JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 8 | November 2015

JONES DAY

Jones Day Attorney Spotlight: John A. Vogt Jr.

The consumer plaintiffs' bar aggressively pursues class claims against businesses that collect, use, and transfer consumer and employee information. In the wake of highly publicized data breaches, the wave of privacy and data protection consumer class actions against businesses and organizations whose data was compromised continues. Jones Day has a long history of defending clients facing significant class claims, including coordinating related actions filed across the 50 states, and its Cybersecurity, Privacy & Data Protection Practice includes lawyers with substantial experience defending clients facing class claims related to consumer privacy and data protection issues.

John Vogt, a partner based in Irvine, California, is a member of Jones Day's Cybersecurity, Privacy & Data Protection Practice. Mr. Vogt is a trial lawyer whose practice exclusively focuses on defending Jones Day clients sued in significant state, federal, and nationwide class actions. Mr. Vogt's class action experience is substantial and includes data breach, identity theft, and privacy litigation, as well as lawsuits arising out of the sale of consumer data, the Telephone Consumer Protection Act, the Fair

EDITORIAL CONTACTS

Daniel J. McLoon
Los Angeles

Undine von Diemar
Munich

Mauricio Paez
New York

Jonathon Little
London

Kevin Lyles
Columbus

Paloma Bru
Madrid

Jay Johnson
Dallas

Olivier Haas
Paris

Adam Salter
Sydney

Anita Leung
Hong Kong

Editor-in-Chief: Anand Varadarajan

Practice Directory

HOT TOPICS IN THIS ISSUE

Credit Reporting Act, and various other unfair competition and consumer protection laws at the state and federal levels. Mr. Vogt frequently writes and speaks on class action litigation.

United States

Regulatory—Policy, Best Practices, and Standards

Administration Announces Appointee for Chief Information Officer of Intelligence Community
In July, President Obama appointed Dr. Raymond Cook to the position of Chief Information Officer of the Intelligence Community, Office of the Director of National Intelligence. Dr. Cook previously was Director of the Office of Space Reconnaissance for the Central Intelligence Agency and is a career member of the Senior Intelligence Service.

FTC Hosts Conference to Promote Cybersecurity Among Tech Startups and Developers
On September 9, the Federal Trade Commission ("FTC") hosted a conference in San Francisco for tech startups and developers as part of its larger Start with Security initiative to promote better cybersecurity practices among small and medium-size companies. The FTC Chairwoman provided opening remarks for the conference and encouraged startups and developers to adopt best security practices and integrate security into their products and services.

U.S. and China Collaborate to Prevent Cyber Theft
On September 25, after face-to-face talks between President Obama and President Xi Jinping, the United States and China announced that they reached a "common understanding" to combat "cyber enabled theft of intellectual property" aimed at "providing a competitive advantage to companies or commercial sectors." For more information, *see* Jones Day publication: "U.S. and China Agree to Collaborate in Addressing Cyber Theft Scourge."

Lawmakers Hold Hearings on "Cyber War" and U.S. Deterrence Policy
On September 30, the House Foreign Affairs Committee held a hearing titled "Cyber War: Definitions, Deterrence, and Foreign Policy," which examined whether recent U.S.–China discussions have resulted in meaningful cybersecurity policies. On the same day, Department of Defense ("DOD") officials told the House Committee on Armed Services that cyber threats from both state and non-state actors continue to increase and evolve, calling

Privacy Resources

RECENT AND PENDING SPEAKING ENGAGEMENTS

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

Panel discussion on The Evolution of Cybersecurity Preparedness, ALM cyberSecure 2015, New York, NY (Dec. 15–16)
Jones Day Speaker: Mauricio Paez

Panel discussion on the Data Protection Challenges of Analytics on Social Data, BDO Consulting Conference, Houston, Texas (Dec. 11)
Jones Day Speaker: Jay Johnson

Panel discussion on Cybersecurity Preparation and Incident Reponse, Asian American Bar Association, Houston, Texas (Dec. 9)
Jones Day Speaker: Nicole Perry

Cybersecurity and Data Breaches, SEC Year-End Conference 2015: An Accounting & Reporting Update for Public Companies, Center for Professional Education, Houston, Texas (Dec. 8)
Jones Day Speaker: Nicole Perry

Panel Discussions on TransAtlantic Cybersecurity Considerations, Business Forum 1, Baltimore, Maryland (Dec. 3)
Jones Day Speaker: Mauricio Paez

Panel discussion on the Data Protection Challenges of Analytics on Social Data, IAPP Europe Data Protection Congress 2015, Brussels, Belgium (Dec. 3)
Jones Day Speaker: Olivier Haas

The New General Data Protection Regulation: Anticipating Compliance, Jones Day Roundtable and Dinner, Brussels, Belgium (Dec. 1)
Jones Day Speaker: Undine von Diemar

***FTC v. Wyndham Worldwide Corporation*: FTC Oversight of Data Security**, IAPP KnowledgeNet, Dallas, Texas (Nov. 19)
Jones Day Speaker: Jay Johnson

Charity Fundraising and Data Protection: The New Landscape , Jones Day Seminar, London, England (Nov. 18)
Jones Day Speakers: Jonathon Little, Elizabeth Robertson, Sion Richards

on lawmakers to pass cybersecurity sharing information legislation. A day earlier, the Director of National Intelligence testified at a Senate Armed Services Committee hearing that a comprehensive government effort is necessary to combat hackers and cyber criminals.

White House Unveils Privacy Principles for Precision Medicine Initiative
The Precision Medicine Initiative: Privacy and Trust Principles is said to guide the implementation of the PMI, a program designed to deliver more targeted therapies to patients. The principles fall into six broad categories: (i) governance that is inclusive, collaborative, and adaptable; (ii) transparency to participants and the public; (iii) respecting participant preferences; (iv) empowering participants through access to information; (v) ensuring appropriate data sharing, access, and use; and (vi) maintaining data quality and integrity.

Regulatory—Critical Infrastructure

NIST Releases Draft Report with Proposed Objectives for International Cybersecurity Standardization
On August 11, the National Institute of Standards and Technology ("NIST") released a two-volume draft report NISTIR 8074 titled *Strategic US Government Engagement in International Standardization to Achieve US Objectives for Cybersecurity (2 Volumes)*. As discussed in NIST's press release, the report was published by an interagency working group and "lays out objectives and recommendations for enhancing the US government's condition and participation in the development and use of international standards for cybersecurity."

DOD Increases Cybersecurity Requirements for Contractors
On August 26, the DOD released an interim rule that implements cloud computing and cyber incident reporting procedures for DOD contractors. The interim rule requires contractors and subcontractors to report cyber incidents that actually or potentially adversely affect covered information, systems, or critical support capabilities. In addition, the rule sets forth cloud computing services policies that require use of U.S. servers for handling covered information. For more information, *see* Jones Day publication: "New DOD Cybersecurity Rule Continues Onslaught of Federal Regulations for Government Contractors."

