Relationship
On June 7, the United States and India issued a joint statement announcing a commitment to increase defense cooperation in the area of cybersecurity. The two countries agreed to share cybersecurity threat information on a real-time or near real-time basis.

DHS and DOJ Release Cyber Threat Indicators and Defensive Measures Procedures
On June 15, the Department of Homeland Security ("DHS") and the Department of Justice ("DOJ") jointly released Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government. The procedures discuss how the government handles cybersecurity information shared by companies and provide guidelines for companies seeking liability protection by sharing cybersecurity threat information with the government.

Regulatory—Energy and Utilities

FBI Sues City and Public Utility to Prevent Privacy Violation
On June 13, the United States filed a complaint for injunctive relief against the City of Seattle and its public utility, attempting to prevent the release of private information related to Federal Bureau of Investigation ("FBI") surveillance. The city has been subjected to information requests under the Washington State Public Records Act for this information. The government objects to the proposed disclosure under law enforcement privilege.

State Department Shares Technology to Decrease Energy Use
In June, a State Department member delivered a presentation at a cloud computing summit regarding "Smart Meter" technology. The technology would rely upon sensors placed in cities throughout the United States to track energy usage and would offer a more cost-effective and efficient means of acquiring this information. The State Department representative discussed the importance of addressing privacy and monitoring concerns as the

Internet of Things, Civil Liabilities and Privacy, IAPP KnowledgeNet, Dallas (September 6). **Jones Day Speaker:** Jay Johnson

A Briefing on the Privacy Shield, Jones Day webinar (August 2). **Jones Day Speakers:** Jonathon Little, Todd McClelland, Undine von Diemar, Jörg Hladjk, Jennifer Everett

Digital Health: Cybersecurity Challenges When Dealing with Medical Device Software and Intercommunication Between Devices, ACI Chicago (July 21). **Jones Day Speaker:** Mauricio Paez

The Changing Landscape of Cybersecurity: Data Breaches, Cross-Border Data Transfers and Risk Management, Sydney (July 21). **Jones Day Speaker:** Mauricio Paez

The Business Impact of (EU) Data Protection Law—How Can Companies Prepare for Compliance?, Milan (July 11). **Jones Day Speakers:** Jörg Hladjk, Giuseppe Mezzapesa, Takuya Ohno

Cyber-Threats: How Businesses Can and Must Prepare, Jones Day seminar, Paris (July 7). **Jones Day Speakers:** Ozan Akyurek, Rémy Fekete, Bénédicte Graulle, Olivier Haas

Recent Developments concerning Privacy in the EU: How to Prepare for the Upcoming General Data Protection Regulation and What is the Current Status of Rules for the International Transfer of Personal Data (July 1). **Jones Day Speakers:** Undine von Diemar, Michiru Takahashi

Recent Developments Concerning Data in the EU: Publication by EMA of Commercially Confidential Information (Clinical Data) and New Rules for the International Transfer of Personal Data (June 30). **Jones Day Speakers:** Christian Fulda, Undine von Diemar, Michiru Takahashi

New European General Data Protection Regulation, Jones Day, Madrid (June 28). **Jones Day Speaker:** Paloma Bru

Stay Calm and Be Prepared: Responding to Ransomware, Jones Day (June 23). **Jones Day Speaker:** Greg Silberman

New Regulation on Privacy and Cybersecurity, Jones Day, Mexico City (June 23). **Jones Day Speakers:** Guillermo Larrea, Mauricio Paez, Paloma Bru

technology is implemented.

Regulatory—Retail

State Attorneys General Request Privacy Requirements on Third-Party Set-Top Box Developers
On June 3, 14 State Attorneys General and the Attorney General of the District of Columbia published a letter to the Federal Communications Commission ("FCC") requesting that the FCC include a privacy certification requirement in prospective rules opening the pay-TV set-top box market to third-party developers. The request seeks to require third-party manufacturers of set-top boxes to publish consumer-facing statements of compliance with privacy obligations that already apply to satellite and cable providers.

Home Depot Appeals Ruling on Banks' Ability to Seek Data Breach Damages
On July 5, Home Depot requested interlocutory review of a May 18 ruling holding that financial institutions have Article III standing to seek damages following a data breach. Home Depot also presented the question of whether retailers owe banks a duty to protect against third-party cyber attacks.

Senate Inquires on "Pokémon Go" Mobile App User Data Collection
On July 12, Senator Al Franken sent a letter to the developer of "Pokémon Go" seeking answers on user privacy and security in its collection of users' personal data, particularly for younger players. The letter asks the company to confirm that it "never collected or stored any information it gained access to as a result of this mistake," identify which third parties the collected data is being shared with, and clarify how children (or their guardians) can meaningfully consent to this data collection.

Regulatory—Financial Services

SEC Names Senior Advisor to Chair for Cybersecurity Policy
On June 2, the Securities and Exchange Commission ("SEC") named a new Senior Advisor to the Chair for Cybersecurity Policy, who will coordinate cybersecurity efforts within the agency and work to "enhanc[e] the SEC's mechanisms for assessing broad-based market risk."

