JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 13 | March 2017

JONES DAY

Jones Day Cybersecurity, Privacy & Data Protection Attorney Spotlight: Mauricio F. Paez

While cybersecurity and data protection laws continue to develop in the United States and around the world, they trail behind more rapid advancements in industrial internet of things ("IoT"), cognitive and other artificial intelligence, cloud 2.0, mobility, and other technologies.

Navigating this evolving and complicated area of law poses a significant challenge for global businesses, which are concerned with ineffective national cybersecurity policy approaches, the rise of data localization and other information/infrastructure sovereignty policies around the world, restrictions on international data flows, protectionist approaches to the use of global cloud services, IoT technologies, remote IT services, and regulatory and liability uncertainty.

Mauricio Paez, a New York-based partner in Jones Day's Cybersecurity, Privacy & Data Protection Practice, has been helping companies, for more than 18 years, address and respond to these cybersecurity and privacy challenges in the United States and abroad. He assists companies with U.S. and global cybersecurity and data privacy

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

compliance; cybersecurity and privacy diligence in corporate transactions; enterprise cyber risk management; and breach preparedness, response, and crisis management.

He also advises on handling internal data breach investigations; supervising forensic examinations and coordinating with law enforcement in investigations of criminal attacks; and regulatory investigations and enforcement actions by the FTC and HHS/OCR. In addition, Mauricio has significant experience advising clients on cybersecurity and privacy legal issues related to new product development and business initiatives, such as connected and driverless vehicles, smart cities, smart-grid, industrial internet applications and services, "big data" applications and analytics, machine learning and data rights, medical devices, and consumer IoT products.

United States

Regulatory—Policy, Best Practices, and Standards

New York Department of Financial Services Relaxes Cybersecurity Proposal
On December 28, 2016, the New York Department of Financial Services ("DFS") released a revised version of a proposed regulation that would require banks, insurance companies, and other financial services institutions regulated by the DFS to adopt broad cybersecurity protections. The revised draft pushes back the effective dates and compliance deadlines, adds limited exemptions, narrows the requirement to notify the DFS of cybersecurity events, adds flexibility to the program's requirements, and narrows certain definitions, among other changes.

New York Attorney General Issues Consumer Alert on Major Data Breach
On December 15, 2016, New York Attorney General Eric Schneiderman issued a consumer alert urging all New Yorkers to take immediate steps to protect their personal information following a data breach of a major online search engine, which compromised the data of 500 million users. The press release notes that the Attorney General's office is communicating with the company regarding the circumstances of the breach and disclosure to law enforcement.

SEC OCIE Includes Cybersecurity in 2017 Examination Priorities
On January 12, 2017, the Security and Exchange Commission's ("SEC") Office of Compliance

RECENT AND PENDING SPEAKING ENGAGEMENTS

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

Client Confidentiality in the Digital Age, Texas District & County Attorneys Association Civil Law Seminar, San Antonio, TX (May 12) **Jones Day Speakers: Jason Varnado, Nicole Perry**

Eliminating the Weakest Link: Cybersecurity for Lawyers, Moms in Law Luncheon, Houston, TX (May 10) **Jones Day Speaker: Nicole Perry**

Enforcing Intellectual Property Rights in the United States, Lone Star Strategies for IP in China—What Texas Companies Need to Know Now, Texas Regional United States Patent and Trademark Office, Dallas, TX (May 2). **Jones Day Speaker: Jay Johnson**

New Trends on Cybersecurity, Conference with American Chamber of Commerce, Madrid, Spain (May). **Jones Day Speaker: Paloma Bru**

Q&A with the SEC on Agency Expectations for Consumer Privacy and Cybersecurity, International Association of Privacy Professionals, 2017 Global Privacy Summit, Washington, D.C. (Apr. 20). **Jones Day Speaker: Jay Johnson**

The Digital Criminal: Cyber Crime Trends and Enforcement, Boston College, Boston, MA (Apr. 10). **Jones Day Speaker: Lisa Ropple**

GDPR in Detail—Analysis of DPA Guidance and National Implementation Efforts, Jones Day webinar (Apr. 5). **Jones Day Speakers: Various**

The EU Cybersecurity Directive—What Do the New Rules Mean for Business?, 10th Annual GDD Seminar Data Protection International, Berlin, Germany (Apr. 3). **Jones Day Speaker: Jörg Hladjk**

The Local Developments of the GDPR, Madrid, Spain (Apr.). **Jones Day Speaker: Paloma Bru**

Health Care Cybersecurity Symposium, North Texas Crime Commission, Fort Worth, TX (Mar. 31). **Jones Day Speaker: Jay Johnson**

Inspections and Examinations ("OCIE") issued its 2017 examination priorities. These priorities represent practices, products, and services that the OCIE perceives to present potential heightened risks to investors or the markets. As part of its 2017 priorities, the OCIE stated that it would continue its initiative to "examine for cybersecurity compliance procedures and controls."

Report Shows Credit Card Fraud Shifts from In-Store to Online
On February 1, 2017, Javelin Strategy and Research reported that the use of stolen card data to pay for merchandise on websites, in mobile apps, and via telephone increased by 40 percent in 2016. In turn, this shift has forced retailers with online sales to enhance online security because the increased use of chip technology in credit cards reduced in-person fraud in retail stores, driving credit card fraud online.

Regulatory—Critical Infrastructure

NIST Releases Guide to Help Organizations Recover from Cybersecurity Incidents
On December 22, 2016, the National Institute of Standards and Technology ("NIST") published the Guide for Cybersecurity Event Recovery to assist organizations in recovering from cybersecurity incidents. The guide consolidates existing NIST recovery guidance on incident handling and contingency planning and provides a process each organization can use to create its own comprehensive recovery plan. The publication supplies tactical and strategic guidance for developing, testing, and improving recovery plans, as well as examples of playbooks to handle data breaches and ransomware.

NIST Updates Cybersecurity Framework
On January 10, 2017, NIST released a draft update to its *Framework for Improving Critical Infrastructure Cybersecurity*. The update provides new details on managing cyber supply-chain risks, clarifies key terms, and introduces measurement methods for cybersecurity. The framework is intended to provide voluntary guidance to organizations to reduce cybersecurity risks.