NIST Working Group Publishes Draft Report Setting Forth Framework for Cyber-Physical Systems, Including Internet of Things
On September 18, NIST issued a Draft Framework for Cyber-Physical Systems, which was developed by

Cybersecurity Preparedness and Litigation Risk, Goldman Sachs 13th Annual Hedge Fund Conference, New York, New York (Nov. 12)
Jones Day Speaker: Jeff Rabkin

FFIEC Cybersecurity Assessment Tool Overview, Mortgage Bankers Association, Webinar (Nov. 12)
Jones Day Speakers: Mike Morgan, Lisa Ledbetter

EU Data Protection and International Data Transfer Regulatory Trends, ORCHSE Strategies, LLC—Global Safety and Health Forum, Washington D.C. (Nov. 12)
Jones Day Speaker: Mauricio Paez

Panel discussion on Data Privacy and Mobile Marketing Compliance, Hispanic Bar Association of New Jersey—Corporate Counsel Roundtable Conference, Newark, NJ (Nov. 10)
Jones Day Speaker: Mauricio Paez

2015 Cybersecurity Institute on Government Contracts, Federal Publications, Tysons Corner, Virginia (Nov. 5)
Jones Day Speaker: Mauricio Paez

The New Smoking Gun: Maximizing the Recovery and Evidentiary Value of Text Messages in the Face of Privacy and Discovery Concerns, American Law Institute Webinar (Oct. 27)
Jones Day Speaker: Jay Johnson

Panel discussion on EU International Data Transfer Legal Developments, International Accounting Operations Conference, Cybersecurity: Effectively Dealing with Today's New International Risks & Threats, New York, NY (Oct 26)
Jones Day Speaker: Mauricio Paez

The Potential Coalescence of Voluntary Cybersecurity Standards and Best Practices into an Applicable Standard of Care, Cybersecurity Symposium, SMU Science & Technology Law Review, Dallas, Texas (Oct. 23)
Jones Day Speaker: Jay Johnson

European Court of Justice Strikes Down Safe Harbor: What it Means for Transatlantic Businesses, PLI Webinar (Oct. 22)
Jones Day Speakers: Mike Morgan, Undine von Diemar, Jonathon Little, Paloma Bru

NIST's CPS Public Working Group. The framework proposed in the report is "intended to help manufacturers create new [cyber-physical systems] that can work seamlessly with other such smart systems that bridge the physical and computational worlds." Cyber-physical systems include the internet of things.

Regulatory—Retail

National Retail Federation Study Reveals Dissatisfaction with Credit Card Fraud Protection

On September 16, the National Retail Federation issued a press release announcing the results of a recent survey showing that the majority of U.S. consumers believe that new credit cards issued by banks do not adequately prevent fraud. Approximately 62 percent of consumers indicated that they preferred chip cards that also require a PIN number rather than cards that only have a chip and require a signature.

Regulatory—Defense, National Security, and Economic Espionage

FBI Begins Campaign to Raise Awareness of Economic Espionage

On July 23, in response to an increase in attempts at economic espionage, the Federal Bureau of Investigation ("FBI") announced a campaign to raise awareness by educating industry and business leaders on how to recognize and prevent economic espionage. The FBI estimated U.S. businesses suffered losses ranging in the hundreds of billions of dollars due to economic espionage in the past year. As part of the campaign, the FBI released an educational pamphlet on the three common methods foreign entities use to spy on U.S. companies.

U.S. District Court Orders End of NSA Bulk Telephony Metadata Program

On November 9, a D.C. federal district court judge ordered the National Security Agency ("NSA") in a 43-page opinion to cease its collection of bulk telephony metadata program several weeks before the collection program was to expire under the USA Freedom Act.

FBI Highlights Economic Espionage Threat to Fracking Technology

On September 16, at a special conference in its San Antonio offices, the FBI warned oil and natural gas companies that foreign nations are seeking to obtain drilling technologies—in particular those related to horizontal drilling and proprietary fracking mixes—from U.S. companies.

Panel discussion on Cybersecurity Liability and Regulatory Trends in Private Equity Markets, PECTO Cybersecurity Roundtable, The Riverside Company, New York, NY (Oct. 22)
Jones Day Speaker: Mauricio Paez

Panel discussion on Medical Device Law 2015: Compliance Issues, Best Practices and Future Trends, ABA Section for Science and Technology, Washington D.C. (Oct. 15)
Jones Day Speaker: Mauricio Paez

Advanced Training for Data Protection Officers on International Data Transfer, German Federal Association of Data Protection Officers, Berlin, Germany (Oct. 14–15)
Jones Day Speaker: Undine von Diemar

8th Annual Northern Kentucky University–Chase School of Law CyberSecurity Symposium, NKU Chase School of Law, NKU METS Center, Ohio (Oct. 9)
Jones Day Speaker: Mauricio Paez

EU–U.S. Safe Harbor Program: What Does the Invalidation Mean to Your Business?, Jones Day Telephonic Briefing (Oct. 7)
Jones Day Speakers: Mauricio Paez, Undine von Diemar, Jonathon Little, Paloma Bru, Olivier Haas, Laurent De Muyter

Cyber Threats: If Only I Had … What Can I Do Now?, Jones Day Seminar, London, England (Oct. 1)
Jones Day Speakers: Rhys Thomas, Elizabeth Robertson

Cybercrime, Data Breaches, and You: How Global Hackers Can Ruin Your Business and What Regulators Expect in Terms of Prevention, Disclosure, and Remediation, 10th Annual National Institute on Securities Fraud, American Bar Association, New Orleans, Louisiana (Oct. 1)
Jones Day Speaker: Jay Johnson

Data Protection—Current Challenges for Banks, Practice Seminar of the Association of Foreign Banks in Germany, Frankfurt, Germany (Sept. 23)
Jones Day Speaker: Undine von Diemar

Panel discussion on Cyberliability Trends, Executive Roundtable Series—Opportunities and Risks in the International Marketplace: Developments and Trends in International Trade, Export

Senator Introduces Bill to Criminalize Flying Drones in Unauthorized Airspace
On October 7, the Senate began consideration of the SAFE DRONE Act, which would make it a misdemeanor to knowingly operate a drone within two miles of a wildfire, airport, or in an airspace that has been placed under temporary flight restriction by the Federal Aviation Authority.

Regulatory—Financial Services

Financial Services Roundtable Launches Ad Campaign to Support Cybersecurity Information Sharing Act
On August 3, the Financial Services Roundtable announced an advertising campaign to urge the Senate to pass the Cyber Security Information Sharing Act.

