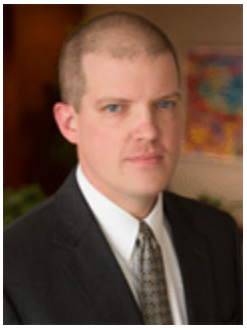
JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 5 | February 2015 JONES DAY

Jones Day Attorney Spotlight: Jay Johnson



Cybersecurity and its attendant privacy implications have dominated recent headlines in the wake of electronic intrusions at some of the country's largest and most respected institutions. Additionally, the increasingly prevalent collection and use of consumer data for a variety of commercial purposes will continue to present opportunities and risks.

Jay Johnson shares responsibility for maintaining a national data breach crisis management team that guides a diverse client base through incident response. Jay represents companies facing privacy- and security-related litigation and government regulatory inquiries, and he leads enterprise-wide privacy and information security assessments for proactive clients looking to minimize the attendant legal risks. He is a former Assistant U.S. Attorney and was responsible for coordinating his district's efforts to combat computer-related crimes and intellectual property theft, and for conducting industry outreach and law enforcement training regarding such crimes.

Jay is vice-chair of the ABA's Privacy and Computer Crime committee. He also is a prolific speaker and

EDITORIAL CONTACTS

Mauricio Paez
New York

Undine von Diemar
Munich

Kevin Lyles
Columbus

Jonathon Little
London

Katherine Ritchey
San Francisco

Paloma Bru
Madrid

Jay Johnson
Dallas

Olivier Haas
Paris

Adam Salter
Sydney

Anita Leung
Hong Kong

Chief Editor: Anand Varadarajan

Practice Directory

HOT TOPICS IN THIS ISSUE

author on privacy and cybersecurity issues of concern and has been published by *Forbes*, *Law360*, and others.

Article 29 Working Party Discusses Surveillance of Electronic Communications for Intelligence and National Security Purposes

China Requires Internet Information Service Providers to Protect User Information and Citizen Privacy

United States

Regulatory—Policy and Best Practices

FTC Issues Staff Report on Internet of Things
On January 27, 2015, the Federal Trade Commission ("FTC") issued a report on the Internet of Things that includes concrete steps and best practices that businesses operating with connected devices should use to protect and enhance consumer privacy and security. The report focuses on the principles of security, data minimization, notice and choice, and ways in which use-based approaches can protect consumer privacy.

FINRA Releases Report on Investment and Financial Firms' Cybersecurity Practices
On February 3, 2015, FINRA released its Report on Cybersecurity Practices. The report, which is based on FINRA's 2014 targeted examination of a cross-section of firms, highlights eight topics to assist firms in developing and implementing a comprehensive cybersecurity risk management program. The management program will be largely dictated by the size of the implementing firm and the assets and threats present to the firm's business.

Regulatory—Retail

Payment Card Industry Security Standards Council Issues Security Requirements and Testing Procedures for Protecting PIN Data
On December 18, 2014, the Payment Card Industry Security Standards Council released the second version of its security requirements for protecting personal identification number ("PIN") data at point-of-sale terminals and ATMs. The Council also released new testing procedures designed to identify minimum security requirements for PIN-based interchange transactions and assist retail participants in establishing safeguards for cardholder PINs.

Retail Groups Urge Broad Preemption in Federal Data Breach Notification Legislation
On January 27, 2015, the Retail Industry Leaders Association's Executive Vice President of Communications and Strategic Initiatives testified before the House Energy and Commerce Committee's subcommittee on data breach regulations. In advocating for the elements of a "sound" federal data breach law, the Executive Vice President testified that the lack of a national standard increases compliance costs for multistate retailers and encouraged committee members to ensure any federal data breach law expressly preempts the patchwork of state laws currently in place.

Regulatory—Financial Services

New York Department of Financial Services Issues Examination Guidance, Including Cybersecurity Preparedness Assessments
On December 10, 2014, the New York Department of Financial Services announced that recently developed and implemented cybersecurity assessments will become a regular, ongoing part of all bank examinations. The announcement includes a list of issues and factors that will be examined as part of the new cybersecurity assessments.

FINRA Releases 2015 Regulatory and Examinations Priorities Letter
On January 6, 2015, the Financial Industry Regulatory Authority ("FINRA") released its

Regulatory and Examinations Priorities Letter. The letter details FINRA's intentions to review firms' approaches to cybersecurity risk management, governance structures and processes for conducting risk assessments, and approaches to compliance with SEC rules regarding electronic storage of records.

SEC Announces 2015 Examination Priorities With Emphasis on Cybersecurity Practices
On January 13, 2015, the Securities and Exchange Commission ("SEC") Office of Compliance Inspections and Examinations ("OCIE") announced its examination priorities, which reflect the practices and products the OCIE perceives to present potentially heightened risks to investors or markets. As discussed in its examination priorities, the OCIE will continue to examine broker-dealers and investment advisers' cybersecurity compliance and will also expand the initiative to include transfer agents.

Financial Industries Organizations Send Joint Letters to the Senate and House of Representatives
On January 23, 2015, seven financial industries organizations—the American Bankers Association, Consumer Bankers Association, Credit Union National Association, Financial Services Roundtable, Independent Community Bankers of America, National Association of Federal Credit Unions, and The Clearing House—sent joint letters to the Senate and House urging that the existing regulatory and enforcement regime ensure robust protection for American's personal financial information.

Financial Services Roundtable Publishes Assessment of Cyber Insurance
In February 2015, the Financial Services Roundtable published an article examining the value, importance, and growth of cyber liability insurance policies as a component of a strong cybersecurity program.

SEC Office of Compliance Inspections and Examinations Releases Report on Broker-Dealers and Investment Advisers' Cybersecurity Practices
On February 3, 2015, the SEC's OCIE released a summary of the results from its Cybersecurity Examination Initiative, which examined 57 broker-dealers and 49 investment advisers in order to better determine how these entities address the legal, regulatory, and compliance issues associated with cybersecurity. The summary provides findings regarding these firms' practices and procedures for identifying, addressing, and protecting their networks and trading activities from cybersecurity risks.

American Bankers Association Provides Testimony Before Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
On February 5, 2015, the American Bankers Association's Senior Vice President of payment and cybersecurity policy testified before the Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security. The testimony focused on the value of a national standard for data security and data breach notifications and urged recognition of existing federal data security requirements.

New York Department of Financial Services Announces Cybersecurity Assessments for Insurance Companies
On February 8, 2015, the New York Department of Financial Services announced that it will integrate regular assessments of cybersecurity preparedness as part of its examination process for insurance companies.