Regulatory—Retail

FTC Settles Deceptive Consumer Tracking Charges with Digital Advertising Company
On December 20, 2016, the FTC settled with a digital advertising company regarding charges that the company deceived consumers by tracking them online and through mobile applications, even after consumers opted out of such tracking. According to

How to Develop a GDPR Compliance Program, Jones Day webinar (Mar. 22). **Jones Day Speakers: Various**

Introduction to the GDPR—Top 10 Implementation Issues for Companies, Jones Day webinar (Mar. 15). **Jones Day Speakers: Various**

Governance, Risk Management & Compliance, The First Boston Conference on Cybersecurity, Boston, MA (Mar. 8). **Jones Day Speaker: Lisa Ropple**

Building Resilient Organizations Through Cyber Wargaming—A Legal Perspective, Jones Day and Deloitte webinar (Mar. 7). **Jones Day Speakers: Todd McClelland, Lisa Ropple**

2017 Cybersecurity Policy Landscape and Practical Implications to Attorneys, Jones Day webinar (Mar. 7). **Jones Day Speakers: Jeffrey Kapp, Mauricio Paez**

Working with Law Enforcement and Government Agencies, Cybersecurity and Data Privacy Law Conference, Institute for Law and Technology, Plano, TX (Jan. 26) **Jones Day Speaker: Jay Johnson**

Cybersecurity Law Primer: An Introduction to the Game, the Players, and the Rules!, Cybersecurity and Data Privacy Law Conference, Institute for Law and Technology, Plano, TX (Jan. 25) **Jones Day Speaker: Jay Johnson**

Client Confidentiality in the Digital Age: Cybersecurity Ethics and Risk Mitigation for Lawyers, Houston Bar Association, Houston, TX (Jan. 12). **Jones Day Speakers: Nicole Perry, Joshua Fuchs**

Cybersecurity and Privacy Litigation Risks, Jones Day University, Columbus, OH (Dec. 6, 2016). **Jones Day Speakers: Jeff Rabkin, Todd Kennard, Richard DeNatale**

Blockchain, Development Institute International Seminar, Paris, France (Dec. 2, 2016). **Jones Day Speaker: Olivier Haas**

RECENT AND PENDING PUBLICATIONS

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

the FTC complaint, the company's privacy policy represented that consumers could block targeted advertising by using their web browser's settings to block or limit cookies. However, the company tracked customers using unique identifiers even after the customers blocked or deleted cookies from websites. The settlement bars the company from misrepresenting the extent of its online tracking and requires an effective opt-out for consumers.

FTC Charges Network Equipment Manufacturer for Inadequate Router and Camera Security
On January 5, 2017, the FTC filed a complaint against a network devices manufacturer and its U.S. subsidiary, alleging that the company's inadequate security measures put consumers' privacy at risk. The FTC alleged that the company failed to take reasonable steps to secure its routers and internet protocol cameras, potentially compromising sensitive information, including live video and audio feeds and files stored on the routers' attached storage devices.

FTC Issues Report on Cross-Device Tracking
In January 2017, the FTC issued a Cross-Device Tracking Report assessing legal challenges associated with cross-device tracking and making recommendations on how to apply privacy and security principles to this new technology. The report outlines industry self-regulatory efforts and encourages companies involved in cross-device tracking to: (i) truthfully disclose tracking to consumers and business partners; (ii) offer consumers choices about how their cross-device activity is tracked; (iii) obtain consumers' affirmative express consent before engaging in cross-device tracking on sensitive topics and regarding geolocation information; and (iv) maintain reasonable security to avoid future unexpected and unauthorized uses of data.

Regulatory—Defense and National Security

Senate Armed Services Committee Creates New Cybersecurity Subcommittee
On January 18, 2017, Senate Armed Services Committee Chairman John McCain and Ranking Member Jack Reed announced that Senator Mike Rounds of South Dakota would chair a new Subcommittee on Cybersecurity. The new subcommittee was first announced on January 4, 2017, and will be tasked with oversight and legislation for policies and programs relating to the Defense Department's cyber forces and capabilities.

DHS Proposes Rule on Treatment of Controlled Unclassified Information
On January 19, 2017, the Department of Homeland Security ("DHS") issued a proposed rule that would apply the same requirements for safeguards to both

International Data Transfers Based on an Adequacy Decision Under the EU GDPR, DuD pp. 77-79 (Feb.) **Jones Day Author: Jörg Hladjk**

A New Swiss–U.S. Privacy Shield Replaces the U.S.–Swiss Safe Harbor, Jones Day Publications (Jan.). **Jones Day Authors: Various**

ePrivacy—European Commission Tries to Catch Up with the Evolution of Modern Communication Technologies, Jones Day Publications (Jan.). **Jones Day Authors: Undine von Diemar**, **Mauricio Paez**, **Jörg Hladjk**, **Laurent De Muyter**, **Martin Lotz**

Règlement Général sur la Protection des Données, Guide de Poche—General Data Protection Regulation Guide (French translation) (Jan.). **Jones Day Authors: Olivier Haas**, **Hatziri Minaudier**

Guía Del Reglamento General de Protección de Datos, General Data Protection Regulation Guide (Spanish translation) (Jan.). **Jones Day Author: Paloma Bru**

General Data Protection Regulation Guide, Jones Day Publications (Jan.) **Jones Day Authors: Various**

France Unveils its Information System Security Plan in the Health Care Sector, Jones Day Publications (Dec. 2016). **Jones Day Authors: Olivier Haas**, **Cristiana Spontoni**, **Daniel McLoon**, **Mauricio Paez**, **Hatziri Minaudier**

France Moves Forward on Implementation of Cybersecurity Framework for Operators of Critical Infrastructures, Jones Day Publications (Dec. 2016). **Jones Day Authors: Olivier Haas**, **Daniel McLoon**, **Mauricio Paez**, **Undine von Diemar**, **Hatziri Minaudier**

Shorting, Reporting and Profiting in the Era of Cyber Security, *Cyber Security Practitioner* (Dec. 2016). **Jones Day Authors: Todd McClelland**, **Frances Forte**

Federal Banking Agencies Propose Enhanced Cyber Risk Management Standards, Jones Day Publications (Nov. 2016). **Jones Day Authors: Lisa Ledbetter**, **Jennifer Everett**

contractors who run federal information systems and contractors who may obtain controlled unclassified information in the course of working with DHS. DHS also proposed two other rules relating to data security and privacy, one addressing privacy training for DHS contractors and one addressing information technology security awareness training for DHS contractors.