Regulators Instruct Banks to Review Cybersecurity Protections Against Fraudulent Money Transfers
On June 7, the Federal Reserve and Federal Financial Institutions Examination Council issued a notice to banks instructing them to review cybersecurity

The State of Cybersecurity: The Latest Threats, Legal Landscape, and Risk Mitigation Techniques, Business Navigators, Dallas (June 22). **Jones Day Speaker:** Jay Johnson

Recent Transactional and Litigation Developments, Association of Corporate Counsel, Columbus (June 21). **Jones Day Speaker:** Todd Kennard

Emerging Cybersecurity Threats Stemming from the Deployment of the Internet of Things (IoT), Mid-Year Cybersecurity and Data Protection Legal Summit, ALM, New York (June 15). **Jones Day Speaker:** Todd McClelland

Tales from the Cybersecurity Front: How to Protect Your Company, Employees, and Customers When Data Has Been Hacked, Lost, Stolen, or Disposed of Improperly, Jones Day University, Chicago (June 9). **Jones Day Speakers:** Jay Johnson, Chaka Patterson

2016 Compliance Outreach Program for Broker-Dealers, U.S. Securities & Exchange Commission and Financial Industry Regulatory Authority, Federal Reserve, Dallas (June 9). **Jones Day Speaker:** Jay Johnson

What the Blockchain Means for Lawyers, Jones Day (June 8). **Jones Day Speakers:** Greg Silberman, Stephen Obie, Harriet Territt, Michael Butowsky

What Will Privacy Look Like in the Big Data World of 2026?, TIA 2016: Network of the Future, Telecommunications Industry Association, Dallas, TX (June 8). **Jones Day Speaker:** Jay Johnson

The EU-US Privacy Shield: Opportunities and Challenges for Personal Data Transfers From the EU to the US, ALM Mid-year Cybersecurity and Data Protection Legal Summit, New York (June 2016). **Jones Day Speaker:** Mauricio Paez

RECENT AND PENDING PUBLICATIONS

For more information on Jones Day's publications, please contact one of the editorial contacts listed above.

The New EU Cybersecurity Directive: What Impact on Digital Service Providers?, Jones Day Publications (August). **Jones Day Authors:** Various

protections against fraudulent money transfers. The warnings follow recent hacking events, including fraudulent money transfers to steal $81 million from the Bangladesh Central Bank and $12 million from Banco del Austro in Ecuador.

SEC Chair Prioritizes Cybersecurity
On June 14, in testimony before the U.S. Senate's Committee on Banking, Housing, and Urban Affairs, the SEC Chairperson called cybersecurity "one of the greatest risks facing the financial services industry." She outlined the Commission's efforts to address the risks posed by cyber attacks and reaffirmed that Commission staff would continue to focus on cybersecurity and controls in 2016.

CFPB Proposes Amendment to GLBA Regarding Annual Privacy Notices
On July 1, the CFPB proposed an amendment to the Gramm-Leach-Bliley Act ("GLBA") that would allow financial institutions that met certain requirements to be exempt from sending annual privacy notices to customers as currently required under the GLBA. The CFPB also proposed the establishment of deadlines for institutions resuming annual privacy notices if their practices change and cease to qualify for exemption.

Regulatory—Health Care/HIPAA

HHS Issues Guidance on Ransomware and HIPAA
In July, the U.S. Department of Health & Human Services ("HHS") issued guidance concluding that a ransomware attack constitutes a "breach" under the Health Insurance Portability and Accountability Act ("HIPAA"). The guidance states that when electronic protected health information is encrypted as the result of a ransomware attack, a breach has occurred because the information encrypted by the ransomware was "acquired" by unauthorized individuals and is thus a "disclosure" not permitted under the HIPAA Privacy Rule. A breach is presumed to have occurred in such a situation unless the covered entity or individual can demonstrate that there is a low probability that the protected health information has been compromised.

FTC Finds Lab's Data Security Practices Unreasonable
On July 28, the Federal Trade Commission ("FTC") issued a unanimous opinion holding that LabMD, Inc.'s data security practices were "unreasonable" and lacked "even basic precautions to protect the sensitive consumer information maintained on its computer system," constituting unfair practices under Section 5 of the FTC Act. Specifically, the FTC found that LabMD failed to protect its computer network or employ adequate risk assessment tools, failed to provide data security training to its employees, and failed to adequately restrict and monitor the computer practices of individuals using its network. The Final Order directs LabMD to undertake remedial measures and imposes a 20-year reporting requirement.

The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws , Jones Day Publications (August). **Jones Day Authors:** Various

Hospitals and Healthcare Systems Are the New Ransomware Target: How to Avoid Becoming a Hostage , Inside Medical Liability Online (August). **Jones Day Authors:** Greg Silberman, Alexandra McDonald

Post-*Spokeo* Decisions Rejecting "No Injury" Lawsuits, Jones Day Publications (July). **Jones Day Authors:** Todd Kennard, John Vogt, Brandy Ranjan

The EU–U.S. Privacy Shield Approved, Jones Day Publications (July). **Jones Day Authors:** Various

Second Circuit Limits Territorial Reach of U.S. Government to Domestically Stored Data, Jones Day Publications (July). **Jones Day Author:** Jay Johnson

New Russian Legislation on Massive Telecoms Surveillance, Jones Day Publications (July). **Jones Day Authors:** Sergei Volfson, Mauricio Paez, Undine von Diemar, Rémy Fekete

Beware the Potential Move from Inapplicable Cybersecurity Standards to an Applicable Standard of Care, *Texas Lawyer* (June). **Jones Day Author:** Jay Johnson

Agencies Establish Baseline Cybersecurity Safeguards for Information Systems Containing Federal Contract Information, Jones Day Publications (June). **Jones Day Authors:** Grayson Yeargin, Chad Dorr

Public and Private Sector Finance and Health Care Groups to Discuss Ransomware
On August 15, the FTC announced that its Chief Technologist will meet with cybersecurity and health care leaders, as well as the FBI, to discuss health care ransomware issues. Representatives from Cisco, Symantec, the Children's National Medical Center, PricewaterhouseCoopers LLP, and the FBI will also be present.

Electronic Health Records Company Practice Fusion Settles with FTC
On August 16, the FTC approved a Final Order resolving its complaint against cloud-based electronic health records company Practice Fusion regarding charges of misleading consumers by soliciting reviews for doctors without adequately disclosing that the reviews would be publicly posted on the internet. The settlement prohibits Practice Fusion from making deceptive statements regarding the extent to which it uses, maintains, and protects the privacy or confidentiality of the information it collects, and requires disclosure and consent prior to making information publicly available. Additionally, the settlement prohibits Practice Fusion from publicly displaying the reviews it collected during the time period covered by the complaint.