Regulatory—Transportation

Transportation Security Administration Reassesses Big Data Pre-Check Expansion
On February 7, 2015, the Transportation Security Administration ("TSA") rescinded a December 2014 Request for Proposals asking vendors for ideas to expand the TSA Pre-Check Program by collecting publicly available and commercial data on participants.

Currently, the program works by approving travelers who voluntarily provide background information to verify that they are not security risks.

Regulatory—Energy/Utilities

DOE Issues Voluntary Guidance to Energy Companies and Utilities
On January 8, 2015, the U.S. Department of Energy's ("DOE's") Office of Electricity Delivery and Energy Reliability ("OE") released the Energy Sector Cybersecurity Framework Implementation Guidance, which was developed in response to the overall Cybersecurity Framework released by the National Institutes of Standards and Technology ("NIST") in early 2014. The guidance offers best practices for the development by privacy sector energy companies of a comprehensive cybersecurity framework.

DOE Task Force Issues Draft Voluntary Code of Conduct
On January 12, 2015, the DOE and the Federal Smart Grid Task Force issued their final Voluntary Code of Conduct ("VCC"), which contains recommendations concerning privacy of data enabled by smart grid technologies and applies to utilities and third parties providing consumer energy use services. The VCC outlines five "core concepts" that "are intended to apply as high level principles of conduct."

OIG Report Finds Sensitive Information Shared About U.S. Electric Grid
On January 30, 2015, the DOE's Office of Inspector General ("OIG") released a report finding that the Federal Energy Regulatory Commission's controls, processes, and procedures for protecting nonpublic information were lacking in February 2014 when the Commission revealed sensitive internal information regarding the U.S. electric grid. The report states that Commission staff inconsistently handled and shared analyses that identified vulnerabilities in the electric grid without ensuring that the data was adequately evaluated for sensitivity and classification.

Regulatory—Standards

NIST Releases Cloud Metrics and Federal IT Security Controls Guidelines
On December 15, 2014, NIST released a draft guideline designed to assist organizations searching for cloud service providers by providing objective measures of capabilities and performance. The guidelines help organizations navigate the "preponderance of cloud based services in the market." On December 16, 2014, NIST released the final version of a revised guide for assessing the security and privacy controls of federal information systems and organizations.

NIST Requests Comments on Crypotographic Standards
On January 23, 2015, NIST released for comment the second draft of the principles, processes, and procedures it plans to use to develop its cryptographic standards and guidelines. The second draft incorporates public comments about weaker cryptographic algorithms that allowed the National Security Agency access to information.

NIST Releases Mobile Application Security Guidance
On January 26, 2015, NIST released new guidance designed to assist organizations in improving security as employees increasingly use mobile device applications for work purposes. The guidance helps companies implement security for mobile applications, develop application security requirements, understand and test for application vulnerabilities, and approve deployment of applications on mobile devices.

Judicial Rulings and Agency Enforcements

FTC Approves Settlement Over In-App Charges
On December 2, 2014, the FTC settled charges with an app store operator who allegedly billed consumers for in-app purchases made by children without the consent of the account holders. According to the order, the platform did not include account holder

verification and failed to inform account holders that entering the password initiated a 30-minute window during which no further authorization would be required for purchases. The company agreed to provide full refunds, modify its practices to ensure express authorization, and notify all affected consumers.

FTC Settles with Mobile Carrier Over Cramming Charges
On December 19, 2014, the FTC announced that it had reached a settlement agreement with a mobile carrier over mobile cramming charges. The carrier agreed to pay at least $90 M in refunds and fines for allegedly billing customers for unwanted third party charges in a way that was difficult to detect or understand.

FTC Charges Data Broker for Selling Consumers' Personal Information
On December 23, 2014, the FTC charged a data broker with purchasing payday loan applications and selling the consumers' personal information—including Social Security and bank account numbers—to marketers who had no legitimate need for the information. The FTC's complaint alleged that at least one of the marketers used the information to withdraw money from the consumers' accounts without authorization.

FTC Approves Settlement With App Maker
On December 31, 2014, the FTC settled charges with an app maker who allegedly deceived consumers with claims that messages and images sent through its service would disappear after they were viewed, misrepresenting both the amount of personal data it collected and the level of security it provided to protect that data from unauthorized access. According to the order, the company must implement a privacy program under the supervision of an independent privacy professional for the next 20 years and must refrain from misleading consumers about its privacy and security practices.

State Attorneys General Reach Settlement with Digital Advertising Company Over Internet Privacy Allegations
On December 16, 2014, attorneys general for New Jersey, Connecticut, Florida, Illinois, Maryland and New York agreed to a $750,000 settlement with a digital advertiser after an investigation into whether it violated consumer privacy by unlawfully circumventing privacy settings in the Safari Web browser. The states alleged that the advertiser circumvented privacy settings that blocked cookies from third party advertisers in order to extract information about consumers. Under the settlement, the advertiser is prohibited from disabling consumer settings that block cookies and must implement a privacy program within six months.

District Court Dismisses Data Breach Action
On December 10, 2014, a Northern District of Illinois court dismissed a data breach class action against a restaurant for lack of standing. Plaintiffs alleged several types of injury in order to demonstrate standing, including a theory that the prices for goods and services implicitly included a fee for protection of personal information, which the court found unpersuasive. The plaintiffs filed a notice of appeal to the Seventh Circuit.

Court Allows Consumer Suit Against Retailer to Proceed
On December 18, 2014, the district court denied a retailer's motion to dismiss for most of the plaintiffs' claims in a data breach matter, including negligence, unjust enrichment, certain state consumer-protection claims, and data breach notice claims from 26 states. The court trimmed certain state-specific claims, but generally found that plaintiffs sufficiently alleged injury in the form of "unlawful payment card charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees."

District Court Dismisses Children's Privacy Case Under VPPA
On January 20, 2015, a New Jersey District court dismissed a multidistrict consolidated class action against a media company and an online search engine brought under the Video Privacy Protection Act ("VPPA") on behalf of children whose activities on a website were allegedly tracked. The court found that the plaintiffs could not maintain their VPPA

claims because they did not establish that the information collected on the website could be used to identify specific users to the videos they watched.

Legislative—Federal

President Signs Five Cybersecurity Bills
On December 18, 2014, President Obama signed into law the following cybersecurity measures:

- The National Cybersecurity Protection Act of 2014, S. 2519, charges the U.S. Department of Homeland Security's ("DHS") National Cybersecurity Communications Integration Center with responsibility for facilitating cybersecurity threat information sharing.
- The Border Patrol Agent Pay Reform Act of 2014, S. 1691, strengthens DHS's cybersecurity workforce by identifying and filling key cybersecurity positions and providing competitive compensation.
- The Cybersecurity Workforce Assessment Act, H.R. 2952, requires DHS to examine its cybersecurity workforce.
- The Cybersecurity Enhancement Act of 2014, S. 1353, authorizes NIST to develop voluntary cybersecurity standards for the private sector.
- The Federal Information Security Modernization Act of 2014, S. 2521, updates the Federal Information Security Management Act.