Regulatory—Transportation

DOT Issues Notice of Proposed Rulemaking and Privacy Impact Assessment on V2V Communications
On December 20, 2016, the Department of Transportation ("DOT") National Highway Traffic Safety Administration ("NHTSA") issued a Notice of Proposed Rulemaking and a Privacy Impact Assessment on Vehicle-to-Vehicle ("V2V") communications. In the document, NHTSA discusses how V2V systems will "contain multiple technical, physical, and organizational controls to help limit potential privacy impacts on consumers including those related to vehicle tracking by individuals and government or commercial entities." The proposed V2V system contains three primary components: (i) Basic Safety Messages ("BSMs"); (ii) a method for validating BSMs; and (iii) a communications network. The report also contemplates various privacy controls, including limited transmission radius, no BSM storage, and rotating security credentials.

Regulatory—Financial Services

Financial Technology Industry Group Urges Bank Regulators to Tailor New Cybersecurity Rules to Risk
On January 19, 2017, several financial technology ("fintech") companies created a new industry group, the Consumer Financial Data Rights, to urge the Office of the Comptroller of the Currency, the Federal Reserve Board, and the FDIC to limit regulation of smaller fintech firms. The group aims to: (i) promote the rights of consumers to access and share their financial data and (ii) modify cybersecurity rules to reflect the size of the banking institution.

Regulatory—Health Care/HIPAA

HHS Settles HIPAA Enforcement Action for Lack of Timely Breach Notification
On January 9, 2017, the Department of Health and Human Services ("HHS") settled an enforcement action with a hospital company for lack of timely breach notification. The Resolution Agreement requires that the company revise its existing policies and procedures, conduct training with its employees, and pay a $475,000 fine. HHS found that the company failed to provide timely written breach notifications to individuals whose protected health information had been compromised on multiple occasions.

Litigation, Judicial Rulings, and Agency Enforcements

Dating Site Settles with FTC and 13 States over 2015 Breach of 36 Million Users
On December 14, 2016, the FTC and 13 states settled charges with an online dating site regarding inadequate security measures that resulted in the 2015 breach of 36 million users' account, profile, and billing information. The settlement requires the defendants to implement a comprehensive data security program, including third party assessments, and pay $1.6 million to the FTC and states. The complaint alleges that the defendants misrepresented that they: (i) had taken reasonable steps to ensure that the site was secure; (ii) had received trusted security awards; and (iii) would delete consumer data upon utilization of a "full delete" service.

Kansas Attorney General Sues Company for Failing to Protect Customer's Personal Information
On January 10, 2017, Kansas Attorney General Derek Schmidt filed a lawsuit in Kansas District Court against a document management company and two of its employees for failing to protect customers' personal information. According to the complaint, the company disposed of documents containing personal information, including Social Security numbers, in public trash receptacles. This case represents the first use of the Kansas Attorney General's enhanced data privacy enforcement powers under HB 2460, which was passed by the Kansas Legislature during the 2016 session.

Mississippi Attorney General Files Consumer Protection Act Complaint Against Internet Search Engine
On January 13, 2017, Mississippi Attorney General Jim Hood filed a complaint in Mississippi Chancery Court against an internet search engine alleging violations of Mississippi's Consumer Protection Act. The complaint asserts that the company collected personal information from students using its education portal and then used the data to create advertising profiles.

Ninth Circuit Ruling Applies *Spokeo*
On January 13, 2017, the Ninth Circuit vacated the lower court's decision to decertify a class and dismissed a plaintiff's case against a large furniture retailer, finding that the plaintiff failed to plead the concrete harm necessary under *Spokeo* for standing to bring suit. This case stemmed from allegations that the retailer illegally collected customer zip code data. The appellate panel based its decision on the plaintiff's own concession that she lacked standing in federal court because she had failed to allege more than a bare procedural violation.

Jury Awards $20+ Million in Telemarketing Class Action Trial
On January 19, 2017, a jury awarded $20.5 million in a class action lawsuit against a large satellite service provider. The plaintiffs in this case alleged the service provider made more than 51,000 unwanted telemarketing calls in violation of the Telephone Consumer Protection Act ("TCPA"). The jury awarded $400 for each unwanted call placed by the service provider. The case marks one of the first jury verdicts for a class of consumers alleging Do Not Call violations since the TCPA's enactment.

Ninth Circuit Says Employer Violated FCRA with Liability Waiver
On January 20, 2017, a Ninth Circuit panel reversed the dismissal of a putative class action, which alleged that a subsidiary of an oilfield services company violated the Fair Credit Reporting Act ("FCRA") by improperly placing a liability waiver on its job application disclosure form. The panel noted that the FCRA specifically requires companies to tell applicants if they intend to obtain their consumer report and allow them to refuse. In reversing and remanding the district court's decision, the panel held that the company had willfully violated the statute, subjecting the company to both statutory and punitive damages.

Seventh Circuit Affirms Dismissal of Class Action
On January 20, 2017, the Seventh Circuit affirmed the dismissal of a proposed class action against a large cable TV company, finding the plaintiff had no standing to bring suit under *Spokeo*. The plaintiff brought suit against the cable company for violation of the Cable Communications Policy Act for storing former customers' personal information. The Seventh Circuit held there was no evidence the company had released the personal information or that it planned to do so, and thus found no evidence of cognizable harm.

NY Attorney General Settles with Computer Manufacturer after Data Breach
On January 26, 2017, the New York Attorney General's office announced that a computer manufacturer would pay $115,000 in penalties and overhaul its cybersecurity practices after an ongoing data breach of its website exposed more than 35,000 credit card numbers. Security vulnerabilities found in the company's system included a debugging mode setting that saved all customer data in an unencrypted plain text form and a

website misconfiguration that allowed unauthorized users to view and access information. The settlement also included multiple new security practices, including a designated employee to supervise the privacy and security of personal information, regular testing of safeguards, and annual trainings on data security.

Eighth Circuit Remands Data Breach Settlement to Reassess Class Certification
On February 1, 2017, the Eighth Circuit Court of Appeals remanded a customer data breach litigation to the District Court of Minnesota to further consider class certification. The Eighth Circuit based its decision on an alleged conflict of interest between the named representatives and the remainder of the class.

Television Manufacturer Settles with FTC and New Jersey Attorney General
On February 6, 2017, a global television manufacturer agreed to pay $2.2 million to the FTC and to the Office of the New Jersey Attorney General to settle charges that it installed software on its TVs to collect viewing data on 11 million consumer TVs without consumers' knowledge or consent. According to the complaint, the manufacturer offered a smart interactivity feature without informing consumers that the setting enabled the collection of viewing data. The complaint alleges that the undisclosed data tracking was unfair and deceptive, in violation of the FTC Act and New Jersey consumer protection laws.