Litigation, Judicial Rulings, and Agency Enforcements

District Court Denies Motion to Dismiss Class Action Against Social Media Platform
In May, the U.S. District Court for the Northern District of California denied a motion to dismiss a claim against Facebook. The plaintiffs alleged the platform's online photo-tagging feature violated the Illinois Biometric Information Privacy Act. Although the case was transferred from Illinois to California, the California court allowed the claim to proceed on grounds that "Illinois will suffer a complete negation of its biometric privacy protections for its citizens if California law is applied."

U.S. Supreme Court Overturns Ninth Circuit's Ruling on Standing
On May 16, the U.S. Supreme Court reversed and remanded the Ninth Circuit's ruling that a plaintiff had standing to sue a consumer reporting agency. The plaintiff filed suit under the Fair Credit Reporting Act, claiming that the consumer reporting agency published incorrect information about the plaintiff online. The Court held that the Ninth Circuit failed to separately analyze whether the alleged injury was both particularized *and* concrete, which is necessary for an analysis of standing under Article III. The Supreme Court remanded the case, requiring the Ninth Circuit to individually analyze the requirements of particularity and concreteness. For more information, please see the corresponding Jones Day *Alert*.

SEC Settles Charges with Broker Dealer Following Disclosure of Customer Information
In June, the SEC settled charges against a registered broker dealer/investment adviser for failing to adopt written policies and procedures reasonably designed to protect customer records and information. The company had stored customers' personally identifiable information on two applications, and one of the company's employees had misappropriated and stored this information on a personal server, which was later hacked. The SEC alleged that the company violated the Safeguards Rule because it failed to ensure the reasonable design and proper operation of its policies and procedures for safeguarding confidential customer data.

Hosting Platform Seeks Preliminary Injunction Against City
In June, following proposed legislation that penalizes failures to register travel accommodations, a travel accommodations hosting platform filed a motion for preliminary injunction against the City and County of San Francisco. The company claimed that such legislation would require the dissemination of the hosts' addresses in violation of the Stored Communications Act.

CFPB Files Suit Against Third-Party Payment Processor
On June 6, the CFPB filed suit against third-party payment processor and two of its executives for allegedly enabling unauthorized and other illegal withdrawals from consumer banking accounts by their clients. The CFPB alleges the processor turned a blind eye to warning signs of its clients' fraud, such as high rates of returned payments, insufficient funds, and invalid or closed accounts, and processed electronic funds transfers from consumer bank accounts on behalf of clients that were breaking the law.

District Court Dismisses Proposed Class Action Against Cable Provider
On June 17, the U.S. District Court for the Eastern District of Wisconsin dismissed a case against a large cable services provider on the grounds that the plaintiff did not have Article III standing. The plaintiff, suing on behalf of himself and putative class members, alleged that the defendant engaged in an illegal practice of keeping customer personal information even after customers terminated their accounts. The court cited *Spokeo, Inc. v. Robins* in finding that the plaintiff did not show a concrete injury, as required by Article III. The plaintiff has filed an appeal in the Seventh Circuit. For more information, please see the corresponding Jones Day *Alert*.

Health and Sciences University Signs Resolution Agreement with Government Agency
On July 13, a health and sciences university signed a resolution agreement with the United States Department of Health and Human Services Office for Civil Rights ("OCR") regarding two data breaches that occurred in 2013. In the first breach, a laptop belonging to the university with electronically protected health information was stolen. The second breach involved the unprotected use of "cloud" storage. The resolution agreement includes a $2.7 million payment and a plan for corrective action.

Second Circuit Holds that U.S. Government Cannot Access Consumer Data Stored Overseas Using Stored Communications Act Warrant
On July 14, the Second Circuit ruled that the U.S. government could not use a Stored Communications Act ("SCA") warrant to access consumer data stored on a server in Ireland. The three-judge panel's unanimous decision explained that the focus of the SCA is the protection of a user's privacy interest, and "Congress did not intend the SCA's warrant provisions to apply extraterritorially." For more information, please see the corresponding Jones Day *Alert*.

Ninth Circuit Holds Accessing Database Violates Computer Fraud and Abuse Act and Economic Espionage Act
On July 15, the Ninth Circuit issued an opinion in *United States v. Nosal*, No. 14-10037 (9th Cir. July 15, 2016), holding that defendant Nosal violated the Computer Fraud and Abuse Act and Economic Espionage Act by logging in to a database with the username and password of a "willing currently-employed accomplice."

FTC Scrutinizes APEC Certification Claims
On June 21, the FTC settled its first action related to the Asia-Pacific Economic Cooperative ("APEC") Cross-Border Privacy Rules ("CBPR") program. A company represented on its website that it was a certified participant in the self-regulatory program but was not actually certified. Following this, the FTC issued warning letters to 28 companies that claimed to be certified participants in the APEC CBPR program but did not appear to have met the requirements for certification.

Legislative—Federal

Lawmakers Oppose FCC's Proposed Internet Privacy Rules
On May 11, in a hearing before the Senate Judiciary Committee's subcommittee on Privacy, Technology and the Law, the FCC faced criticism over the agency's decision to draft specific privacy rules for internet service providers. The privacy proposal would place limits on providers' use and sharing of certain customer data, while requiring that they notify affected customers within 10 days of discovering a data breach. On July 7, the

House voted 239–185 to approve an appropriations bill that included a provision preventing the FCC from moving ahead with its plan.

House Criticizes FDIC's Data Breach Prevention and Response Efforts
On July 12, the House Committee on Science, Space, and Technology publicized an internal report detailing data breach prevention and response failures by the Federal Deposit Insurance Corporation ("FDIC").