House Reintroduces Cyber Intelligence Sharing and Protection Act
On January 8, 2015, Rep. Dutch Rupperberger (D-MD) reintroduced the Cyber Intelligence Sharing and Protection Act (CISPA), which would amend the National Security Act of 1947 to provide for real-time sharing of cyber threat information between federal agencies and cybersecurity providers. The bill was first introduced in 2011 and reintroduced in 2013, but it has never passed the Senate.

White House Releases Text of Proposed Data Breach Notification Bill
On January 15, 2015, the White House issued the text of a proposed Personal Data Notification & Protection Act, which would establish a uniform, national standard requiring certain companies to provide notice to individuals in the event of a personal data breach. In a press release on January 13, 2015, the White House explained that the proposed national standard "helps business and consumers by simplifying and standardizing the existing patchwork of 46 state laws (plus the District of Columbia and several territories) that contain these requirements into one federal statute, and puts in place a single clear and timely notice requirement to ensure that companies notify their employees and customers about security breaches."

President Focuses on Privacy and Cybersecurity Proposals in State of the Union Address
On January 20, 2015, President Obama stressed the need for privacy and cybersecurity legislation in his annual State of the Union Address. The President's speech followed a series of White House initiatives, including a speech at the Federal Trade Commission (accompanying fact sheet), a speech at the National Cybersecurity and Communications Integration Center (accompanying fact sheet), remarks before congressional leadership, a joint statement with Prime Minister David Cameron on U.S./U.K. cybersecurity cooperation, and an announcement by Vice President Joseph Biden regarding a cybersecurity consortium at historically black colleges and universities. The central components of these proposals include:

- Facilitating cyber threat information sharing between the government and private sector;
- Updating law enforcement authority to pursue and prosecute cybercriminals;
- Establishing a national data breach notification standard;
- Allowing educational data to be used only for educational purposes;
- Advancing a renewed proposal for a Consumer Privacy Bill of Rights;
- Launching Department of Energy programs;
- Convening a cybersecurity summit at Stanford University.

House and Senate Consider Uniform Federal Legislation on Data Privacy Standards and Breach Notification
On January 27, 2015, the House Subcommittee on Commerce, Manufacturing, and Trade held a hearing on the need for uniform federal data breach legislation to supplant the host of individual state laws currently in place. Three bills were introduced to provide uniformity:

- The Data Accountability and Trust Act, reintroduced in the House and referred to the House Committee on Energy and Commerce, would provide a national data security standard enforced by the FTC.
- The Data Security and Breach Notification Act of 2015, reintroduced in the Senate and referred to the Committee on Commerce, Science, and Transportation, would establish procedures to be followed in the event of an information security breach.
- The Cyber Privacy Fortification Act of 2015, introduced in the House, would provide criminal penalties for intentional failures to provide required notices of a security breach, and would authorize the Attorney General and state attorneys general to bring civil actions and obtain injunctive relief for federal violations relating to data security.

Legislative—States

New Jersey Considers Amendment to Data Breach Notification Law
On December 15, 2014, the New Jersey Assembly unanimously approved a bill to expand the definition of "personal information" in the state data breach notification law to include email addresses, passwords, and security questions that permit access to an online account. The Assembly bill must pass the New Jersey Senate before becoming law.

Indiana Attorney General Promotes Comprehensive Data Security and Privacy Legislation
On December 22, 2014, the Indiana Attorney General proposed several changes to his state's data breach notification act, including mandatory data use limitations and online privacy policies for website operators. The proposed bill prohibits "data users" from making misrepresentations to Indiana residents concerning the collection, storage, use, sharing, or destruction of their personal information. A bill was introduced in the State Senate on January 12, 2015. If passed, it would take effect on July 1, 2015.

Washington State Attorney General Introduces Bipartisan Data Security Legislation
On January 6, 2015, the Washington Attorney General requested enhancements to the state's data breach notification law in a bipartisan legislative proposal. The proposals, Senate Bill 5047 and House Bill 1078, would eliminate a blanket exemption for encrypted data and require notification to the Attorney General within 30 days of a data breach. In addition, breach notification to consumers would have to include information necessary to secure their financial accounts and recover their identities.

New Jersey Requires Encryption of Personal Health Information
On January 9, 2015, the New Jersey Governor signed legislation that will require health insurance companies to utilize encryption or other technologies to protect personal information from unauthorized access. Covered entities may be subject to monetary penalties of up to $20,000 for violations. The law unanimously passed both houses of the state legislature and will take effect on August 1, 2015.

New York Attorney General Proposes Overhaul of State Data Security Law
On January 15, 2015, the New York Attorney General announced that he would propose legislation to update New York's protection of personal data. The Attorney General called for modifications to the definition of personal information, a requirement that entities implement more robust safeguards, and incentives to encourage companies to adopt heightened forms of data security by creating a safe harbor to eliminate liability.

New Mexico Data Breach Notification Law Passes State House
On February 19, 2015, the New Mexico State House of Representatives unanimously passed a data breach notification law that requires business to notify consumers, and possibly the state attorney general and credit reporting agencies, in the event of a data breach. Currently, New Mexico is one of three states without a data breach notification statute. The law must pass the State Senate before it becomes official.

Federal—Economic Espionage

FBI Announces Indictment of NOAA Employee for Downloading Restricted Government Data
On October 20, 2014, the FBI announced that a hydrologist at the National Oceanic and Atmospheric Administration was indicted for allegedly downloading restricted government data from the National Inventory of Dams database in May 2012. The indicted individual was charged with one count of theft of U.S. government property, one count of illegally accessing a U.S. government computer database, and two counts of making materially false statements in connection with the investigation.

Former Korn Ferry Executive Files Opening Brief in Conviction Appeals
On December 2, 2014, a former executive at Korn Ferry who was convicted for violations of the CFAA and the Economic Espionage Act filed his opening brief in his appeal of his convictions to the Ninth Circuit. The defendant argued that the CFAA does not make it a federal crime to obtain permission to use another's login credentials to access a third party's computer system. He also challenged the classification of the "source lists" that he obtained as "trade secrets."

Fourth Circuit Upholds Conviction Under CFAA Relating to Former Employee's Unauthorized Access to Employer's Computer System
On December 24, 2014, the Fourth Circuit Court of Appeals upheld a jury conviction of a defendant for 12 felony violations of the CFAA for accessing his former employer's computer server without authorization. The defendant had joined a competing firm and was using his former login credentials to obtain information relating to contract bids in order to obtain a competitive advantage for his new firm.