Legislative—Federal

House Hearing Explores Role of Internet-Connected Devices in Recent Cyberattacks
On November 16, 2016, the House Committee on Energy and Commerce held a hearing to address the cybersecurity vulnerabilities of internet-connected consumer devices. Representatives weighed cybersecurity experts' calls for increased regulation of the growing Internet of Things ("IoT") and evaluated the consequences of unsecured IoT devices on the public at large and the direct purchaser.

Congress Passes Legislation to Enhance Cybersecurity Cooperation with Israel
On December 16, 2016, the Senate passed the U.S.–Israel Advanced Research Partnership Act. The legislation authorizes the Science and Technology Directorate of the DHS to expand its cooperation agreements with Israel to include research to improve cybersecurity capability and preparedness. A similar bill, the U.S.–Israel Cybersecurity Cooperation Enhancement Act, was passed by the House of Representatives on January 31, 2017, and was referred to the Senate Committee on Homeland Security and Governmental Affairs. The bill seeks to establish a cybersecurity grant program under the DHS to support joint ventures between U.S. and Israeli businesses, nonprofits, academic institutions, and government agencies.

Senate Urges Companies to Address Cybersecurity Threats
On January 5, 2017, the Senate Armed Services Committee held a hearing titled "Foreign Cyber Threats to the United States" led by Senator John McCain. Top intelligence officials testified that private–public partnerships to address cybersecurity are essential, while noting also that U.S. companies should not wait for Congress to take action before developing their own preparedness to counter cyber-threats.

House Passes Email Privacy Act for Second Time
On February 6, 2017, the House of Representatives passed the Email Privacy Act, which requires the government to obtain a warrant before accessing stored electronic communications held by third-party service providers. This bill amends the Electronic Communications Privacy Act of 1986, under which emails that have been opened or are more than 180 days old are available with a subpoena. The same bill passed the House last year but did not pass the Senate before the end of the session.

Legislative—States

California and Illinois Data Breach Notification Amendments Take Effect
On January 1, 2017, amendments to the data breach notification laws in California and Illinois went into effect. California's amendment requires notification of a security breach when: (i) there is unauthorized acquisition of both encrypted personal information and the encryption key or security credential; and (ii) the business has a reasonable belief that the encryption key or security credential could render such personal information readable or useable. The Illinois amendment expands the definition of "personal information" to include medical and health insurance information, unique biometric information, and a username or email address in combination with a password or security question and answer to access an account. It also clarifies the encryption safe harbor provision, amends the notice requirements, creates requirements to maintain reasonable safeguards to protect information for Illinois residents, and exempts from certain compliance requirements entities that comply with certain federal statutes.

Massachusetts Allows Public Access to Data Breach Information
On January 3, 2017, the Massachusetts Office of Consumer Affairs and Business Regulation announced that it will make information about security breaches affecting Massachusetts citizens publicly available online, pursuant to an update to the state's public records law. Massachusetts joins California, Oregon, and Washington in allowing public access to data breach information.

Canada

Canadian Securities Administrators Issue Staff Notice on Cybersecurity Disclosures
On January 19, 2017, the Canadian Securities Administrators issued a staff notice to report the findings regarding issuers' disclosures of cybersecurity risks and cyberattacks. The notice also provided guidance on how issuers should approach disclosures of cybersecurity risks and incidents.

The following Jones Day lawyers contributed to this section: Jeremy Close, Jay Johnson, Lindsey Lonergan, Alexandra McDonald, Dan McLoon, Mary Alexander Myers, Mauricio Paez, Nicole Perry, Alexa Sendukas, John Sullivan, Anand Varadarajan, and Jenna Vilkin.

[Return to Top]

Latin America

Argentina

Argentina Issues New Regulations on Personal Data Transfers
On November 16, 2016, the Personal Data Protection National Directorate (*Dirección Nacional de Protección de Datos Personales* or "DNPDP") issued new rules (source document in Spanish) for international transfers of personal data. The new regulation contains an official model for international data transfer agreements. Should parties wish to enter into agreements different from the model, these agreements must be approved by the DNPDP. The new rules also list the countries offering adequate levels of protection for the transfer of personal data.

Data Protection Authority Approves Guidelines for App Development
On December 1, 2016, the Argentinean Data Protection Authority issued a report (source document in Spanish) on amendments to the Data Protection Act, Law No. 25.326/2000. The report includes several proposals from the public, internet, businesses, and scholars. While Argentina's statute was recognized as adequate by the EU Commission, the Argentinean government decided to amend the law in light of new international regulations and developments in technology.

Brazil

Special Commission Discusses Brazilian Personal Data Processing Bill
On December 7, 2016, a special parliamentary commission began to review a draft of the Personal Data Processing Bill No. 4060/2012 (source document in Portuguese). The bill, along with the Data Privacy Law No. 5276/2016, aims to protect individual rights as they relate to freedom, privacy, and intimacy in the processing of personal data.

Colombia

National Database Registry Takes Effect
On November 8, 2016, the deadline to register Colombian databases in the National Database Registry ("NDR") expired. Part of the Personal Data Protection General Regime, the NDR (source document in Spanish) serves as a public directory of all databases in the country with information about data owners, data processors, and types of data processing. The NDR imposes various sanctions, including fines, suspension of activities, and temporary and definite closure of operations, on entities that are not registered in the database. The Superintendence of Industry and Commerce will operate the public registry and will allow access to both Colombians and foreign citizens.

Mexico

Mexico Enacts New Data Protection General Law
On January 26, 2017, the new General Law for the Protection of Personal Data held by Regulated Subjects (source document in Spanish) was published in the Federal Official Gazette (*Diario Oficial de la Federación*). The law regulates the processing of personal data by any authority or agency of the executive, legislative, or judicial branch of the government at the federal, state, and municipal level, as well as by all autonomous bodies, political parties, and public trusts and funds, for which there was no prior framework. Under the law, regulated subjects must implement privacy notices, document security policies, and establish procedures to ensure data owners' rights to access, rectify, or oppose the processing of their personal data by a regulated subject. The law also provides specific rules for domestic and international transfers of personal data between authorities. State congresses have six months to conform their current local laws to the national standards.