Legislative—States

Vermont and Illinois Limit Law Enforcement Surveillance
On June 6, the Vermont governor signed S.B. 155 into law, which limits warrantless surveillance and prohibits law enforcement officers from obtaining data from service providers absent a warrant or court-issued subpoena. The bill specifically limits the use of drones by law enforcement personnel. The bill becomes effective on October 1. On June 16, the Illinois General Assembly sent S.B. 2343 to the governor for enactment. The bill would place restrictions on Illinois law enforcement agencies' use of stingray or cell site simulator devices.

Ten States Enact Student Data Privacy Bills in First Half of 2016
Since March, at least 10 states—Arizona, Connecticut, Colorado, Hawaii, Kansas, New Hampshire, Tennessee, Utah, Virginia, and West Virginia—have added laws to protect the privacy of students.

- **Arizona**: On May 18, the Arizona governor approved H.B. 2088, which requires informed consent before children can be subjected to invasive surveys. The bill requires schools to obtain written informed consent from parents before administering any survey that solicits personal information from students. The bill became effective on August 6.
- **Connecticut**: On June 9, the Connecticut governor signed into law H.B. 5469, which requires businesses that collect and maintain educational records to take steps to safeguard student data and to refrain from using it for targeted advertising purposes. The bill is specifically targeted at educational software and services contractors, as well as website, online services, and mobile applications operators. The bill becomes effective on October 1.
- **Colorado**: On June 10, the Colorado governor signed H.B. 1423, which adds to the existing Colorado laws pertaining to student data security by adopting additional duties with which the state Board of Education, Department of Education, school districts, boards of cooperative services, and charter schools must comply to increase the transparency and security of student information. The bill became effective on August 10.
- **Hawaii**: On May 2, the Hawaii governor signed S.B. 2607 into law, which limits the ways in which the operator of a website, online service, online application, or mobile application working with the Department of Education can use student data. The bill took effect upon its approval.
- **Kansas**: On May 6, Kansas enacted H.B. 2008, which creates the Student Online Personal Protection Act. The bill prohibits an operator of an educational online product from knowingly engaging in targeted advertising on the operator's educational online product, using information to create a profile about the student, selling or renting student information to a third party, and disclosing student information, except as provided. The law became effective on July 1.
- **New Hampshire**: On May 5, the New Hampshire governor signed H.B. 1497 into law, which requires school districts to destroy personal information of students following the completion and verification of certain tests and gives students taking college entrance exams the option to have all of their personal information destroyed by the testing entity following the completion and verification of the test. The bill became effective on July 4.
- **Tennessee**: On April 12, the Tennessee governor signed H.B. 1931 into law, which prohibits an operator of an internet website, service, or application primarily used for K–12 school purposes from engaging in targeted advertising

based on any information the operator acquired because of the website, service, or application, using information created or gathered by the operator's site, service, or application to create a profile about a student except in furtherance of K–12 school purposes, and selling or renting a student's information. The bill became effective on July 1.

- **Utah**: On March 23, the Utah governor signed H.B. 358 into law, which enacts the Student Data Privacy Act, provides for student data protection governance at the state and local levels, enacts requirements for data protection and maintenance by state and local education entities and third-party contractors, provides for penalties, and enacts a requirement for notice given to a parent or guardian before a student is required to take a certain type of survey. The bill became effective on May 10.
- **Virginia**: On March 11, the Virginia governor signed H.B. 749, which makes several changes to the provisions relating to the protection of student personal information by school service providers, including defining targeted advertising and clarifying that other provisions of law do not prohibit school service providers from performing certain acts, including disclosing student personal information to ensure legal or regulatory compliance. The bill became effective on July 1.
- **West Virginia**: On March 25, the West Virginia governor signed H.B. 4261 into law, which prohibits the West Virginia Department of Education from transferring confidential student information or certain redacted data to any federal, state, or local agency or other person or entity (subject to certain exceptions); allows the ACT or the College Board to use certain information; requires written consent if information classified as confidential is necessary; and requires that the consent contain a detailed list of the confidential information required and the purpose of its requirement. The bill became effective in June.

Data Breach Notification Statute Amendments Take Effect in July and August
Data breach notification requirements in Arizona, Nebraska, and Tennessee took effect in July and August.

- On July 1, Tennessee S.B. 2005 took effect, which amends Tennessee's breach notification law to require notification of a breach even if the personal information involved in the breach was encrypted. The law was further amended to include employees of the information holder as "unauthorized persons" and requires disclosure of the breach no later than 45 days from the discovery or notification of the breach.
- On July 20, Nebraska L.B. 835 took effect, which amends Nebraska's Consumer Notification of Data Security Breach Act. The bill amended the definition of "personal information" to include a user name or email address in combination with a password or security question and answer, requires notice to the Nebraska Attorney General, and lays out an exception to the exemption for encrypted data.
- On August 6, Arizona H.B. 2363 took effect, which amends Arizona's data breach law to ensure it does not apply to business associates of covered entities as defined under regulations implementing HIPAA.

The following Jones Day lawyers contributed to this section: Jeremy Close, Jay Johnson, Alexandra McDonald, Dan McLoon, Kelly Ozurovich, Mauricio Paez, Nicole Perry, Alexa Sendukas, John Sullivan, and Anand Varadarajan.

[Return to Top]

Latin America

Brazil

Court Orders Nationwide Suspension of WhatsApp Application
On May 2, a state judge from the State of Sergipe granted a preliminary injunction

ordering a 72-hour suspension of WhatsApp (source document in Portuguese) in order for law enforcement to obtain information regarding organized crime and drug trafficking allegations. The suspension lasted only 24 hours (source document in Portuguese) because WhatsApp filed an appeal with Sergipe's Court of Appeals, which vacated the order.

Brazilian Civil Rights for Internet Framework Takes Effect
On May 11, Decree No. 8,771 (source document in Portuguese), an executive order regulating the Brazilian Civil Rights Framework for the Internet (source document in Portuguese), became effective. The decree regulates procedures for internet service providers and application service providers regarding data storage and protection, internet data package discrimination and traffic degradation, standards for investigation of criminal offenses, and transparency measures concerning data record requests by governmental authorities.