Man Pleads Guilty To Violations of Espionage Act and CFAA Relating to Classified Defense Information
On January 23, 2015, an individual pled guilty to a violation of the Espionage Act for the willful retention of classified national defense information and one violation of the Computer Fraud and Abuse Act ("CFAA") relating to computer intrusions. The defendant, who worked as a computer systems administrator at a U.S. military base in Honduras, accessed computer files that belonged to the Department of Defense and the U.S. Southern Command's Joint Task Force Bravo, and retained classified national defense information.

U.S. National Security and Defense

National Academy of Science Releases Report on Software-Based Alternatives to Bulk Data Collection
In January 2015, the National Academy of Sciences released a prepublication copy of Bulk Collection of Signals Intelligence: Technical Options, a technical report commissioned by the Office of the Director of National Intelligence ("ODNI"). The 80-page report assesses "the feasibility of creating software that would allow the U.S. intelligence community more easily to conduct targeted information acquisition rather than bulk collection."

Administration Declassifies Order Reauthorizing Telephony Metadata Collection Program
In January 2015, ODNI publicly released the Foreign Intelligence Surveillance Court's

December 4, 2014 order renewing the government's bulk telephony metadata collection program until February 27, 2015.

Privacy Oversight Board Assesses Administration's Intelligence Surveillance Reforms
On January 29, 2015, the Privacy and Civil Liberties Oversight Board ("PCLOB") released its assessment of the Administration's implementation of the PCLOB's surveillance reform recommendations. In its report, the PCLOB found that the Administration made substantial progress toward implementing many recommendations, but that it did not stop the Section 215 bulk telephone record collection program.

Administration Speaks on Domestic Intelligence Surveillance Reform
On February 4, 2015, ODNI spoke on domestic intelligence surveillance reforms at the Brookings Institute. ODNI General Counsel Robert Litt addressed the transparency of intelligence activities, limitations on surveillance, bulk data collection, incidental collection, protections for U.S. and non-U.S. persons, and continued efforts to implement the reforms directed by the President. The ODNI also released a progress report titled "Signals Intelligence Reform 2015 Anniversary Report," which addressed the Intelligence Community's progress in implementing reforms set forth by Presidential Policy Directive 28. ODNI will release another public progress report in 2016.

[Return to Top]

Canada

Canada Appoints New Privacy Commissioner to Investigate Complaints Against Office of Privacy Commissioner of Canada
On December 16, 2014, the Canadian government appointed a new Privacy Commissioner, Ad Hoc, for the Office of the Privacy Commissioner of Canada ("OPC"). The privacy commissioner independently investigates Privacy Act complaints brought against the OPC.

Alberta Personal Data Protection Law Amendments Take Effect
On December 17, 2014, the Alberta government passed the Amendments to Alberta's Personal Information Protection Act ("PIPA"), which allow the collection, use, and disclosure of personal information by a trade union when certain conditions are satisfied. The Amendments respond to a November 2013 Supreme Court of Canada case that provisionally invalidated PIPA on the basis that it infringed trade unions' freedom of expression.

Canadian Privacy Commissioners Sign Memorandum of Understanding
On January 13, 2015, the Information and Privacy Commissioners of British Columbia and Alberta and the Privacy Commissioner of Canada signed a Memorandum of Understanding outlining how they will work together to provide comprehensive privacy protection for Canadian citizens.

Canada's Anti-Spam Software Installation Provisions Take Effect
On January 15, 2015, a portion of Canada's anti-spam legislation ("CASL") related to the installation of computer programs came into force. The law prohibits companies from installing computer programs on a laptop, smart phone, or other connected device, even where the program does not have an improper purpose, absent the express consent of the device owner or authorized user.

British Columbian Privacy Commissioner Releases Report on Government Privacy Breach Management
On January 28, 2015, the Information and Privacy Commissioner for British Columbia issued a report analyzing the current breach management policies, procedures, and training within the British Columbian government. The report includes an examination of

more than 300 privacy breach reviews completed by the government's central breach management agency and makes five recommendations that are designed to help the government enhance the effectiveness of its breach management program.

Canadian Privacy Commissioner Questions Proposed Anti-Terrorism Act
On January 30, 2015, Canada's Privacy Commissioner raised privacy concerns about the proposed new Canadian anti-terrorism legislation, Security of Canada Information Sharing Act, including the potential for a lack of oversight and excessive sharing of personal information.

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

[Return to Top]

Latin America

Argentina

Argentina Implements "Do Not Call" National Registry
On January 14, 2015, Argentina implemented a "Do Not Call" national registry (*Registro Nacional No Llame*), a data protection measure introduced by Law No. 26,951 (source document in Spanish). This program allows users to register to a database that prevents them from receiving any marketing communications on their mobile or land telephone lines.

Brazil

Ministry of Justice Launches Public Debate Platforms on Internet Usage and Data Protection
On January 28, 2015, the Brazilian Ministry of Justice launched two public debate platforms to discuss internet usage and the protection of citizen's personal data. The first debate portal seeks public input and suggestions on data storage or net neutrality issues that will influence regulations governing the Internet Civil Framework (source document in Portuguese). The second debate portal provides a platform to discuss the draft data protection law (source document in Portuguese).

Chile

Bill Seeks to Require Mobile Providers to Register Data of Prepaid Users
On December 9, 2014, Chilean legislative representatives proposed legislation (source document in Spanish) to the Chilean Chamber of Deputies seeking to require the registration of customers' personal data for prepaid mobile phones. Current legislation, which requires that customers enter an agreement with mobile operators, does not apply to prepaid mobile phone lines. The bill seeks to require all mobile operators registered under General Telecommunications Law No. 18,168 (source document in Spanish) to register all data obtained from the customer purchasing prepaid chips.

President of the Supreme Court Criticizes the Unified Database
On January 21, 2015, the president of the Chilean Supreme Court of Justice issued a public statement (source document in Spanish) setting forth several weaknesses in the Unified Database ("BUD") project relating to personal privacy violations. He further stated that BUD development does not align with current advances in technology and conflicts with the data protections provided for in Law 19,628 (source document in Spanish).

Ecuador

FTCS Submits Data Protection Bill to Ecuadorian Congress
On January 19, 2015, the President of the Transparency and Social Control Function ("FTCS") announced that the FTCS had sent the Ecuadorian Congress a bill establishing regulations on the use of each Ecuadorian citizen's personal information. The text of the data protection bill is not yet publicly available.