Mexican Data Protection Authorities Discuss International Data Protection Issues
On January 26 and 27, 2017, the National Institute for Transparency and Access to Information and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*), together with local data protection agencies from the various states and Mexico City's Institute of Transparency, Access to Public Information, Personal Data Protection of Personal Data and Accountability (*Instituto de Transparencia, Acceso a la Información Pública*, *Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México*), commemorated International Data Protection Day (source document in Spanish) by holding forums on personal data protection, privacy rights of "digital individuals," and challenges facing the implementation of the newly enacted General Law for the Protection of Personal Data Held by Regulated Subjects.

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

[Return to Top]

Europe

European Union

ECJ Issues Judgment on National Data Retention
On December 21, 2016, the European Court of Justice ("ECJ") issued a judgment concerning national data retention laws, deciding that national data retention laws for fighting crime violate European Union law if they provide for the "general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication." It thus confirmed the opinion held by Tele2 and other telecoms carriers that such a broad national data retention law would violate EU law. This judgment can have far-reaching impacts on the applicability of other national data retention laws in Germany and other EU Member States. Even if the content of communication may not be retained, the Court confirmed that the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and thus on users' exercise of their freedom of expression. The Court concluded that, under very strict conditions, national data retention laws may be justified. In particular, Member States may enact provisions that: (i) serve to fight serious crime, (ii) provide for targeted retention, and (iii) are strictly necessary. The retention order must be subject to court review, and the user must be notified as soon as the notification would no longer jeopardize the investigations. Retained data must stay within the EU.

European Commission Seeks to Improve EU's Data Economy
On January 10, 2017, the European Commission issued a press release regarding its proposed policy and legal solutions to expand the EU's data economy, as part of its Digital Single Market Strategy presented in May 2015. According to the Commission, in order to make the most of its data potential, the EU must address unjustified restrictions to the free movement of data across borders as well as several legal uncertainties. The Commission launched two public consultations and a debate with Member States and stakeholders to define next steps.

European Commission Pushes ePrivacy Regulation
On January 10, 2017, the European Commission published a statement regarding its proposal of high-level privacy rules for all electronic communications. The Commission published its proposal for an "ePrivacy Regulation," replacing the ePrivacy Directive, and new legislation to ensure stronger privacy and a higher level of data protection already imposed by the new General Data Protection Regulation ("GDPR"). The measures also aim to create new possibilities to process communication data and reinforce trust and security in the Digital Single Market, a key objective of the Digital Single Market Strategy. For more information on the proposal, please see Jones Day's *Commentary*.

Article 29 Working Party

Working Party Seeks EU–U.S. Law Enforcement Umbrella Agreement
On October 26, 2016, the Article 29 Working Party welcomed an initiative to create a general data protection framework for EU–U.S. law enforcement cooperation. The Umbrella Agreement would complement existing EU–U.S. law enforcement agreements and create a data protection standard for future agreements concluded in this field. The Working Party believes that the Umbrella Agreement would strengthen safeguards in existing law enforcement bilateral treaties with the United States.

Working Party Releases Key Guidelines under GDPR
On December 13, 2016, the Article 29 Working Party published three sets of guidelines: Guidelines on Data Protection Officers, Guidelines on the Right to Data Portability, and Guidelines on the Lead Supervisory Authority. These guidelines were issued pursuant to the GDPR, and the Working Party noted that the guidelines were assembled using input from various stakeholders and consultations with national data protection authorities.

Working Party Adopts 2017 GDPR Action Plan
On January 3, 2017, the Article 29 Working Party adopted its Action Plan for 2017, which outlines new objectives and deliverables for the coming year and builds on 2016 priorities

and topics. The key features of the 2017 Action Plan include producing guidelines on consent and profiling, transparency, data transfers to third countries, and data breach notifications.

European Data Protection Supervisor

EDPS Issues Press Release on Control of Online Identities
On October 20, 2016, the European Data Protection Supervisor ("EDPS") published a press release discussing a system in which individuals, rather than online service providers, manage and control their online identity. The EDPS encouraged the Commission to support the development of innovative digital tools such as personal information management systems and take policy initiatives that inspire the development of economically viable business models to facilitate their use.

European Network and Information Security Agency

ENISA Publishes Report on Cyber Insurance
On November 7, 2016, the European Network and Information Security Agency ("ENISA") issued a report on market advances in the cyber insurance sector. The report identifies significant cyber insurance developments over the past four years and discusses good practices and challenges during the early stages of the cyber insurance lifecycle, i.e., before an actual policy is signed, laying the foundation for future work in the area.

ENISA Releases National Cyber Security Strategy Guide
On November 14, 2016, ENISA published a National Cyber Security Strategy ("NCSS") Good Practice Guide to update the different steps, objectives, and practices from the original guide. The guide aims to support EU Member States in their efforts to develop and update their NCSS. The guide also provides specific insights for private, civil, and industry stakeholders involved in the lifecycle of the NCSS.

ENISA Issues Report on PETs Control Matrix
On December 20, 2016, ENISA published a report related to the Privacy Enhancing Technologies ("PETs") control matrix, which is an assessment framework and tool for the systematic presentation and evaluation of online and mobile privacy tools for end users. The document, based on research in the area of secure messaging applications as well as the testing of different privacy tools, draws key conclusions and makes recommendations to be considered by all involved stakeholders in the area of PETs.

ENISA Publishes Guidelines for SMEs on Security of Personal Data Processing
On January 27, 2017, ENISA issued guidelines for small and medium-sized enterprises ("SMEs") on the security of personal data processing. ENISA undertook a study to support SMEs on how to adopt security measures for the protection of personal data following a risk-based approach. In particular, the objectives of the study were to facilitate SMEs' understanding of personal data processing operations and assessing associated security risks.

Belgium

Privacy Commission Finds Big Data Use by Telecommunications Operator Does Not Violate Law
On November 24, 2016, the Privacy Commission issued a press release (source document in French and Dutch) explaining that the use and third-party offering of anonymized location data by a telecommunications operator did not infringe the telecommunication law. The decision is subject to the conditions that the data is sufficiently aggregated and that underlying data is not used in the process.

Privacy Commission Reviews Impact Assessments under GDPR
On December 20, 2016, the Privacy Commission published for consultation (source

document in French and in Dutch) a draft recommendation on the obligation to conduct impact assessments introduced by the GDPR. The review addresses the content of the assessment, the compulsory nature of impact assessments, and stakeholders involved the process.