American Bankers Association Offers Guidance for New Computer Chip in Payment Cards
On September 15, the American Bankers Association released instructions to educate consumers on how to use the computer chip embedded in new credit and debit cards. Each time a chipped payment card is used, the computer chip generates a unique code valid for only one transaction, making it more difficult for thieves to duplicate a payment card.

SEC Identifies Focus Areas for Upcoming Cybersecurity Examinations
On September 15, the Securities and Exchange Commission ("SEC") Office of Compliance Inspections and Examinations ("OCIE") issued a risk alert identifying areas of focus for its upcoming cybersecurity examinations of registered broker-dealers and investment advisers. The OCIE indicated that examinations would focus on governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.

SEC Enforcement Director Opposes Changes to Email Privacy Law
On September 16, in testimony provided to the Senate Judiciary Committee, the SEC Enforcement Division Director warned that proposed changes to the Electronic Communications Privacy Act would impede civil law enforcement agencies from pursuing financial fraud and other misconduct. The bill at issue would require law enforcement to get a search warrant before accessing Americans' email and data stored in the cloud.

SEC Announces First Cybersecurity Enforcement Action
On September 22, the SEC announced its first cybersecurity-related enforcement action against a regulated entity. As part of the enforcement action,

Controls, and Global Cybersecurity, Jones Day, Washington D.C. (Sept. 15)
Jones Day Speaker: Mauricio Paez

Litigation and Risk Management in the Age of Digital Vulnerability, Jones Day Seminar, Tokyo, Japan (Sept. 11)
Jones Day Speaker: Jeff Rabkin

RECENT AND PENDING PUBLICATIONS

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

The Future After Safe Harbor, Year In Review, American Bar Association (Dec.)
Jones Day Author: Laurent de Muyter

Australia Introduces New Telecommunications Data Retention Laws, Jones Day Publications (Nov.)
Jones Day Author: Adam Salter

Russian Data Privacy Law: Data Localization Requirement Is In Effect, Jones Day Publication (Nov.)
Jones Day Author: Sergei Volfson

Conference of German Data Protection Officers' Position Paper Offers Guidance on Safe Harbor Decision, Jones Day Publications (Oct.)
Jones Day Authors: Undine von Diemar, Ted-Philip Kroke, Stefanie Stöhr

EU Data Protection: Article 29 Working Party Says Standard Contractual Clauses, Binding Corporate Rules are Adequate—for Now, Jones Day Publications (Oct.)
Jones Day Authors: Undine von Diemar, Mauricio Paez, Olivier Haas

EU–U.S. Data Protection Safe Harbor: Not Safe Anymore, Jones Day Publications (Oct.)
Jones Day Authors: Elizabeth Robertson, Mauricio Paez, Undine von Diemar, Paloma Bru, Laurent De Muyter

Spear Phishing for Dollars: Hackers Masquerading as Corporate Executives Pose a Global Threat to Businesses, Metropolitan Corporate Counsel (Oct.)
Jones Day Authors: Shireen Becker, Jeff Rabkin

Interview Regarding the Safe Harbor Decision, Expansion (Oct.)

the SEC entered into a settlement agreement with the defendant investment advisor in which it found that the adviser had violated Rule 30(a) of Regulation S-P by failing to adopt written policies and procedures reasonably designed to safeguard its clients' personally identifiable information. The investment advisor was censured and required to pay a civil money penalty of $75,000.

Independent Community Bankers of America Encourages Consumers to Protect Data
On October 1, the Independent Community Bankers of America ("ICBA") released a statement in recognition of Cybersecurity Awareness Month. ICBA offered eight tips to help consumers safeguard their online accounts and encouraged consumers to learn more about data privacy and Cybersecurity Awareness Month by visiting Stay Safe Online.

Georgia Tech's Information Security Center Releases Report on Governance of Cybersecurity
On October 2, the Georgia Institute of Technology Information Security Center released a 2015 report titled Governance of Cybersecurity. The report concluded that the financial sector has better privacy and security practices than other industries. Specifically, 64 percent of financial sector boards consider cyber risks when reviewing supplier relationships, and 86 percent of financial sector boards have shifted IT risk management from the Audit Committee to a more focused Risk Committee.

Regulatory—Transportation

FCC Cites Lyft for Telemarketing Violations
On September 11, the Federal Communications Commission ("FCC") cited Lyft, a transportation ride-matching service, for violating federal telemarketing regulations. Among other things, the FCC cited Lyft for unlawfully conditioning consumers' use of Lyft's ride-matching services on consumers' agreement to receive marketing text messages.

FTC Testifies Before Congress on Proposed Safe Harbor for Connected Cars
On October 21, the FTC Commissioner provided testimony regarding proposed legislation on connected cars. The Commissioner told the House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing and Trade that the proposed safe harbor for manufacturers of connected cars would prevent the FTC from enforcing compliance with privacy policies and from taking a host of other consumer protection actions currently within its authority.

Jones Day Author: Paloma Bru

U.S. and China Agree to Collaborate in Addressing Cyber Theft Scourge, Jones Day Publications (Sept.)
Jones Day Authors: Mauricio Paez, Jay Johnson, Mike La Marca

New DOD Cybersecurity Rule Continues Onslaught of Federal Regulations for Government Contractors, Jones Day Publications (Sept.)
Jones Day Authors: Various

Phishing for Corporate Dollars: The Emerging Global Threat Posed by Spear Phishing and Business Email Compromise, Jones Day Publications (Sept.)
Jones Day Authors: Jeff Rabkin, Shireen Becker, Alexandra McDonald

German Data Protection Commissioners Call for Improvements to the General Data Protection Regulation, Jones Day Publications (Sept.)
Jones Day Authors: Undine von Diemar, Mauricio Paez, Ted-Philip Kroke

Mobile Apps: Redefining the Virtual California Economy and the Laws that Govern It, COMPETITION: The Journal of the Antitrust and Unfair Competition Law Section of the State Bar of California, Vol. 24, No. 2 (Fall)
Jones Day Authors: Alexandra McDonald, Jason McDonell, Caroline Mitchell

Trilogue Is On: Preparing for the EU General Data Protection Regulation, Financier Worldwide Magazine (Aug.)
Jones Day Authors: Olivier Haas, Philippe Marchiset, Evgenia Nosareva

Third Circuit Affirms the FTC's Authority to Regulate and Enforce Data Security, Jones Day Publications (Aug.)
Jones Day Authors: Various

GLOBAL PRIVACY & CYBERSECURITY UPDATE ARCHIVES

Global Privacy & Cybersecurity Update, Issue 7

Global Privacy & Cybersecurity Update, Issue 6

Global Privacy & Cybersecurity Update, Issue 5

Global Privacy & Cybersecurity Update,

Regulatory—Energy/Utilities

FERC Issues Notice of Proposed Rulemaking Regarding Revised Standards Aimed at Enhancing Cybersecurity Controls
On July 16, the Federal Energy Regulatory Commission issued a notice of proposed rulemaking seeking comment on seven critical infrastructure protection ("CIP") Reliability Standards aimed at enhancing the cybersecurity of the bulk electric system. The proposed standards would revise existing CIPs on issues affecting the cybersecurity posture of relevant entities and address existing gaps in the supply chain management security controls for bulk electrical systems that are not currently addressed by existing CIPs.