Brazilian Congress Considers Data Privacy Bill
On May 13, the Brazilian Federal Executive Branch introduced Bill of Law No. 5,276/2016 (source document in Portuguese) to the Brazilian Congress. The proposed legislation addresses consent for personal data management, international data transfers, government collection of data for public policy, and administrative penalties for violations. The bill also provides that the National Data Protection Agency will be created to oversee compliance with data privacy laws.

ANATEL Announces Changes on Regulations
On June 24, the Brazilian National Telecommunications Agency ("ANATEL") announced changes to its regulatory agenda (source document in Portuguese) for the rest of 2016. ANATEL decided to define a new telecommunications regulatory framework and announced that it will open public consultations to reassess the scope of telecommunication services in Brazil and the model of granting operating licenses.

Chile

Chilean President Announces New Legislation for Technology Sector
On May 21, Chile's president announced (source document in Spanish) that Chile's Congress would soon consider legislation regarding the creation of a Ministry of Science and Technology to oversee developments in Chile's technology sector. She also stated that another bill would create an organization to update Chile's data privacy regulation in line with the European Union's privacy standards.

Colombia

Colombia Hosts International Conference on Data Protection
On June 9 and 10, the City of Santa Marta in Colombia hosted the 4th International Conference on Data Protection and the 15th Iberoamerican Meeting on Data Protection. Discussion topics included changes in privacy environment; data breach incidents; national security, private sector data, and individual control via encryption; and social network and observational data. The conference hosted authorities from Mexico, Spain, Colombia, Peru, Uruguay, Argentina, and Chile.

Mexico

INAI Proposes Data Protection Iberoamerican Regional Agreement
On June 8, the National Institute for Transparency, Access to Information and Personal Data Protection ("INAI") issued a press release (source document in Spanish) on creating a Regional Agreement and a Case Law Platform on data protection matters. The Regional Agreement would set the minimum standards for countries in the region to maintain data privacy. The Case Law Platform would integrate databases containing international and local case law and policy documents related to privacy matters, private life, habeas data,

and protection of personal data.

INAI Creates Data Protection Innovation and Best Practices Contest
On June 10, INAI issued a statement inviting data controllers and data processors in Mexico to submit applications for the Award for Innovation and Best Practices on Protection of Personal Data (source document in Spanish). The award will recognize best practices developed by public and private companies as well as individuals in charge of processing of personal data, as measured against Mexico's Federal Law for the Protection of Personal Data Held by Private Parties, and Federal Law of Transparency and Access to Information.

INAI Issues Guide for the Secure Deletion of Personal Data
On July 14, INAI issued the Guide for the Secure Deletion of Personal Data (source document in Spanish), which provides methods for the effective deletion of personal data from documents, files, or devices in the public and private sectors. The Guide advises data controllers on legal criteria and best practices for safe destruction, removal, and deletion of such information.

The following Jones Day lawyers contributed to this section: Daniel C. D'Agostini, Mónica Peña Islas, Guillermo E. Larrea, and Elie J. Sherique.

[Return to Top]

Europe

European Union

Advocate General Asks EU Court of Justice to Consider Dynamic IP Addresses as Personal Data
On May 12, Advocate General Campos Sanchez-Bordona released an opinion in *Patrick Breyer v. Germany Federal Republic* (C-582/14). According to the opinion, a dynamic IP address constitutes personal data within the meaning of Directive 95/46/EC when an internet service provider has other data that, when linked to the dynamic IP address, facilitates identification of the user.

EU and U.S. Sign Law Enforcement "Umbrella" Agreement
On June 2, the European Commission issued a press release on the "Umbrella" agreement between the EU and U.S. The agreement sets standards for the protection of personal data transferred by law enforcement authorities and enhances individual rights.

Commission Publishes Cybersecurity Fact Sheet
On July 5, the European Commission released a fact sheet on tackling cyber threats. The Commission proposed an action plan to strengthen Europe's cyber resilience because of constantly evolving cyber threats that could potentially cause a large-scale cyber incident or harm data protection, trade secrets, and the digital economy.

European Trade Secrets Directive Takes Effect
On July 5, Directive (EU) 2016/943 took effect, providing for common measures against the unlawful acquisition, use, and disclosure of trade secrets. The new instrument protects companies against industrial and economic espionage without undermining fundamental rights and freedoms of the public interest, such as public safety, consumer protection, public health, environmental protection, and mobility of workers. Member States have two years to transpose the Directive into their national laws.

European Parliament Adopts EU Cybersecurity Directive
On July 6, the European Parliament adopted the EU Network and Information Security Directive ("NIS Directive") to achieve a common level of network security and information systems within the EU. The new instrument provides for EU-wide rules on cybersecurity

and organizes the cybersecurity cooperation between Member States. The NIS Directive took effect in August, and Member States have 21 months to transpose the Directive into their national laws.

European Commission Adopts Privacy Shield
On July 12, the Commission adopted the Privacy Shield to provide a new framework for transatlantic exchanges of personal data for commercial purposes. According to a statement made by Vice-President Ansip and Commissioner Jourová, the final version imposes clear and strong obligations on companies handling data; ensures that U.S. access to personal data for law enforcement and national security will be subject to clear limitations, safeguards, and oversights; and protects fundamental rights. Certification under the Privacy Shield took effect on August 1. For more information, please see the corresponding Jones Day *Alert*.

European Court of Justice Rules on Jurisdiction Criteria in Article 4(1)(a) EU Data Protection Directives
On July 28, the European Court of Justice issued a decision in *VKI v. Amazon EU*, holding in part: "while the fact that the undertaking responsible for the data processing does not have a branch or subsidiary in a Member State does not preclude it from having an establishment there within the meaning of Article 4(1)(a) of Directive 95/46, such an establishment cannot exist merely because the undertaking's website is accessible there." The decision followed an action for an injunction brought by VKI against Amazon EU.