France

France Unveils Information System Security Plan in the Health Care Sector
On October 14, 2016, France's Ministry of Social Affairs and Health issued an instruction notice (source document in French) providing for the implementation of the "information systems security plan" for the health care sector. The plan is intended to ensure a harmonized minimum baseline level of cybersecurity for information systems of health care facilities, such as hospitals, biomedical laboratories, radiation therapy centers, and imaging and radiology public and private centers. For more information on the proposal, please see Jones Day's *Alert*.

France Moves Forward on Implementation of Cybersecurity Framework for Operators of Critical Infrastructures
On November 28, 2016, France's Secretary General for Defense and National Security, on behalf of the Prime Minister, adopted four sector-specific orders. These orders (source document in French) aim to complete the information systems security plan applicable to the Operators of Critical Infrastructures in the finance, audiovisual and information, industry, and electronic communications and internet sectors.

New Law Requires Certificate of Compliance for Health Data Hosting Services
On January 12, 2017, France issued an ordinance (source document in French) modifying Article L. 1111-8 of the Public Health Code to require health data hosting services to obtain a certificate of compliance from the French Accreditation authority. In addition, when archiving such data, service providers will be required to obtain the approval of France's Ministry of Culture. This certification process will replace the current approvals given by the Minister of Health. The *Conseil d'Etat* will set forth the conditions for approval.

Minister of Interior Issues Audit Report on TES
On January 17, 2017, the Minister of the Interior published an audit report (source document in French) relating to the system security of the Secured Electronic Documents file ("TES"). Used by both the French National Cybersecurity Agency and the *direction interministérielle du numérique et du système d'information et de communication de l'État* (France's interministerial directorate on digital, information systems, and communication, or DINSIC), TES processes personal data related to identity cards and passports, including scanned fingerprints and scanned copies of signatures. Although the audit report notes that TES's security systems were adequate, it makes 11 improvement recommendations to ensure that the biometric identification purposes are properly implemented.

Germany

Data Protection Authorities Discuss Issues with Health Data Processing
On December 5, 2016, seven German DPAs issued press releases (example press release (source document in German)), stating that none of the tested wearables, activity trackers, and fitness and health apps met data protection requirements. The DPAs tested 16 wearables and their respective apps, which were downloaded more than 30 million times. The privacy policies examined did not meet regulatory requirements, and the DPAs pointed out that sensitive health data is processed by third parties, used for marketing purposes, and shared with affiliates. In addition, users cannot purge their data, even if their devices are lost, stolen, or sold. The DPAs are researching ways to handle user complaints relating to this data processing.

German Federal Cabinet Adopts GDPR Implementation Bill
On February 1, 2017, the German Federal Cabinet adopted (source document in German) the revised Draft Implementation Bill of the Federal Ministry of Interior (source document in German) for the upcoming EU GDPR. The GDPR, while aimed at streamlining the data protection requirements for all EU Member States, contains opening clauses that allow Member States to deviate in some circumstances. The proposal for a new Federal Data Protection Act ("FDPA") provides details regarding the scope and implementation of existing GDPR provisions and implements additional data protection requirements from the current FDPA.

Bavarian Data Protection Commissioner Publishes Activity Report
On January 31, 2017, the Bavarian Data Protection Commissioner published an activity report for 2015–2016. The Commissioner focused on video surveillance activities in Bavaria and conducted a comprehensive review of the outsourcing activities of hospitals. The activity report also addresses concerns relating to wearables and health apps, smart water meters, and monitoring employees via GPS.

Italy

DPA Renews General Authorizations
On December 15, 2016, the Italian Data Protection Authority ("DPA") renewed existing authorizations for the processing of the following: (i) sensitive data within employment relationships; (ii) data revealing health and sex life; (iii) sensitive data processed by associations and institutions; (iv) sensitive data processed by professionals; (v) sensitive data processed by banks and financial institutions; (vi) sensitive data processed by private investigators; (vii) judicial data processed by private individuals and public entities; (viii) genetic data; and (ix) personal data processed for purposes of scientific research. The general authorizations will be effective until May 24, 2018, when the GDPR will take effect.

DPA Bans Reputation Databases
On November 24, 2016, the Italian DPA issued a decision (source document in Italian) prohibiting a web platform and an IT archive from providing reputation ratings of individual businesspeople. The prohibited service aims to create ratings of suppliers, distributors, contractors, employees, and business partners by compiling and processing information uploaded by users and collected over the web. According to the decision, such massive collection and dissemination is detrimental to the dignity of individuals and is unreliable given the algorithm for compiling such ratings.

Spain

Spanish DPA Analyzes Impact of New European Data Protection Regulation on SMEs
In January 2017, the Spanish DPA published new materials and resources designed to facilitate SMEs' adaptation to the new GDPR. Specifically, the DPA issued the Guide for Controllers to the Regulation, the Guide for Contracts between Controllers and Processors, and the Guide for Fulfilling the Duty to Inform (source documents in Spanish). These materials, built from the articles and opinions of the Article 29 Working Party, provide practical advice on the GDPR's scope and on how to ensure company compliance with the regulation.

Switzerland

Swiss–U.S. Privacy Shield Takes Effect
On January 11, 2017, the Swiss Federal Data Protection and Information Commissioner and the U.S. Department of Commerce finalized a new Swiss–U.S. Privacy Shield Framework ("Swiss Privacy Shield") that will allow companies to transfer Swiss personal data to the United States in compliance with Swiss data protection requirements. The

Swiss Privacy Shield will replace the U.S.–Swiss Safe Harbor Framework, which was declared inadequate, and will adopt requirements almost identical to those incorporated in the EU–U.S. Privacy Shield. For more information on the proposal, please see Jones Day's *Commentary*.

The Netherlands

Legislative Proposal on Intelligence and Security Services
On November 1, 2016, the Dutch government submitted a proposal (source document in Dutch) to update legislation regarding intelligence and security services in response to technological developments in the area of telecommunications, Wi-Fi networks, and the use of messaging apps. The intelligence and security services will be monitored by an independent commission. According to the Dutch government, a privacy impact assessment was prepared during the preparation of the proposal, and feedback was incorporated accordingly.