Issue 4

Global Privacy & Cybersecurity Update, Issue 3

Global Privacy & Cybersecurity Update, Issue 2

Global Privacy & Cybersecurity Update, Issue 1

NIST Releases Draft Cybersecurity Guide for Electric Utilities
On August 25, NIST released a draft practice guide NIST SP 1800-2a, titled "Identity and Access Management for Electric Utilities," which was developed by NIST's National Cybersecurity Center of Excellence. According to NIST's press release, the guide is intended "to help energy companies better control who has access to their networked resources, including buildings, equipment, information technology and industrial control systems."

Department of Energy Releases Quadrennial Technology Review
In September, the Department of Energy released its Quadrennial Technology Review, which examines science and technology in various energy sectors and possible research and development opportunities. The Review also focuses on risks and developments related to cybersecurity in the energy industry.

House Subcommittees Hold Hearing on Power Systems Cybersecurity
On October 21, the House Subcommittees on Energy and Research and Technology held a hearing to investigate efforts of federal agencies, industry, and other entities to address looming cybersecurity threats to the U.S. power supply. The hearing considered existing threats as well as potential solutions to mitigate these threats.

Regulatory—Health Care/HIPAA

NIST Issues Draft Guide for Securing Medical Information on Mobile Devices
On July 23, NIST published a draft practice guide NIST SP 1800-1a, titled "Electronic Health Records on Mobile Devices," which was developed by NIST's National Cybersecurity Center of Excellence. As explained in NIST's press release, the guide "demonstrates how health care providers can make mobile devices, such as smartphones and tablets, more secure, in order to better protect patient information and still take advantage of advances in communications technology."

Litigation, Judicial Rulings, and Agency Enforcements

Seventh Circuit Finds Standing in Data Breach Case
On July 20, the Seventh Circuit held that data breach plaintiffs' claims of injuries associated with resolving fraudulent charges and protecting against identity theft are sufficient to establish injury in fact for purposes of Article III standing.

FTC Reaches $10.8M Settlement with Data Broker
On August 7, the FTC alleged that two data broker companies sold sensitive consumer information contained in payday loan applications without disclosing this practice to

consumers, and sold the information to at least one company known to be engaged in fraudulent activity. Three individual defendants affiliated with the data broker companies agreed to settle with the FTC for a total sum of $10.8M.

FTC Settles Charges Against 13 Companies that Falsely Certified Compliance with Safe Harbor Frameworks
On August 17, the FTC announced that it had entered into proposed consent agreements with 13 companies to settle charges that the companies engaged in false and deceptive trade practices under § 5 of the FTC Act by claiming that they were certified members of the U.S.–EU or U.S.–Swiss Safe Harbor Frameworks, even though their certifications had lapsed or never existed.

Third Circuit Upholds FTC Authority to Regulate Corporate Cybersecurity
On August 24, a panel of three judges from the U.S. Court of Appeals for the Third Circuit upheld the FTC's authority to regulate corporate cybersecurity in a unanimous opinion finding that corporate cybersecurity practices could qualify as unfair practices under § 5 of the FTC Act. For more information, see Jones Day publication: "Third Circuit Affirms the FTC's Authority to Regulate and Enforce Data Security."

Washington Supreme Court Rules Public Employee Text Messages on Private Phone are Public Records
On August 27, the Washington Supreme Court ruled that a public employee's work-related text messages sent on a private cell phone are public records under the Washington Public Records Act and are subject to disclosure in response to a records request.

Arizona Solar Business Settles Unwanted Phone Call Case
On August 27, the Arizona attorney general's office announced a settlement with a solar company for violations of telemarketing and consumer-fraud laws, pursuant to which the latter agreed to pay $55,000 in restitution to victims, $100,000 in civil penalties, and $15,000 in attorneys' fees.

FTC Approves Final Settlement with Retail Tracking Technology Startup
On September 3, the FTC approved a final order with a developer of technology that tracks customers' movement and actions in retail outlets. The FTC complaint alleged that Nomi misled consumers when it failed to provide opt-out mechanisms and notice of tracking to consumers in stores. The settlement, originally reached in April, provides that Nomi must not mislead consumers as to whether they will be notified or as to their options regarding information sharing.

Auto Group Reaches Settlement with FTC Over Fair Credit Reporting Act Violations
On September 15, the FTC settled with the loan-servicing arm of a Texas-based auto dealer over charges that it failed to have written policies and procedures in place to maintain the accuracy of consumer credit information reported to credit bureaus and failed to properly investigate disputed credit information in violation of the Furnisher Rule of the Fair Credit Reporting Act.

California Attorney General Settles Privacy Claims with Major Telecommunications Provider
On September 17, the California attorney general announced that the California Department of Justice and the California Public Utilities Commission reached a $33M settlement with a major telecommunications provider over allegations that the provider posted the names, phone numbers, and addresses of customers who had paid for unlisted voice over internet protocol phone service.

Russian Man Pleads Guilty to Involvement in Largest Worldwide Hacking Scheme Ever Prosecuted
On September 25, DOJ announced that a Russian man extradited to the United States after being arrested in the Netherlands pled guilty to conspiracy to commit unauthorized

access of protected computers and conspiracy to commit wire fraud. The government alleged that the man participated in hacks that compromised more than 160 million credit card numbers.

Massachusetts Court Rules Warrant Needed for Cell Phone Data
On September 28, the Massachusetts Supreme Judicial Court ruled that police need a warrant whenever they request a mobile phone service provider to produce more than six hours of cell tower historical data to track the phone's past movements.

Federal Judge Sentences Twin Brother Hackers
On October 2, a federal judge sentenced twin brothers to multi-year sentences for hacking a cosmetics company and stealing thousands of customers' personal information, including credit card information. The brothers also hacked a data aggregation company's database and stole information relating to government contract bids in order to obtain a competitive advantage for one of their technology companies.

California Attorney General Requires Hiring of Privacy Officer as Part of Settlement
On October 2, the California Attorney General reached a settlement with a home design and renovation company over allegations that the company recorded customer and employee conversations without providing proper notice. As part of the settlement, the company must pay a fine of $175,000, conduct a risk assessment, and hire a chief privacy officer.