Article 29 Working Party

Article 29 Working Party Issues Opinion on Publication of Personal Data for Transparency Purposes
On June 8, the Article 29 Working Party adopted an opinion explaining how to apply data protection principles to the processing and publication of personal data for transparency purposes in the public sector, especially as it relates to anti-corruption measures and the prevention of conflicts of interests.

European Data Protection Supervisor

EDPS Presents 2015 Annual Report
On May 24, the European Data Protection Supervisor ("EDPS") presented its annual report. The report focuses on the successful implementation of new rules under the GDPR, reaching agreements on Regulation 45/2001, and the ePrivacy Directive closing the data protection package.

EDPS Comments on EU–U.S. Privacy Shield
On May 30, the EDPS released an opinion to present practical solutions to address concerns raised by the EU–U.S. Privacy Shield. The EDPS emphasized that the EU–U.S. Privacy Shield is not robust enough to replace the U.S.–EU Safe Harbor Framework and to withstand future legal scrutiny before the European Court of Justice.

European Network and Information Security Agency

ENISA Publishes Report on Cloud Incidents
On June 1, the European Network and Information Security Agency ("ENISA") issued a report on the current status of forensic analysis techniques and processes of cloud incidents. The report aims to "identify and analyze the current technical, legislative, organizational challenges or any other kind of limitations that could hamper a sufficient and seamless investigation of cloud incidents."

ENISA Analyzes Security and Privacy Standards for SMEs
On June 17, ENISA published a study showing that, despite rising concerns on information security risks, the level of information security and privacy standard adoption for small

and medium enterprises ("SMEs") is low. The report discusses the drivers for the trend and the barriers to widespread adoption of security and privacy standards for European SMEs.

Belgium

Privacy Commission Recommends Reliable Third Party to Process Judicial Data to Comply with Foreign Anti-Bribery Laws
On June 8, the Privacy Commission issued a recommendation (source document in French and Dutch) on how to process judicial data to comply with foreign anti-bribery obligations. The Commission recommended using a reliable third party, such as law firms, to do anti-bribery prior checks of commercial partners.

Brussels Court of Appeal Annuls Interim Decision on Use of Cookies by Social Media Platform
On June 29, the Court of Appeal of Brussels struck down (source document in French and Dutch) a lower court's interim decision barring a social network company from using cookies. The Court of Appeal noted that Belgian courts do not have jurisdiction over foreign companies and held that there was no urgency justifying the interim relief procedure. The main proceedings remain pending before the lower court.

Privacy Commission Refuses Transfer of Biometric Data to U.S. Authorities
On June 29, the Privacy Commission published an opinion (source document in French and Dutch) denying the U.S. embassy's request to obtain from Belgian authorities the biometric data of four individuals subject to EU sanctions. The Commission held that such transfer must be justified by specific legislation, which does not include the public interest exception under the Belgian Privacy Law.

France

French Supreme Court Limits Right to Object
On May 12, the French Supreme Court ruled (source document in French) that a request to remove a name and surname from the title of a press article exceeded the Right to Object and unduly restricted the freedom of the press.

CNIL Communicates Priority Topics of 2016 Controls Program
On May 12, the French Data Protection Authority ("CNIL") published an article (source document in French) stating that more than 400 controls will be carried out in 2016. A quarter of the controls correspond to key areas identified by the program: the national system of health insurance information, the system of flight passenger information, and data brokers.

French Supreme Court Rejects Personal Data Protection for Legal Entities
On June 29, the French Supreme Court (*Cour de cassation*) issued a decision (source document in French) holding that only natural persons can invoke a breach of their privacy within the meaning of Article 9 of the Civil Code. Although French judges previously held that legal entities could benefit from some privacy attributes, the French Supreme Court refused to extend such protection and to recognize a general right to privacy for legal entities.

CNIL Orders Software Company to Comply with French Data Protection Law
On June 30, CNIL issued a formal injunction (source document in French) ordering Microsoft to stop collecting excessive and irrelevant personal data and tracking the users' browsing without their consent. The order also requires Microsoft to ensure the security and confidentiality of users' personal data.

CNIL Analyzes Impact of Digital Republic Bill on Personal Data Protection
On July 7, CNIL published its analysis (source document in French) on how the Digital

Republic Bill affects CNIL and the rights of data subjects. The report discusses the systematic involvement of CNIL in future privacy legislation, increased financial sanctions, a new right to be forgotten for minors, and the concept of "informational self-determination." The bill will take effect in October.

CNIL Sanctions Company for Breaches of French Data Protection Law
On July 7, the CNIL fined (source document in French) Brandalley €30,000 for multiple breaches of French data protection laws. Violations included: failure to request credit card fraud authorizations from CNIL; failure to set up a data retention period for clients' data; and failure to implement sufficient measures to ensure the security and confidentiality of internet users' personal data.

Germany

Bavarian DPA and Data Protection Commissioner Publish Joint Guideline for Commissioned Data Processing in Bavarian Hospitals
In June, the Bavarian Data Protection Authority ("DPA") and the Bavarian Data Protection Commissioner published a joint guideline (source document in German) regarding the use of external providers in hospitals. The guideline discusses how to ensure that commissioned data processing (*Auftragsverarbeitung*) complies with data protection requirements, such as Article 27 of the Bavarian Act on Hospitals.

Bavarian DPA Interprets GDPR Provisions
On June 10, the Bavarian DPA began interpreting the GDPR. The papers cover Article 32 GDPR (security of processing), Article 42 GDPR (certification), and video surveillance (all source documents in German), and they address how these provisions relate to the German Federal Data Protection Act (*Bundesdatenschutzgesetz*).

Federation of German Consumer Organizations Warns Pokémon Go Developer
On July 20, the Federation of German Consumer Organizations (*Verbraucherzentrale Bundesverband*) issued a press release (source document in German) regarding privacy concerns relating to 15 provisions in the terms of use and the privacy policy of the Pokémon Go app. The press release and letter to the app developer addressed concerns regarding liability and warranty disclaimers and the discretionary disclosure of personal data of users to third parties.