Sportswear Company Ends Privacy Violations
On November 8, 2016, the Dutch DPA announced that a sportswear company's fitness app no longer violated the Dutch data protection act. During an earlier investigation, the DPA concluded that the company had not provided its users with sufficient information on the use of health data transmitted through the app, nor had it determined retention periods for this data. Such data included running distances, calories burned, user location, and other metrics such as a user's gender, height, and weight. The DPA announced that the company began to request the data subject's consent and allowed the data subjects to minimize the specificity of their health data. In addition, the company encrypted all running data from inactive users of the older app versions to ensure that health data was not used for analytical purposes.

DPA Reviews First Year under Data Leaks Reporting Obligation Act
On December 28, 2016, the DPA published an analysis (source document in Dutch) of data breaches notified in 2016. Between January 1, 2016, and December 15, 2016, a total of 5,500 data breaches were notified to the DPA under the Data Leaks Reporting Obligation Act. Most of the notifications stem from the health care sector, financial sector, and governmental organizations. The most common cause of data breaches involved receipt by a person other than the intended addressee of messages containing personal data and stolen or lost USB flash drives and laptops.

United Kingdom

UK Investigatory Powers Act Takes Effect
On December 30, 2016, the Investigatory Powers Act 2016 came into force. The Act sets out how investigatory powers may interfere with privacy and "abolishes and restricts various general powers to obtain communications data and restricts the circumstances in which equipment interference, and certain requests about the interception of communications, can take place."

UK ICO Seeks to Fine Charities for Data Misuse
On January 30, 2017, the Information Commissioner's Office ("ICO") gave notice to 11 UK charities threatening fines for breaches of the UK Data Protection Act. The charities have 28 days to respond. The notices come as part of ICO's wider review of the use of personal data by charities and concerns about media reports of pressure on supporters to contribute donations.

ICO Warns UK Companies about Legal Risks of Selling Marketing Lists
On February 2, 2017, the ICO fined a UK company £20,000 for unlawfully trading personal information, stressing that any sale of personal information must be "clear and open." Specifically, the ICO noted that a common form of wording used in website terms ("we may share your information with carefully selected third parties where they are

offering products or services that we believe will be of interest to you") was overly general and nonspecific.

The following Jones Day lawyers contributed to this section: Paloma Bru, Laurent De Muyter, Marina Foncuberta, Olivier Haas, Jörg Hladjk, Bastiaan Kout, Matthijs Lagas, Jonathon Little, Martin Lotz, Giuseppe Mezzapesa, Hatziri Minaudier, Selma Olthof, Audrey Paquet, Elizabeth Robertson, Rhys Thomas, and Undine von Diemar.

[Return to Top]

Asia

People's Republic of China

China Releases Cybersecurity Law
On November 7, 2016, the Standing Committee of the National People's Congress released the Cybersecurity Law, which will become effective on June 1, 2017. The law introduces a number of new provisions and makes substantive amendments to the previous draft, such as tightening regulatory requirements imposed on network service providers and operators, and clarifying reporting obligations.

Research Center and Think Tank Release Report on China's Personal Information Security and Privacy Protection
On November 21, 2016, the Internet Law Research Center of China Youth Politics Institute and Fengmian Think Tank jointly released the first domestic report (source article in Chinese) regarding China's personal information security and privacy protection. The report was based on survey data on personal information security and privacy protection in China.

Hong Kong

PCPD Charges Bank for Using Personal Data in Direct Marketing
On January 10, 2017, the Eastern Magistrates' Court convicted a bank for failing to comply with a customer's request to stop using his personal data in direct marketing. Pursuant to Section 35G(3) of the Personal Data Privacy Ordinance, a company receiving a customer request to cease use of personal data in direct marketing must comply with the request without charge. Failure to comply is punishable by a fine of up to HK$500,000 and imprisonment of up to three years. The bank pled guilty to the charge and paid a fine of HK$10,000.

PCPD Urges IoT Manufacturers to Enhance Transparency of Privacy Protection Measures
On January 24, 2017, the Office of the Privacy Commissioner for Personal Data, Hong Kong ("PCPD") reported a general lack of awareness among Internet of Things ("IoT") device manufacturers regarding communicating privacy and security protection measures to consumers. The report stems from a study conducted by PCPD to explore the privacy challenges and implications brought by fitness bands and their apps. The PCPD urged manufacturers engaged in the development of IoT devices to improve their privacy communications so that consumers can assess the privacy impact and take necessary steps to protect their personal data.

Japan

Personal Information Protection Commission Releases Guidelines Regarding Amended Personal Information Protection Act
On November 10, 2016, after a review of public comments, the Personal Information Protection Commission released Guidelines Concerning Personal Information Protection Act (General Rules) (source document in Japanese). On the same date, the Commission

also released a set of specific guidelines, including: (i) guidelines regarding the provision of personal data to a foreign third party; (ii) guidelines regarding verification and recording obligations related to the transfer of data to third parties; and (iii) guidelines regarding de-identified information (all source documents in Japanese). Companies are advised to review their internal handling of personal information and the relevant internal rules in light of these guidelines, which will provide practical guidance to measures that companies will need to take pursuant to the Act.

Amended Personal Information Protection Act Takes Effect in May 2017
On December 20, 2016, the Cabinet decided to fully bring into force the Amended Act on the Protection of Personal Information.

Personal Information Protection Commission Releases Draft Guidelines Regarding Health Care Sector for Public Comments
On January 31, 2017, the Personal Information Protection Commission released draft guidelines concerning the Personal Information Protection Act for the health care sector (source document in Japanese) for public comments. The draft discusses proper handling of personal information for medical and long-term-care business operators.

Supreme Court Rules on Request for Removal of Search Results
On January 31, 2017, the Japanese Supreme Court issued a decision (source document in Japanese) dismissing an individual's request to remove search results from an online search engine. In reaching its decision, the Supreme Court set a balancing test weighing the individual's legal interest and the potential harm to the individual against the public interest and needs for such facts to be published. The Supreme Court affirmed the lower court's decision to dismiss the individual's claim because the facts were related to public interest and because the search results were not widely disseminated.

Personal Information Protection Commission Releases Guidelines Regarding Data Breach Responses
On February 16, 2017, after a review of public comments, the Personal Information Protection Commission released Guidelines Concerning Reponses, Etc. in Case of Data Breaches (source document in Japanese). The guidelines set recommended measures to be taken in response to data breaches.