Legislative—Federal

Senate Removes Social Media Reporting Requirement from Intelligence Bill
On September 21, the Senate removed language from the 2016 intelligence authorization bill requiring social media companies to report suspected terrorist activity on their platforms. Proponents of the removal argued that social media companies are not qualified to judge which posts amount to "terrorist activity" and should not be forced to police their users' speech.

House Approves Bill Requiring DHS to Develop Federal Cybersecurity Strategy
On October 6, the House of Representatives passed the Department of Homeland Security Cybersecurity Strategy Act. The legislation would require the Department of Homeland Security ("DHS") to develop a federal strategy laying out tasks needed to achieve strategic and operational cybersecurity goals, expected costs and timelines for implementation, and the plans to evaluate ongoing performance.

House Passes Airport Workers Security Improvement Act
On October 6, as part of Congress' ongoing efforts to improve Transportation Security Administration ("TSA") security processes, the House of Representatives passed the Airport Access Control Security Improvement Act requiring TSA to tighten airport employees' access to secured areas and use a "risk-based and intelligence-driven" model for screening employees based on position and authorized access level.

House Approves Privacy Suit Bill for European Union Citizens
On October 20, the House of Representatives approved legislation granting European Union citizens access to U.S. courts to allege misuse of their personal data shared with the U.S. for law enforcement purposes. Enacting the so-called Judicial Redress Act was a prerequisite for a recently negotiated U.S.–EU law enforcement data-sharing agreement to take effect.

Senate Passes Cybersecurity Information Sharing Act
On October 27, the Senate passed the Cybersecurity Information Sharing Act ("CISA") after adopting a 10-year sunset provision by voice vote. The bill, introduced in March, protects private companies from liability when they share cyber threat data with the government. The House of Representatives passed similar legislation to CISA (H.R. 1560,

H.R. 1731) earlier this session as well.

Legislative—State

Illinois Governor Rejects Certain Revisions to Data Breach Amendment
On August 26, the Illinois governor vetoed revisions to Illinois's Personal Information Protection Act, asserting that the bill previously passed by the Illinois Senate and General Assembly would have imposed "burdensome requirements" on entities that collect and retain sensitive personal data. The governor deleted language adding consumer marketing and geolocation data to the list of personal information protected by the statute and extended the period for notifying the Illinois Attorney General to 45 calendar days. The revised bill will go back to the General Assembly, which could accept the governor's changes or override the veto with a three-fifths majority vote in both houses.

California Governor Creates Cybersecurity Center
On August 31, the California governor issued an executive order to form the California Cybersecurity Integration Center, whose primary mission will be "to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public or private sector computer networks." Under the order, the Center will also establish a multi-agency Cyber Incident Response Team, which will assist efforts to detect, report, and respond to cybersecurity threats.

California Enacts Trio of Data Breach Notification Law Amendments
On October 6, the California governor signed three bills into law that revise California's data breach notification statute. The first bill (A.B. 964) defines encryption, the second bill (S.B. 570) describes the required content and format of breach notices, and the third bill (S.B. 34) broadens the definition of "personal information" to include license plate data collected by automated readers. The bills take effect on January 1, 2016.

California Enacts Data Privacy Bill Requiring Law Enforcement Warrants
On October 8, the California governor signed the California Electronic Communications Privacy Act, which requires law enforcement agencies to obtain warrants based on probable cause before accessing a person's digital information, such as emails, text messages, and online documents, and tracking or searching electronic devices.

[Return to Top]

Canada

Canadian Government Announces Funding for National Cyber Ssecurity Strategy
On July 22, the Canadian government announced that it would devote CA$142.6M to advance Canada's Cyber Security Strategy and specifically to various initiatives aimed at securing nongovernment entities against cyber threats. In April 2015, the government similarly committed CA$94.4M as part of its 2015 Economic Action Plan to support "essential cyber systems and critical infrastructure against cyber attacks" and "support the operators of Canada's vital cyber systems."

The following Jones Day attorneys contributed to the United States and Canada sections: Steven Gersten, Jay Johnson, Colin Leary, Tyson Lies, Alexandra McDonald, Chiji Offor, Nicole Perry, Scott Poteet, Jessi Sawyer, Alexa Sendukas, and Anand Varadarajan.

[Return to Top]

Latin America

Brazil

House of Representatives Considers Legislation on Internet Crimes
On August 6, a Brazilian congressman approved a motion to submit legislative changes to the Brazilian Criminal Code and to the Internet Civil Rights Framework. The draft legislation (source document in Portuguese) aims to (i) increase sanctions for crimes committed on the internet harming one's reputation; (ii) establish the right to be forgotten in connection with associating one's name with groundless criminal allegations; and (iii) require internet providers to disclose users' personal information to facilitate law enforcement investigation. The legislation awaits vote from the Brazilian House of Representatives.

Mexico

Data Protection Certification System Begins Operations
On August 1, the certification branch of the National Institute of Transparency, Access to Information, and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* or "INAI") officially began its operations (source document in Spanish). This certification arm, known as the Mexican Accreditation Entity (*Entidad Mexicana de Acreditación* or "EMA"), has the power to authorize and certify self-regulated individuals or entities that comply with data protection provisions.

Data Protection Authority Publishes Preliminary Guidelines for Public Consultation
On September 3, INAI issued for public comment its preliminary guidelines (source document in Spanish) on publishing privacy notices through alternative measures. Alternative measures become necessary when it is impossible to deliver privacy notices directly to data owners or if delivery involves disproportionate efforts.

Peru

Peruvian Government Enacts Data Retention Decree
On July 26, the Peruvian government enacted a legislative decree (source document in Spanish) regulating the use of internet data by telecommunications providers in order to assist law enforcement authorities with fighting common and organized crime. This decree granted Peruvian police full access to users' real-time location data and created a duty for telecommunications providers to retain data for a certain period of time.

The following Jones Day attorneys contributed to this section: Daniel D'Agostini, Guillermo Larrea, Lucas Milani, Monica Pena, and Elie Sherique.

[Return to Top]

Europe

European Union

EU and United States Finalize Negotiations on Data Protection "Umbrella Agreement"
On September 8, the European Commission finalized negotiations with the United States on high data protection standards for transatlantic law cooperation. The Commission also issued a question and answer press release summarizing the "Umbrella Agreement."

European Court of Justice

ECJ Rejects "One-Stop-Shop" Principle for Determination of Applicable Law
On October 1, the Court of Justice of the European Union ("ECJ") ruled that the Hungarian Data Protection Authority can apply its national data protection law to a Slovak company to the extent the company was exercising a real and effective activity through stable arrangements in Hungary. The decision rejected the "one-stop-shop" principle for

determining the data protection regulations applicable to companies conducting foreign business.