Honduras

National Congress Approves E-Commerce Law
On January 21, 2015, the Honduran National Congress approved (source document in Spanish) the Electronic Commerce Law. The E-Commerce Law, the text of which is not yet publicly available, facilitates online commerce and provides a legal framework for businesses.

Mexico

IFAI Issues Guidelines to Process Personal Data in Extrajudicial Collection Activities
On December 17, 2014, the Mexican Federal Institute of Access to Public Information and Data Protection ("IFAI") issued guidelines (source document in Spanish) to financial institutions on the processing of personal data when carrying out extrajudicial debt collection activities. According to the IFAI, nearly 200,000 formal complaints regarding improper collection practices prompted the issuance of these guidelines.

IFAI Investigates Liverpool Hack
On January 15, 2015, the IFAI announced (source document in Spanish) a preliminary investigation into the vulnerabilities of a database of personal information belonging to credit card retailer Liverpool. On December 24, 2014, Liverpool, the third largest issuer of credit cards in Mexico, publicly disclosed (source document in Spanish) that cybercriminals accessed the company's personnel email accounts and clients' personal information.

IFAI May Sanction Internet Search Engine in Right to be Forgotten ("RTBF") Case
On January 26, 2015, the IFAI issued a resolution to initiate proceedings against an internet search engine for possible breach of Mexico's data privacy law. The search engine allegedly ignored IFAI's request to erase an individual's personal data from its search engine after the individual's request in September 2014. The parties did not reach an agreement at the conciliation hearing in December 2014, and the search engine may face fines of up to 22.4M pesos (approximately USD 1.53M).

Mexican Senate Discusses Secondary Laws to Transparency Amendment
On February 1, 2015, the Mexican Senate resumed discussions on secondary laws relating to transparency, access to public information, and data privacy, pursuant to last year's amendment of the 6th article of the Mexican Constitution. On February 7, 2015, the IFAI released a statement (source document in Spanish) on the importance of approving the secondary laws in order to standardize data privacy obligations for governmental authorities.

Suriname

Suriname Begins Development of National Cyber Security Plan with OAS Support
On December 16, 2014, the Organization of American States ("OAS") issued a press release regarding meetings in Suriname focused on the development of a National Cyber Security Plan for Suriname. Following the initial assessment, OAS will work with Suriname to prepare an implementation outline that addresses the multi-stakeholder priorities and security needs. OAS recently developed this type of cybersecurity program in Colombia,

Panama, and Trinidad and Tobago, and plans to assist other countries in the region as well.

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

[Return to Top]

Europe, Middle East, and Africa

European Union

Data Protection Authorities Urge App Marketplace Operators to Improve Access to Privacy Policies in Apps
On December 9, 2014, 23 data protection authorities sent a letter to app marketplaces requesting mandatory links to privacy policies within apps that collect personal information. Currently, few marketplaces provide individuals with links to obtain their consent to the privacy policies. The data protection authorities urged the app marketplace operators to implement measures that allow individuals to conduct their own assessments prior to downloading apps and being subject to the processing of their personal data.

ECJ Holds Home Cameras Monitoring Public Spaces Not Exempt from Data Protection Regulations
On December 11, 2014, the European Court of Justice ("ECJ") ruled that cameras with data storage capabilities that monitor public spaces, even when installed by an individual for home security purposes, are subject to data privacy protection principles and requirements. This decision follows a Czech court's request for a preliminary ruling on whether home surveillance that captures public spaces can be classified as a "purely personal or household activity."

EDPS Gives Speech on Data Privacy in Context of Counter-Terrorism
On January 27, 2015, the new European Data Protection Supervisor ("EDPS"), gave a speech warning EU legislators about the risks of adopting counter-terrorism measures that fail to comply with the ECJ's annulment of the data retention directive. The EDPS identified several measures that do not pose data privacy problems, including the establishment of a European Counter-Terrorism Centre, the exchange of data on terrorist related convictions, and the improvements to border controls and information sharing. However, the EDPS called for closer scrutiny on other measures, including the proposal for a EU system for processing passenger name records.

EU Commission Provides Update on Reform of EU Data Protection Rules
On January 28, 2015, the new EU Commission published a summary on the current status of the General Data Protection Regulation and expressed its willingness to conclude negotiations in 2015. While several issues remain unresolved, the European Parliament and Council have reached agreements on territorial scope, rules governing transfers to non-EU countries, and additional flexibility for the public sector.

EDPS Gives Speech on Antitrust and Data
On February 3, 2015, the EDPS gave a speech on antitrust, privacy, and big data. He noted that competition and privacy are both challenged by the proliferation of consumer advertising-supported business models. As such, he called for data protection enforcement during merger investigations and the establishment of an inter-regulatory "clearing house."

Article 29 Working Party

Article 29 Working Party Discusses Surveillance of Electronic Communications for Intelligence and National Security Purposes
On December 5, 2014, the Article 29 Working Party issued recommendations to ensure

adherence to fundamental rights of privacy by intelligence and security services and to improve supervision of these entities' activities while maintaining national security. The recommendations address the applicability of EU data protection law to secondary transfers of EU data and whether a third country's national security interests can justify the transfer of EU personal data.

Article 29 Working Party Provides Clarity on Health Data in Apps and Devices
On February 5, 2015, the Article 29 Working Party provided clarification on the definition of health-related data for lifestyle and wellbeing apps. The Working Party defined health data as information that is: (i) medical data or (ii) raw sensor data that can be used itself or in combination with other data to draw a conclusion about the actual health status of a person. This would include information about smoking and drinking habits, allergies, patient support groups, medical product purchases, or medical examination results. The Working Party also clarified the requirement for explicit consent, transparency, purpose limitation, and security when transmitting this data.

Article 29 Working Party Issues Declaration on Processing of Passenger Data in Europe
On February 5, 2015, the Article 29 Working Party released a statement on the creation of the Passenger Name Records ("PNR"). The Working Party did not take a position for or against the existence of this type of registry, but stated that any PNR system should offer sufficient data protection safeguards to ensure the proportionality of the collection and the subsequent use of PNR data.

Article 29 Working Party Sends Letter to Internet Search Engines on De-Listing
On February 5, 2015, the Article 29 Working Party sent letters to Internet search engines, providing them with guidelines for implementing the ECJ's ruling on de-listing of search results. In its letters, the Working Party stated that limiting de-listing to EU domains was insufficient because de-listing was required across all relevant domains. The Working Party also requested information on how search engines deal with de-listing requests and an in-country contact for each EU data protection authority.

European Network and Information Security Agency ("ENISA")

ENISA Issues Report on SMART Grid Security Certification in Europe
On December 19, 2015, ENISA issued a report on SMART grid certification approaches across EU and EFTA countries. Within the report, ENISA provided several recommendations to Member States and the EU Commission, including the appointment of an EU steering committee to coordinate smart grid certification activities.