Personal Information Protection Commission Releases Guidelines Regarding Financial Sector
On February 28, 2017, after a review of public comments, the Personal Information Protection Commission released four guidelines concerning the Personal Information Protection Act for the financial sector, namely, (i) Guidelines Concerning Personal Information Protection in the Financial Sector, (ii) Practical Guidelines Concerning Security Measures for Personal Information Protection in the Financial Sector, (iii) Guidelines Concerning Personal Information Protection in the Credit Sector, and (iv) Guidelines Concerning Personal Information Protection in the Debt-Collection Sector (all source documents in Japanese).

Singapore

PDPC Assesses Penalties Against Wine Company and Site Developer for Violations of Data Protection Act
On December 23, 2016, Singapore's Personal Data Protection Commission ("PDPC") found that a wine company and its website developer failed to make reasonable security arrangements to prevent the unauthorized access of customers' personal data. The wine company was ordered to conduct a security audit and patch website vulnerabilities. The Commission imposed a financial penalty of S$5,000 on the wine company and a financial penalty of S$3,000 on the site developer for violating the Personal Data Protection Act of 2012.

PDPC Assesses Penalty against Real Estate Agency for Failure to Secure

Personal Data
On January 25, 2017, the PDPC ruled that a real estate agency failed to make reasonable security arrangements to prevent the unauthorized access of personal data stored online, and failed to cease storing documents containing personal data on its system until a security scan had been conducted. The Commission imposed a financial penalty of S$10,000 for violating the Personal Data Protection Act of 2012.

PDPC Fines Restaurant Operator for Breach of Protection Obligations
On January 25, 2017, the PDPC held that a restaurant operator group failed to secure its membership portal from unauthorized access to the individuals' personal data. The PDPC noted that personal data of members was accessible through a simple search on the organization's website. The company will pay S$10,000 for its conduct.

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

[Return to Top]

Australia

Australian Privacy and Information Commissioner Releases 2015–2016 Annual Report
On September 27, 2016, the Australian Information Commissioner released its annual report for July 2015 to June 2016. During this time frame, the Commissioner conducted 17 Commissioner-initiated investigations, received 2,128 privacy complaints, managed 107 data breaches that were voluntarily notified to the Commissioner, and conducted 21 assessments of the privacy practices of businesses and Australian government agencies. The Commissioner made a formal determination under the Australian Privacy Act in seven investigations.

Federal Court Rules on Individual's Right to Metadata
On January 19, 2017, the Federal Court of Australia ruled on an individual's right to access account metadata from a telecommunications provider. The case stems from an individual's request to a telecommunications provider to access the metadata retained by the company regarding his account. The court ruled that the telecommunications provider did not have an obligation to provide an individual with metadata that was not "about" the individual, such as mobile phone network data recording IP address, URL information, cell tower location information, incoming call records, or billing information of incoming callers.

Australia Adopts Mandatory Data Breach Notification Law
On February 13, 2017, the Australian Privacy and Information Commissioner announced a new mandatory data breach notification scheme in Australia. The Privacy Amendment (Notifiable Data Breaches) Bill 2016 "will require government agencies and businesses covered by the Privacy Act to notify any individuals affected by a data breach that is likely to result in serious harm." The Office of the Information Commissioner will work with agencies and businesses to implement the bill in the coming months, as an exact commencement date has not been set.

The following Jones Day lawyers contributed to this section: Adam Salter and Nicola Walker.

[Return to Top]

Jones Day Cybersecurity, Privacy, and Data Protection Lawyers

Emmanuel G. Baud | Edward S. Chang | Po-Chien Chen | James A. Cox

Paris

Walter W. Davis
Atlanta

Michael B. Hazzard
Washington

Robert W. Kantner
Dallas

Ted-Philip Kroke
Frankfurt

Richard M. Martinez
Minneapolis

Daniel J. McLoon
Los Angeles

Jeff Rabkin
San Francisco

Michiru Takahashi
Tokyo

Sergei Volfson
Moscow

Paloma Bru
Madrid

Jörg Hladjk
Brussels

Margaret I. Lyle
Dallas

Peter T. Brabant
Sydney

Marina Foncuberta
Milan

Jan Grootenhuis
Amsterdam

Martin Lotz
Munich

Selma Olthof
Amsterdam

Ann T. Rossum
Irvine

Kerianne N. Tobitsch
New York

Natalie A. Williams
Atlanta

Irvine

Richard DeNatale
San Francisco

Karen P. Hewitt
San Diego

Elena Kaplan
Atlanta

Jonathan Little
London

Todd S. McClelland
Atlanta

Caroline N. Mitchell
San Francisco

Elizabeth A. Robertson
London

Rhys Thomas
London

Undine von Diemar
Munich

Laurent De Muyter
Brussels

Celia Jackson
San Francisco

Giuseppe Mezzapesa
Milan

Jeremy S. Close
Irvine

Chiara B.L. Formenti-Ujlaki
New York

Aaron M. Healey
Columbus

Alexandra A. McDonald
San Francisco

Kelly M. Ozurovich
Los Angeles

Jessica M. Sawyer
Los Angeles

Raquel Travesí
Madrid

Taipei

Timothy P. Fraelich
Cleveland

John E. Iole
Pittsburgh

Jeffrey L. Kapp
Cleveland

Kevin D. Lyles
Columbus

Kristen P. McDonald
Atlanta

Mauricio F. Paez
New York

Adam Salter
Sydney

Michael W. Vella
Shanghai

Toru Yamada
Tokyo

Bénédicte Graulle
Paris

Guillermo E. Larrea
Mexico City

Jérémy Attali
Paris

Daniel C. D'Agostini
São Paulo

Frances P. Forte
Atlanta

Bastiaan K. Kout
Amsterdam

Mary Alexander Myers
Atlanta

Mónica Peña Islas
Mexico City

Alexa L. Sendukas
Houston

Anand Varadarajan
Dallas

Dallas

Joshua L. Fuchs
Houston

Jay Johnson
Dallas

J. Todd Kennard
Columbus

John M. Majoras
Columbus/Washington

Carmen G. McLean
Washington

Nicole M. Perry
Houston

Cristiana Spontoni
Brussels

John A. Vogt
Irvine

Sidney R. Brown
Atlanta

Olivier Haas
Paris

Christopher J. Lopata
New York

Laura Baldisserra
Milan

Jennifer C. Everett
Washington

Bart Green
Irvine

Lindsey Lonergan
Atlanta

Evgenia Nosareva
Paris

Brandy H. Ranjan
Columbus

John T. Sullivan
Dallas

Nicola Walker
Sydney