Italy

Italian DPA Adopts Proactive Approach for Protecting Consumer Data
On June 28, the Italian DPA published its 2015 annual report (source document in Italian). The DPA discussed the risks related to cyber crimes, data breach notification requirements, sanctions issued in 2015, and data privacy inspections in 2015.

Russia

Russian Parliament Adopts New Legislation on Massive Telecoms Surveillance
In June, the Russian parliament adopted amendments to counterterrorism laws and public security measures, many of which affect the technology sector. Among other requirements, the amendments oblige communication service providers to store in Russia all information on their customers' and internet users' communications and messages for specified periods and disclose any data to Russian law enforcement authorities upon their request. For more information, please see the corresponding Jones Day *Alert*.

Spain

DPA Publishes 2015 Annual Report
On June 21, the Spanish DPA published its 2015 annual report (source document in Spanish). The DPA reported that key issues in 2015 related to irregular procurement and

credit blacklist files, and citizen complaints increased by more than 15 percent due to the right to be forgotten judgment issued by the European Court of Justice in 2014. According to the report, telecommunications companies were the most sanctioned companies for data protection violations in Spain.

DPA Holds Annual Open Meeting
On June 29, the Spanish DPA held the annual open meeting (source document in Spanish), during which it explained the new features of the GDPR and confirmed that a new Spanish data protection bill similar to the GDPR will be submitted in the first quarter of 2017.

DPA Releases Guidelines on GDPR
On June 29, the Spanish DPA issued guidelines regarding practical implications of the GDPR (source document in Spanish). The document provides recommendations for companies regarding new obligations and requirements established by the GDPR.

The Netherlands

DDPA Issues Report on Delisting Search Results [Google]
On May 25, the Dutch Data Protection Agency ("DDPA") published an overview of requests it had received to remove personal information from search engines since July 2014. The overview tracks the number of requests, mediations, takedowns, and site misinterpretations relating to the delisting process.

DDPA Alerts Shops and Municipalities on Conditions for Wi-Fi Tracking
On June 16, the DDPA notified (source document in Dutch) local governments and stores on the requirements applicable to Wi-Fi tracking. According to the DDPA, tracking information may be retained by stores for 24 hours only, after which it must be destroyed or irreversibly anonymized. In the public domain, tracking data needs to be irreversibly anonymized immediately upon collection.

Hospital Websites User Tracking Violates Dutch Law
On June 23, the DDPA determined (source document in Dutch) that nearly 50 percent of Dutch hospital websites transfer visitors' data to third parties by using tracking cookies in violation of Dutch law. The DDPA has notified hospitals and will re-examine hospital websites in six weeks.

United Kingdom

UK Parliament Reports on Online Data Security
On June 15, the Culture, Media and Sport Committee reported on cybersecurity and incident readiness and made a series of recommendations for the Information Commissioner's Office ("ICO"). The committee called for custodial sentences for those convicted of unlawfully obtaining personal data.

UK ICO Holds GDPR Relevant
On July 7, the ICO stated that the GDPR will continue to be relevant to UK business irrespective of the referendum vote to leave the EU.

The following Jones Day lawyers contributed to this section Jérémy Attali, Laura Baldisserra, Paloma Bru, Laurent De Muyter, Bénédicte Graulle, Jan Grootenhuis, Olivier Haas, Jörg Hladjk, Bastiaan Kout, Jonathon Little, Martin Lotz, Giuseppe Mezzapesa, Evgenia Nosareva, Selma Olthof, Undine von Diemar, and Sergei Volfson.

[Return to Top]

Asia

People's Republic of China

CAC Issues Rules for Search Providers
On June 25, the Cyberspace Administration of China ("CAC") published the Provisions on the Administration of Internet Information Search Services (source document in Chinese). Some provisions require search providers to: (i) adopt information security management systems to ensure the real-time inspection of information by relevant government agencies and protection of personal data; (ii) refrain from posting obscene content; (iii) block any search results prohibited by laws and report them to the CAC; and (iv) establish comprehensive regulatory systems for public complaints and reports.

CAC Issues Rules for Mobile Internet Providers
On June 28, the CAC published Provisions on the Administration of Information Services of Mobile Internet Application Programs (source document in Chinese). Under the provisions, mobile providers must verify the mobile phone numbers or other identity information of any new mobile providers, impose sanctions for users who publish content that violates applicable laws, respect and protect intellectual property rights, and record user logs and store them for at least 60 days.

China Considers Second Draft of Cybersecurity Law
On July 5, the Standing Committee of the National People's Congress published the full Second Draft of the Cybersecurity Law (source document in Chinese) ("Draft"). Major features of the Draft include establishing sanctions, a proposal for data anonymization for big data activities, and requiring that network operators cooperate with state surveillance authorities. The Draft also discusses requirements to obtain individual consent for the handling of personal data and circumstances for cross-border transfer of personal data.

Hong Kong

PCPD Publishes Media Statement on Online Shopping
On June 21, the Office of the Privacy Commissioner for Personal Data ("PCPD") published a media statement (source document in Chinese) alerting the public to stay smart when shopping online and reminding organizations operating online businesses to keep up to date with the latest technological developments and to strengthen their network security measures.

PCPD Publishes New Guidance Note on Handling Personal Data for Beauty Industry
On June 26, PCPD issued the Guidance on the Proper Handling of Customers' Personal Data for the Beauty Industry in response to major complaints against the beauty sector. The guidance note examines the unique business features and practices in the beauty industry and sets out best practices to maintain compliance with the Personal Data (Privacy) Ordinance.