ECJ Invalidates Safe Harbor Framework
On October 6, the ECJ issued judgment in which it (i) recognized the right of national data protection authorities to evaluate whether the transfer of a person's data to a third country complies with the requirements laid down by the directive; (ii) asserted that the ECJ alone has authority to declare an EU act, such as a Commission adequacy decision, invalid; and (iii) ruled the Safe Harbor adequacy decision of July 26, 2000 invalid because of the data protection issues posed by U.S. surveillance operations. For more information, see Jones Day publication: " EU–U.S. Data Protection Safe Harbor: Not Safe Anymore."

Article 29 Working Party

Article 29 Working Party Releases Letter Regarding Implementation of Financial Instruments (MIFID II) and Market Abuse (MAR) Regulations
On July 7, the Article 29 Working Party published MIFID and MAR comments containing recommendations for the implementation of the MIFID and MAR Regulations. Recommendations include: (i) clarifying the recording obligation of telephone or electronic communications in light of the proportionality principle; (ii) clarifying the information provided to clients and employees regarding recording operations; and (iii) defining data retention periods that are proportionate to the data processing circumstances.

Article 29 Working Party Finds Standard Contractual Clauses and Binding Corporate Rules Adequate
On October 16, the Article 29 Working Party published a joint statement providing guidance on the practical impact of the ECJ decision invalidating the U.S.–EU Safe Harbor system. In the statement, the Working Party found that Standard Contractual Clauses and Binding Corporate Rules may be considered adequate tools for securing the transfer of data to countries outside of the EU, at least until January 31, 2016. For more information, see Jones Day publication: " EU Data Protection: Article 29 Working Party Says Standard Contractual Clauses, Binding Corporate Rules are Adequate—for Now."

European Data Protection Supervisor

EDPS Contemplates Ethics Advisory Board
On September 11, the European Data Protection Supervisor ("EDPS") announced the idea of creating a European Data Protection Supervisor Ethics Advisory Board. The board's mission would be to ensure that fundamental values are respected when implementing new technologies. Additionally, the announcement contains several recommendations about big data, cloud computing, drones, and ambient computing.

EDPS Warns Against Unjustified and Massive Passenger Data Collection
On September 25, the EDPS released an opinion on the collection of passenger name records ("PNR") for the prevention, detection, investigation, and prosecution of terrorist offenses and serious crimes. Specifically, the EDPS commented on the current lack of support justifying the necessity of a PNR scheme in the EU.

European Network and Information Security Agency (ENISA)

ENISA Releases After Action Report Relating to Pan-European Cybersecurity Exercise
On September 23, the European Union Agency for Network and Information Security ("ENISA") released a report reviewing the complex cybersecurity exercise carried out in 2014. The exercise trained European Member States on how to react in a cyber crisis, and the report contains various recommendations and protocols for effective response.

Belgium

Privacy Commission Favors Police Information Amendment to Belgian Data Protection Law
On July 22, the Belgian Privacy Commission released an opinion (source document in French) favoring the Amendment to the Data Protection Law, which contains provisions empowering the Control Agency for Police Information.

Privacy Commission Favors BE-Alert System
On September 9, the Privacy Commission published an opinion (source document in French) favoring citizens' voluntary subscription to the BE-Alert system, a system meant to alert citizens in emergency situations.

Belgian Privacy Commission Reacts to Safe Harbor Decision
On October 16, the Privacy Commission issued a press release (source document in French) on the impact of the ECJ decision invalidating the U.S.–EU Safe Harbor system, in which it stressed coordination among national data protection authorities and favored a pragmatic approach to be discussed at the international conference on November 27.

France

Constitutional Council Approves New Intelligence Law
On July 23, the Constitutional Council approved the majority of the provisions in the recently enacted law relating to intelligence (source document in French). The newly enacted legislation broadens the powers of the French intelligence services and requires the implementation of surveillance measures to be authorized by the French Prime Minister. The law contemplates new surveillance methods including real-time collection of data and obtaining automated data processing from electronic communications processors to detect connections likely to reveal terrorist threats.

CNIL Sends Formal Notices to Eight Online Dating Service Providers
On July 24, the French data protection authority ("CNIL") announced that it had sent formal notices to eight online dating service providers (source document in French) to remedy numerous breaches of the data protection framework, including the processing of sensitive customer data without specific consent from the data subjects.

CNIL Defines Simplified Registration for Health Care Data Processing
On September 11, CNIL announced simplified registration procedures for specific health care data processing. New procedures include single authorization for organized programs to detect specific types of cancer and a reference methodology defining a framework for performance studies relating to medical devices.

Germany

Bavarian State Data Protection Authority Issues Fine for Illegal Customer Data Transfer
On July 30, the Bavarian State Data Protection Authority ("BayLDA") imposed a fine (source document in German) on both parties in an asset deal transaction for illegally transferring customer data. BayLDA's president stated that the transfer of detailed customer data like phone numbers, email addresses, account and credit card information, and purchasing history is permissible only after the relevant customer consents to the transfer or is given an opportunity to object to the transfer.

Bavarian State Data Protection Authority Imposes Fines for Illegally Commissioned Data Processing Agreement
On August 20, BayLDA announced a fine (source document in German) against a company for not setting forth concrete technical and organizational measures to protect personal data in its agreements with commissioned data processors. BayLDA emphasized that the technical and organizational measures must be specific, not generic, for the

individual case to allow the data controller to properly assess the security measures in place.

German Data Protection Commissioners Call for Improvements to GDPR
In September, the Conference of the Data Protection Commissioners of the German Federation and the German States ("Conference") publicly criticized crucial points of the General Data Protection Regulation ("GDPR"), calling on the European Parliament, European Council, and European Commission to address its concerns regarding data economy, purpose limitation, individual's consent, data subject's rights and profiling, the need for data protection officers in private and public bodies, and the transfer of data to authorities and courts in third countries. For more information, see Jones Day publication: "EU Data Protection: Article 29 Working Party Says Standard Contractual Clauses, Binding Corporate Rules are Adequate—for Now."

German State Data Protection Authority Warns Against Data Transfers to the U.S. on Basis of SCCs
On October 14, one German State Data Protection Authority (*Schleswig-Holstein*) issued a position paper stating that data transfers to the U.S. on the basis of Standard Contractual Clauses ("SCCs") should no longer be permitted. The authority further stated that unlawful data transfers can be punished with an administrative fine of up to EUR 300,000.