ENISA Issues Report on Design Based Privacy and Data Protection
On January 12, 2015, ENISA published a report on "Privacy and Data Protection by Design—from Policy to Engineering." The report emphasizes the integration of privacy protections during the early stages of a product or service's development process and promotes discussion on concrete and effective implementation using engineering methods.

ENISA Publishes Latest Research on Network and Information Security for Finance Sector
On January 15, 2015, ENISA published a report titled Network and Information Security ("NIS") for the EU's Finance Sector, which contains information on the regulatory landscape and industry priorities. The report compares information security obligations in the finance sector, identifies the industry's prospects and priorities, and highlights compliance costs for companies. The report recommends that ENISA draft specific guidelines to streamline NIS obligations and enforcement.

ENISA Completes Study on Best Practices for Internet Infrastructure
On January 15, 2015, ENISA finished a study mapping out Internet infrastructure assets and security threats, reviewing emerging trends, and providing adapted security

measures. The study details best practices to protect Internet infrastructure assets and is targeted at infrastructure owners, internet organizations, security experts, developers of security guides, and policy makers.

ENISA Issues Good Practice Guide on Actionable Information for Security Incident Response
January 19, 2015, ENISA issued a report on Actionable Information for Security Incident Response. The report serves as a best practices guide for exchanging and processing actionable information for Computer Emergency Response Teams (CERTs).

ENISA Recaps 2014 Cyber Threat Landscape
On January, 27 2015, ENISA published its consolidated version of the ENISA Threat Landscape 2014, which analyzes the top cyber threats and evolutions from the past year.

ENISA Launches Cloud Certification Schemes Metaframework
January 29, 2015, ENISA launched the Cloud Certification Schemes Metaframework ("CCSM"), which describes security requirements and objectives in existing cloud certification schemes used in the public sector. The CCSM aims to provide transparency about certification schemes to help customers obtain cloud computing services.

Belgium

Belgian and Moroccan Data Protection Authorities Agree on Cross Border Cooperation Framework
On November 29, 2014, the Belgian Privacy Commission signed a protocol (source document in French) with the Moroccan data protection authority to establish a framework on cross border data protection issues such as transfer authorizations, complaints handling, and compliance audits. The data protection authorities ("DPAs") will define the applicable industry sectors at a later date.

Belgian Privacy Commission Adopts Guidelines on Data Security
In December 2014, the Belgian Privacy Commission published new guidelines (source document in French) on data security. The document defines general security objectives for companies and public authorities when retaining, using, processing or disclosing personal data that requires prior authorization.

Belgian Telecom Regulator Identifies Failure in Telecommunications Operators' Compliance
On December 16, 2014, the Belgian telecom regulator ("BIPT") summarized the results (source document in French) of its inquiry into telecommunication operators' compliance with specific rules governing their processing of traffic and location data. The BIPT identified failures by operators on issues such as transparency, prior consent, and contracts with third parties. The BIPT will not take legal action but intends to discuss remedies with operators and other stakeholders.

Belgian Privacy Commission Comments on Draft Legislation on International Exchange of Data for Tax Purposes
On December 17, 2014, the Belgian Privacy Commission issued an opinion (source document in French) on draft legislation concerning the establishment of an international exchange of financial data for tax purposes. The Commission recommended: (i) additional clarity on the tax purposes for which information can be exchanged; (ii) penalties for data transfers leading to non-tax offenses (e.g., money laundering, corruption, and terrorist financing); (iii) notification from tax authorities to the Belgian taxpayer whose data is being transferred.

Belgian Privacy Commission Publishes a Brochure on Workplace Privacy
In January 2015, the Belgian Privacy Commission created a brochure (source document in French) summarizing its previous opinions, recommendations, and guidelines for maintaining data privacy in the workplace.

France

CNIL Creates New Seal for Businesses Compliant with Data Protection Principles
On December 11, 2014, the French Data Protection Authority ("CNIL") created a seal (source document in French) for data controllers who have designated a data protection officer to communicate about the compliance of internal governance processes with the existing data protection framework. In order to obtain the seal, data controllers will have to demonstrate compliance with 25 different data protection requirements.

Paris Tribunal Enforces Right to be Forgotten against Internet Search Engine
On December 19, 2014, the Tribunal of First Instance of Paris enforced an individual's right to be forgotten ("RTBF") against an Internet search engine. The search engine refused to remove links providing details of a crime committed by the individual eight years earlier. However, because the offense dated back eight years and was not specifically mentioned on the individual's legal record, the court ruled that the individual's RTBF outweighed the public's right to be informed about the crime. As a result, the search engine was required to de-list the links from its search results.

CNIL Issues Recommendations for Open Access Internet and Wi-Fi Hotspots
On December 22, 2014, CNIL published its recommendations for legal compliance for open Internet and Wi-Fi access hotspots (source document in French). The recommendations follow CNIL's audit of several Wi-Fi access hotspots and outline the need to: (i) collect connection data in accordance with the Code of Posts and Electronic Communications; (ii) define a limited and proportionate data retention period; (iii) inform users about the processing of their personal data; (iv) check the compliance of the control systems in place; and (v) implement encryption solutions to protect the confidentiality and the security of the processed data.

French Government Specifies Conditions for Governmental Access to Electronic Communications Data Held by Telecommunications Operators
On December 24, 2015, the French government enacted a decree (source document in French), specifying the conditions under which the French government may access the data held by the telecommunications operators. Under the decree, the government may only access limited types of information and must request it from telecommunications operators before using the information.

Germany

German DPA Imposes 1.3M Euro Fine on Insurance Company
On December 29, 2014, the Rhineland-Palatinate Commissioner for Data Protection and Freedom of Information concluded administrative offense proceedings against an insurance company by imposing a 1.3M Euro fine. The proceeding centered around individual employees of the company who had acquired contact data of potential customers without their consent. In addition to paying the fine, the company will contribute 600,000 Euro to the endowment of a chair at the University of Mainz that will be focused on data protection related research.

Ministry of Health Proposes Draft eHealth Legislation
On January 13, 2015, the Ministry of Health proposed draft legislation (source document in German) on ensuring secure digital communication and applications in the health sector. Specifically, the proposed legislation targets quick implementation of useful electronic health card applications, enhanced telematics infrastructure for secure communication within the health sector, and improved interoperability of IT systems within the health sector.