Japan

Personal Information Protection Commission Releases Draft Cabinet Order and Regulations for Public Comments
On August 2, the Personal Information Protection Commission released (source document in Japanese) a draft cabinet order and a draft enforcement regulation for public comments. The draft cabinet order defines the term "Individual Identification Code" as one category of personal information and lists DNA data, finger or palm print data, passport number, or basic pension code as Individual Identification Codes. The draft regulation provides rules for creating and using De-Identified Information and safeguards for extraterritorial data transfer. Public comments are due on August 31.

Ministry of Economy, Trade and Industry Publishes Manual for Creation of De-Identified Information

On August 8, the Ministry of Economy, Trade and Industry ("METI") published Reference Materials to Consider Methods to Create De-Identified Information (source document in Japanese). Given the utilization of big data for the creation and promotion of new services and industry, METI prepared the manual as guidance for the industry to create De-Identified Information under the new rules established under the amended Personal Information Protection Act.

Singapore

PDPC Imposes Fine for Personal Data Disclosure
On July 21, the Personal Data Protection Commission ("PDPC") imposed a $5,000 fine on Toh-Shi Printing Singapore for its failure to implement proper and adequate verification procedures while processing personal data on behalf of another company. The incident resulted in the unauthorized disclosure of personal data relating to 195 individuals.

Taiwan

Ministry of Justice Issues Medical Information Collection Exception
On July 4, the Ministry of Justice announced (source document in Chinese) that the government may collect medical, medical treatment, genetic information, sexual life, health examination, and criminal records without obtaining prior written consent for purposes of family violence prevention.

The following Jones Day lawyers contributed to this section: Li-Jung Huang, Chiang Ling Li, Michiru Takahashi, Richard Zeng, and Grace Zhang.

[Return to Top]

Australia

Australia Releases Guide to Big Data and Australian Privacy Principles
In May, the Office of the Australian Information Commissioner ("OAIC") released a consultation draft guide to big data and the Australian Privacy Principles. The guide provides guidance on how to facilitate big data activities while ensuring the protection of personal information and addresses big data privacy challenges such as notice and consent, data collection, retention minimization, and use limitation. The OAIC is currently accepting feedback on the draft.

OAIC Resumes Investigation of FOI Complaints
As of July 1, 2016, OAIC resumed the investigation of complaints involving agency actions relating to the handling of Freedom of Information ("FOI") matters. Since November 2014, the Commonwealth Ombudsman had been assigned FOI complaints following the Australian government's decision to abolish the OAIC and the associated reduction in OAIC resources. However, the government's 2016–2017 budget allocated A$37 million over the next four years to fund OAIC's privacy and FOI regulatory functions, allowing it to review FOI complaints moving forward. The Commonwealth Ombudsman will retain all complaints it is currently overseeing.

The following Jones Day lawyers contributed to this section: Adam Salter, Peter Brabant, Nicola Walker, and Madeleine Harkin.

[Return to Top]

Jones Day Cybersecurity, Privacy, and Data Protection Lawyers

Emmanuel G. Baud
Paris

Walter W. Davis
Atlanta

John E. Iole
Pittsburgh

J. Todd Kennard
Columbus

John M. Majoras
Columbus/Washington

Daniel J. McLoon
Los Angeles

Chaka M. Patterson
Chicago

Adam Salter
Sydney

Rhys Thomas
London

Toru Yamada
Tokyo

Bénédicte Graulle
Paris

Guillermo E. Larrea
Mexico City

Jérémy Attali
Paris

Jeremy Close
Irvine

Steven G. Gersten
Dallas

Aaron M. Healey
Columbus

Evgenia Nosareva
Paris

Brandy H. Ranjan
Columbus

John T. Sullivan
Dallas

Natalie Williams
Atlanta

Po-Chien Chen
Taipei

Timothy P. Fraelich
Cleveland

Robert W. Kantner
Dallas

Ted-Philip Kroke
Frankfurt

Todd S. McClelland
Atlanta

Caroline N. Mitchell
San Francisco

Nicole M. Perry
Houston

Gregory P. Silberman
Silicon Valley

Michael W. Vella
Shanghai

Sidney R. Brown
Atlanta

Olivier Haas
Paris

Christopher J. Lopata
New York

Laura Baldisserra
Milan

Daniel C. D'Agostini
São Paulo

Bart Green
Irvine

Bastiaan K. Kout
Amsterdam

Selma Olthof
Amsterdam

Jessica M. Sawyer
Los Angeles

Raquel Travesí
Madrid

Shawn Cleveland
Dallas

Joshua L. Fuchs
Houston

Elena Kaplan
Atlanta

Jonathan Little
London

Kristen P. McDonald
Atlanta

Matthew D. Orwig
Dallas

Jeff Rabkin
San Francisco

Cristiana Spontoni
Brussels

Sergei Volfson
Moscow

Paloma Bru
Madrid

Jörg Hladjk
Brussels

Margaret I. Lyle
Dallas

Peter Brabant
Sydney

Jennifer C. Everett
Washington

Jan Grootenhuis
Amsterdam

Martin Lotz
Munich

Kelly M. Ozurovich
Los Angeles

Alexa L. Sendukas
Houston

Anand Varadarajan
Dallas

James A. Cox
Dallas

Karen P. Hewitt
San Diego

Jeffrey L. Kapp
Cleveland

Kevin D. Lyles
Columbus

Carmen G. McLean
Washington

Mauricio F. Paez
New York

Elizabeth A. Robertson
London

Michiru Takahashi
Tokyo

Undine von Diemar
Munich

Laurent De Muyter
Brussels

Jay Johnson
Dallas

Giuseppe Mezzapesa
Milan

Nigel Chin
Singapore

Adrian Garcia
Dallas

Joshua M. Grossman
New York

Alexandra A. McDonald
San Francisco

Mónica Peña Islas
Mexico City

Elie J. Sherique
São Paulo

Nicola Walker
Sydney

Follow us on: 

Jones Day is a legal institution with more than 2,500 lawyers on five continents. We are One Firm Worldwide[SM].