The Netherlands

Dutch Data Protection Agency Approves Employment Agencies' Pre-Employment Screening Procedures
On August 5, the Dutch Data Protection Agency ("DDPA") declared that pre-employment screening procedures used by Randstad and Adecco (source documents in Dutch) were lawful. The DDPA found that the extensive pre-employment screening and background checks used by Randstad and Adecco sufficiently safeguarded the candidates' privacy.

Court Allows Employee to Send Confidential Information to Private Email Account
On August 17, the Gelderland District Court issued a judgment (source document in Dutch) on employer responsibility regarding confidential work information sent to private email accounts. In its judgment, the court commented that employers bear the burden of setting and enforcing rules regarding the use of private email accounts, and the employee charged in the case did not violate the company's internal rules regarding the use of personal email accounts.

DDPA Publishes Draft Guidance on Data Breach Reporting Duty
On September 1, the DDPA published draft guidance (source document in Dutch) to assist organizations in complying with the newly introduced duty to report data breaches coming into effect on January 1, 2016. The draft guidance discusses which organizations are covered, the type of breaches triggering notification to the DDPA, and applicable notification procedures to both the DDPA and affected individuals.

Numerous Interest Groups Criticize Proposed Extension of Surveillance Powers
On September 1, the public consultation on the Intelligence and Security Services Bill concluded after receiving more than 500 responses (source document in Dutch). Many respondents criticized the proposed legislation for the overbroad scope of wiretapping authorizations, the lack of judicial supervision, and other potential privacy and human rights violations enabled by the legislation.

Spain

SDPA to Collaborate with General Council of the Judiciary
On July 13, the Spanish Data Protection Authority ("SDPA") and General Council of the Judiciary signed a collaboration agreement under which they will share the Council's

database of more than six million judgments relating to personal data protection rights and privacy. Moving forward, the SDPA will contribute to the database by entering its own resolutions relating to personal data protection rights and privacy.

Spanish Government Appoints Director of the SDPA
On July 24, the Spanish government appointed (source document in Spanish) a new Director of the SDPA.

Spanish Supreme Court Outlaws Mandatory Disclosure of Employee Personal Phone and Email
On September 21, the Spanish Supreme Court ruled (source document in Spanish) that employment contract clauses cannot require employees to provide their personal phone number and email. The Court discussed the voluntary nature of communicating this data in an employment relationship and how any mandatory disclosure requirement infringes on fundamental privacy rights.

United Kingdom

Information Commissioner Fines Short Term Lender £180,000 for Inadequate Server Security
On August 4, the UK Information Commissioner ("ICO") issued a monetary penalty notice to the Money Shop for £180,000 after losing servers containing several thousand unencrypted customer records.

English High Court Refuses to Order Compliance with Unreasonable Subject Access Request
On August 6, after considering a request under the Data Protection Act addressed to a law firm for all data held about litigants on behalf of its client, the High Court ruled that it was neither reasonable nor proportionate to require the law firm to conduct lengthy and costly searches to determine whether the requested information was protected by legal privilege (and was therefore exempt).

The following Jones Day attorneys contributed to this section: Paloma Bru, Laurent De Muyter, Olivier Haas, Bastiaan Kout, Ted Kroke, Jonathon Little, Selma Olthof, and Undine von Diemar.

[Return to Top]

Asia

People's Republic of China

Amendment to Criminal Code Adds Internet Service Provider Regulations
On August 29, the People's Republic of China passed Amendment IX to the Criminal Law, which describes punishment for (i) network service providers' failure to perform information network security management; (ii) the sale or provision of any citizen's personal information in violation of the relevant provisions of the state; and (iii) the improper disclosure of any information relating to a nonpublic judicial proceeding.

State Post Bureau of China Passes Guideline and Regulation to Protect Personal Information During Postal Service
On September 2, the Post Bureau of China passed (source document in Mandarin) *The Guideline of Personal Information Protection* and *The Regulation of Monitoring Information Transfer during Express Service* in order to protect personal information in the postal service.

Hong Kong

PCPD Publishes New Guidance on Collection and Use of Biometric Data

On July 20, the Office of the Privacy Commissioner for Personal Data ("PCPD") published its Guidance on Collection and Use of Biometric Data, which provides practical guidance to assist data users collecting biometric data to comply with the Personal Data Ordinance. Under the guidance, data users must consider "whether it is feasible to collect less sensitive biometric data to achieve the same purpose without compromising effectiveness." The guidance encourages data users to conduct a Privacy Impact Assessment to evaluate the impact of the proposed collection on personal data privacy.

PCPD Releases Investigation Report on Company's Collection of Employee Fingerprint Data
On July 21, the PCPD published an investigation report on the collection of employees' fingerprint data by Queenix (Asia) limited for the purposes of security and monitoring staff attendance. The report deemed the collection excessive because employees did not give their informed consent, were not provided with the choice to opt for other alternatives, and were not informed of the privacy risks associated with the collection.

PCPD Sanctions 42 Employers for Placing Blind Recruitment Advertisements
On July 21, the PCPD released an investigation report on unfair collection of personal data by "blind" recruitment advertisements that solicit job applicants' personal data without disclosing the employers' identities. The report found 46 advertisements in breach of the Data Privacy Ordinance for failing to collect personal data in a fair way. The PCPD served enforcement notices on 42 employers directing them to delete the personal data and to formulate company policies for placing recruitment advertisements in compliance with the Ordinance.

PCPD Updates Information Leaflet on Cloud Computing
On July 30, the PCPD published the updated information leaflet on cloud computing, which advises organizations on privacy concerns and risks to consider when engaging in cloud computing. Although engaging cloud providers to process or store personal data can be an outsourcing arrangement, the pamphlet states that data users are still legally responsible for the protection of the personal data collected by them.

PCPD Convicts and Fines Two Companies Under Direct Marketing Regulatory Regime
On September 7, the PCPD released a media statement revealing that a company was convicted of using the personal data of a customer in direct marketing without complying with the requirements in the Ordinance. On September 9, in another media statement, the PCPD explained that another company was convicted of failing to comply with a customer's request for cessation of using his personal data in direct marketing, in contravention of the Ordinance. Both companies received fines for their violations. The PCPD reminded consumers that organizations must notify consumers of their opt-out right when using personal data in direct marketing for the first time, even if the consumers might have consented to such use of their personal data.

Japan

Diet Amends Personal Information Protection Act
On September 3, the National Diet enacted the Law to Amend the Personal Information Protection Act (source document in Japanese). Key changes enacted by the Law include the establishment of a privacy commissioner, expansion of the definition of "personal information," new rules regarding utilization of the anonymized personal data, applicability of the Act to foreign entities, and new regulations on extraterritorial transfer of personal data. The Law will take effect within two years from the date of promulgation.