DPA Appeals Decision on Liability for Facebook's Fan Pages
On January 14, 2015, the DPA of the Federal State Schleswig-Holstein ("ULD") appealed

(source document in German) a decision from the Administrative Court of Appeals Schleswig regarding the use of information on a social media company's fan pages. The appellate court held that companies using the fan pages have no control over the use of the data by the social media company and cannot be held responsible for possible data breaches. The ULD appealed the decision to the European Court of Justice, requesting a preliminary ruling on whether control over personal data includes the use of a website in a separate social media network.

New German Draft Bill Aims to Strengthen Data Protection Rights of Consumers
On February 4, 2015, the German Federal Cabinet adopted draft legislation (source document in German) that aims to improve enforcement of civil claims for violations of consumer data protection rights. Under the proposed legislation, consumer associations and other defined organizations may now bring collective actions for certain data protection violations.

The Netherlands

Dutch Data Protection Authority Launches Investigation in Social Media Company's Privacy Terms and Conditions
On December 16, 2014, the Dutch Data Protection Authority ("DPA") launched an investigation (source document in Dutch) into a social media company's recently adjusted worldwide privacy terms and conditions. Under the new privacy policy, the social media company can use the content of user profiles for commercial purposes. The DPA will investigate possible consequences for Dutch user privacy and how users authorize the social media platform to use their personal content.

Telecom Providers Take Measures to Prevent Future Data Protection Act Violations
On January 20, 2015, certain telecommunications providers agreed to take measures to prevent future violations of the Data Protection Act. Following a 2013 investigation, the DPA noted that these companies violated the Data Protection Act by storing detailed data about customers' internet behavior and app use and by misinforming their customers about data storage practices. To comply with the Act, the companies must either remove or depersonalize the data.

Dutch Secretary for Security Seeks Immediate Fines for Privacy Violations
On February 5, 2015, the Dutch Secretary for Security and Justice advocated passing an amendment to legislation (source documents in Dutch) that outlines penalties for companies committing privacy violations. Under the original bill, the DPA must first issue a "binding instruction" prior to levying a penalty on a company for a privacy violation. However, the new proposal allows the DPA to levy a penalty without first giving the instruction. The Dutch House of Representatives must vote on the bill and its suggested amendments before the legislation is enacted.

Spain

Spanish National High Court Issues First Judgment on Right to be Forgotten Following European Court of Justice Ruling
On December 29, 2015, the Spanish National High Court ruled for the first time (source document in Spanish) on the RTBF doctrine established by the ECJ. In its decision, the High Court set forth criteria to be followed in Spain when an individual requests removal of personal data accessible through the Internet. In January 2015, the High Court followed these criteria when issuing 17 other RTBF judgments, 13 of which favored the individual seeking relief.

United Kingdom

Retailer Agrees to Address Security Issues Following Breach

On January 19, 2015, the UK Information Commissioner warned a major shoe retailer to strengthen its data security practices after the retailer left the personal data of over one million customers exposed on an unencrypted database that was due to be decommissioned. Although no financial information was compromised, the retailer signed an undertaking to resolve these data security issues.

UK Competition Regulator Calls for Information on Use of Commercial Data
On January 27, 2015, the Competition and Markets Authority (the UK's competition regulator) invited submissions on the commercial use of consumer data. The authority stated that such information furthers a "fact-finding exercise to help understand fully how businesses collect and use this data for commercial purposes and the implications for firms and consumers."

UK Regulator Requires Internet Search Engine to Change Privacy Policy after Investigation
On January 30, 2015, an Internet search engine signed a formal undertaking with the UK Information Commissioner ("ICO") to improve its privacy policy after an investigation. The Commissioner previously found that the search engine was vague when describing how it used the personal data it gathered and that its privacy policy failed to include sufficient disclosures to users.

ICO Receives New Powers to Audit National Health Service
Starting February 1, 2015, the ICO may audit public healthcare organizations to review how the National Health Service ("NHS") handles patients' personal information. Specifically, the ICO may review areas such as data security, data sharing, records management, and staff training. The ICO acquired these new powers as the NHS considers a number of "big data" initiatives, including the possible re-launch of its care.data project.

UK Government Agrees to Curb Monitoring of Journalists under Regulation of Investigatory Powers Act 2000
On February 4, 2015, the Interception of Communications Commissioner ("ICC") released an official report finding significant intrusion into the data privacy of journalists. According to the report, 19 police forces looked for information from journalists' devices in relation to 34 investigations into illicit dealings between public officials and journalists, with over 600 applications being authorized by the investigating police forces. Because the ICC stated that police did not provide adequate safeguards to protect data privacy or journalistic sources, the UK Home Secretary agreed that judges will now need to approve requests by law enforcement before examining journalists' devices.

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

[Return to Top]

Asia

China

Counterespionage Law Authorizes National Security Employees to Collect Relevant Information
On November 1, 2014, China passed the Counterespionage Law of the People's Republic of China. Under the law, after providing the requisite credentials, a national security authority may legally inspect the electronic communication tools, instruments, and other equipment of a relevant organization or individual, so long as the inspection is for counterespionage work.

China Clarifies Requirements for Companies Using Consumers' Personal Information
On January 5, 2015, China's State Administration of Industry and Commerce issued measures to implement China's Consumer Rights Protection Law ("CRPL"). Taking effect on March 15, the measures (i) clarify the definition of "personal information of consumers"; (ii) clarify CRPL's requirements for the collection, use, and protection of consumer personal information; and (3) provide for significant penalties for violations.

China Requires Internet Information Service Providers to Protect User Information and Citizen Privacy
On February 4, 2015, the State Internet Information Office issued Provisions on the Administration of Internet User Account Name that will come into force on March 1, 2015. The Provisions require Internet information service providers to review registration information submitted by internet users, such as account name, head portrait, and introduction. This will allow the providers to protect user information, ensure citizens privacy, and promptly handle illegal and improper information contained in the registrations.

Hong Kong

Privacy Commissioner Releases Investigative Reports on Mobile Applications Providing Access to Travel Service
On December 15, 2014, Hong Kong's Privacy Commissioner for Personal Data published a report condemning the excessive collection of customers' personal data by a travel service company. The Commissioner released another report detailing how customers' personal data was leaked by an airline services company. Both reports discuss these data issues vis-a-vis the use of smartphone applications by customers. In response to these investigations, the Commissioner launched a campaign themed "Developing Mobile Apps: Privacy Matters" on January 8, 2015.

Privacy Commissioner Issues Guidelines on Personal Data Protection in Cross-Border Data Transfer
On December 29, 2014, the Privacy Commissioner published guidance notes to help companies better understand Section 33 of the Personal Data (Privacy) Ordinance. Although the Ordinance has not yet taken effect, the guidance provides information on best practices for cross border transfers of data, such as model clauses to be included in cross border data transfer agreements.

Privacy Commissioner Announces Rise in Complaints Against Information and Communications Technologies
On January 27, 2015, the Commissioner announced the highlights of its achievements in 2014. In the announcement, the Commissioner noted that the 206 complaints relating to information and communications technologies ("ICT") amounted to nearly 12% of the total complaints received by Commissioner in 2014. This represents a 122% increase in ICT complaints from 2013.

Japan

Specific Personal Information Protection Commission Releases Guidelines for Handling "My Numbers"
On December 11, 2014, the Specific Personal Information Protection Commission released Guidelines for Proper Handling of Specific Personal Information (For Private Entities) (source document in Japanese) in connection with Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure. The guidelines provide explanations for private entities on how to collect, use, and transfer Specific Personal Information for the limited administrative purposes defined in the Act. The Act becomes effective in the private sector in January 2016.

Government Publishes Framework of Bill to Amend Personal Information Protection Act
On December 19, 2014, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunication Network Society released the draft framework of a bill to amend the Personal Information Act (source document in Japanese). The major amendments include the establishment of a privacy commissioner, expansion of the definition of the personal information, new rules on utilizing anonymous personal data, applicability to foreign entities, and extraterritorial transfer of the personal data.

Singapore

New Regulations Take Effect under Singapore Personal Data Protection Act
On January 23, 2015, two new regulations came into force: the Personal Data Protection (Amendment of Seventh Schedule) Order 2015 and the Personal Data (Appeal) Regulations 2015. The Seventh Schedule introduces new rules pertaining to the Secretary of the Appeal Panel and the proceedings of Appeal Committees. Meanwhile, the Appeal Regulations contain new detailed procedures for appeals brought under the Singapore Personal Data Protection Act, including the form of briefings and case management of appeals.

Data Protection Advisory Committee Appoints New Members
On January 28, 2015, the Data Protection Advisory Committee welcomed six new members who will help advise the Personal Data Protection Commission on key policies and enforcement issues under Singapore's Personal Data Protection Act.

Taiwan

Ministry of Transportation Issues Personal Information Maintenance Plan for Civil Air Transportation Enterprise
On October 16, 2014, the Ministry of Transportation promulgated the Regulations Governing Personal Information File Security Maintenance Plan and Processing Method for the Civil Air Transport Enterprise ("Regulation") (source document in Chinese). The Regulation requires civil air transportation companies to implement robust data privacy frameworks to prevent personal data from being stolen, damaged, or illegally disclosed.

The following Jones Day attorneys contributed to the Asia sections: Emmanuel Amos, Li-Jung Huang, Anita Leung, Michiru Takahashi, and Grace Zhang.

[Return to Top]

Australia and New Zealand

Law Council of Australia Raises Concerns About Proposed Mandatory Data Retention Scheme
On January 20, 2015, the Law Council of Australia ("LCA") submitted a report to an Australian parliamentary committee recommending that proposed mandatory data retention legislation be withdrawn, amended, and released as exposure draft legislation for public consultation. Although the report supports the legislation's crime prevention objective, it raises concerns regarding the proportionality of the regime, the security of retained data, and the legislation's impact on privacy and confidentiality. Within the legislation, the report recommends full disclosure of the data set and agencies with access to the data as well as specific protections for privileged and confidential information. The Australian parliamentary committee is expected to submit its report on the legislation on February 27, 2015.

The following Jones Day attorneys contributed to this section: Adam Salter, Nicola Walker, and Alexandra Einfeld.

[Return to Top]

Jones Day Privacy and Cybersecurity Lawyers

Emmanuel G. Baud
Paris

James A. Cox
Dallas

Joshua L. Fuchs
Houston

Elena Kaplan
Atlanta

Anita Leung
Hong Kong

Todd McClelland
Atlanta

Janine Cone Metcalf
Atlanta

Chaka M. Patterson
Chicago

Gregory P. Silberman
Silicon Valley

Undine von Diemar
Munich

Sidney R. Brown
Atlanta

Jay Johnson
Dallas

Stefano Macchi di Cellere
Milan/London

Olivier Haas
Paris

Matthew R. Bowles
Washington

Laurent De Muyter
Brussels

Joshua Grossman
New York

Nancy L. Hoffman
New York

Gabriel Ledeen
San Francisco

Nicole M. Perry
Houston

Raquel Travesí
Madrid

Natalie A. Williams
Atlanta

Jean-Paul Boulee
Atlanta

Walter W. Davis
Atlanta

Karen P. Hewitt
San Diego

Jeffrey L. Kapp
Cleveland

Jonathon Little
London

Jason McDonell
San Francisco

Caroline N. Mitchell
San Francisco

Katherine S. Ritchey
San Francisco

Michiru Takahashi
Tokyo

Toru Yamada
Tokyo

Paloma Bru
Madrid

Guillermo E. Larrea
Mexico City

Georg Mikes
Frankfurt

David L. Odom
Dallas

Po-Chien Chen
Taipei

Adrian Garcia
Dallas

Javier Gutiérrez Ponce
Madrid

Nandini Iyer
Silicon Valley

Tyson M. Lies
Dallas

Scott B. Poteet
Dallas

Virginia Uelze
São Paulo

Wolfgang G. Büchner
Munich

Scott A. Edelstein
Washington/Los Angeles

John E. Iole
Pittsburgh

J. Todd Kennard
Columbus

Kevin D. Lyles
Columbus

Carmen G. McLean
Washington

Matthew D. Orwig
Dallas/Houston

Elizabeth A. Robertson
London

Rhys Thomas
London

Amanda B. Childs
Dallas

Christopher J. Lopata
New York

Michael G. Morgan
Los Angeles

Nigel Chin
Singapore

Steven G. Gersten
Dallas

Aaron M. Healey
Columbus

Bastiaan K. Kout
Amsterdam

Afra Mantoni
Milan

Brandy Hutton Ranjan
Columbus

Anand Varadarajan
Dallas

Shawn Cleveland
Dallas/Houston

Timothy P. Fraelich
Cleveland

Robert W. Kantner
Dallas

Ted-Philip Kroke
Frankfurt

John M. Majoras
Columbus/Washington

Daniel J. McLoon
Los Angeles

Mauricio F. Paez
New York

Adam Salter
Sydney

Michael W. Vella
Shanghai

Michele L. Gibbons
Houston/New York

Margaret I. Lyle
Dallas

Sergei Volfson
Moscow

Christopher S. Cogburn
Atlanta

Bart Green
Irvine

Elaine Ho
Singapore

Colin Leary
San Francisco

Susan M. O'Connor
New York

Jessica M. Sawyer
Los Angeles

Zachary M. Werner
New York

Follow us on: 

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