Japanese Government Issues Cybersecurity Strategy
On September 4, the Japanese government issued a Cybersecurity Strategy pursuant to the Basic Act of Cybersecurity (source document in Japanese). The strategy outlines basic strategic directions such as drafting comprehensive guidelines and standards for internet of things system security and strengthening the role of the National Center of Incident

Readiness and Strategy for Cybersecurity.

Cybersecurity Strategy Headquarters Issues Recommendation to MHLW
On September 11, in response to the recent cyber attack on the Japan Pension Service affecting more than 1 million people, the Cybersecurity Strategy Headquarters of the Cabinet Secretarial issued a recommendation (source document in Japanese) to the Ministry of Health, Labor and Welfare ("MHLW") to strengthen its organizational, personnel, and technical security measures against data breach and cyberattack. This is the first recommendation made by the Cybersecurity Strategy Headquarters under the Basic Act of Cybersecurity.

Diet Amends My Numbers Act
On September 25, the National Diet passed and enacted the Law to Amend the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (source document in Japanese). This amendment of the My Numbers Act expands application of Individual Numbers ("My Numbers") from limited administrative purposes such as taxation and social security to bank accounts, immunization records, and metabolic syndrome health check records. The amendment takes effect in 2018.

Specific Personal Information Protection Commission Issues Guidelines on Measures against My Number Data Breach
On September 28, the Specific Personal Information Protection Commission issued a Notice on Measures in Case of Data Breach Incidents Regarding Specific Personal Information for Private Entities (source document in Japanese). The guidelines explain material data breach incidents that require immediate reporting of the incident to Specific Personal Information Protection Commission and distinguish cases where reporting is not required.

Singapore

Singapore and UK Sign Memorandum of Understanding to Boost Cooperation in Cybersecurity
On July 29, the Cabinet Office of the United Kingdom and Singapore's Cyber Security Agency signed a Memorandum of Understanding on Cyber Security Cooperation covering four broad areas, including cybersecurity incident response and cybersecurity talent development. The memorandum also contemplates joint cyber research and development collaboration, increased funding over the next few years, and specific deliverables for the next UK–Singapore Cyber Dialogue.

Taiwan

Financial Supervisory Commission Requires Limited Disclosure of Personal Information
On July 15, Financial Supervisory Commission published a rule requiring payment processing institutions to not disclose complete personal information of users, such as ID numbers, while engaging convenience stores to collect payment documents.

Financial Supervisory Commission Issues Online Service Terms Announcement
On July 22, Financial Supervisory Commission issued a rule requiring banks to set up SQL mechanisms (source document in Mandarin) to protect personal information while providing an online service.

The following Jones Day attorneys contributed to this section: Elaine Ho, Li-Jung Huang, Anita Leung, Michiru Takahashi, and Richard Zeng.

[Return to Top]

Australia

Australian Information Commissioner Requests Comments on Draft Health Privacy Resources
In October, the Office of the Australian Information Commissioner ("OAIC") requested public comment on a series of new draft health privacy resources for health service providers and consumers. The OAIC published 11 new draft business resources to assist health service providers in understanding and meeting their obligations under the Privacy Act 1988 when handling health information. The resources provide guidance on the collection, use, disclosure, access to, and correction of health information.

Amendment to Telecommunications Act Commences Data Retention Scheme
On October 13, a new data retention scheme (under Part 5-1A of the Telecommunications (Interception and Access) Act of 1979) took effect, requiring telecommunications service providers to collect and retain telecommunications data for a minimum of two years. Telecommunications service providers are required to retain data about the subscriber of services; the source, destination, date, time, duration and type of a communication; and the location of the equipment or line used in connection with a communication. The retained data must be encrypted and protected from unauthorized interference or access. Telecommunications service providers may apply for approval of a "data retention implementation plan" outlining the provider's current practices for ensuring confidentiality of information and interim arrangements prior to full compliance with the Act. If the plan is approved, the service provider will have 18 months before full compliance with the Act is required.

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

[Return to Top]

Jones Day Cybersecurity, Privacy, and Data Protection Lawyers

Emmanuel G. Baud Paris	Wolfgang G. Büchner Munich	Shawn Cleveland Dallas	James A. Cox Dallas
Walter W. Davis Atlanta	Scott A. Edelstein Washington/Los Angeles	Timothy P. Fraelich Cleveland	Joshua L. Fuchs Houston
Karen P. Hewitt San Diego	John E. Iole Pittsburgh	Robert W. Kantner Dallas	Elena Kaplan Atlanta
Jeffrey L. Kapp Cleveland	J. Todd Kennard Columbus	Ted-Philip Kroke Frankfurt	Anita Leung Hong Kong
Jonathon Little London	Kevin D. Lyles Columbus	John M. Majoras Columbus/Washington	Todd McClelland Atlanta
Kristen Pollock McDonald Atlanta	Jason McDonell San Francisco	Carmen G. McLean Washington	Daniel J. McLoon Los Angeles
Janine Cone Metcalf Atlanta	Caroline N. Mitchell San Francisco	Matthew D. Orwig Dallas/Houston	Mauricio F. Paez New York
Chaka M. Patterson Chicago	Jeff Rabkin San Francisco	Elizabeth A. Robertson London	Adam Salter Sydney
Gregory P. Silberman Silicon Valley	Cristiana Spontoni Brussels	Michiru Takahashi Tokyo	Rhys Thomas London

Michael W. Vella
Shanghai

Undine von Diemar
Munich

Toru Yamada
Tokyo

Sidney R. Brown
Atlanta

Paloma Bru
Madrid

Jay Johnson
Dallas

Guillermo E. Larrea
Mexico City

Christopher J. Lopata
New York

Margaret I. Lyle
Dallas

Georg Mikes
Frankfurt

Michael G. Morgan
Los Angeles

Sergei Volfson
Moscow

Olivier Haas
Paris

David L. Odom
Dallas

Po-Chien Chen
Taipei

Nigel Chin
Singapore

Christopher S. Cogburn
Atlanta

Laurent De Muyter
Brussels

Adrian Garcia
Dallas

Steven G. Gersten
Dallas

Bart Green
Irvine

Joshua Grossman
New York

Javier Gutierrez Ponce
Madrid

Aaron M. Healey
Columbus

Elaine Ho
Singapore

Nancy L. Hoffman
New York

Nandini Iyer
Silicon Valley

Bastiaan K. Kout
Amsterdam

Colin Leary
San Francisco

Nicole M. Perry
Houston

Scott B. Poteet
Dallas

Brandy Hutton Ranjan
Columbus

Jessica M. Sawyer
Los Angeles

Raquel Travesí
Madrid

Anand Varadarajan
Dallas

Natalie A. Williams
Atlanta

Marc L. Swartzbaugh
Cleveland

Follow us on:

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