JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 9 | March 2016

JONES DAY

Jones Day Attorney Spotlight: Jonathon Little

For decades, EU data protection rules have set some of the world's highest standards of data protection and are currently undergoing significant change. Jones Day advises clients globally on compliance issues, particularly on the problems caused by the need to reconcile the needs of international business with regional regulation. Our team works closely to provide commercially aware compliance advice.

Jonathon Little, a London-based partner, is a member of the Firm's Intellectual Property and Cybersecurity, Privacy & Data Protection Practices. He covers data security and privacy issues as well as other commercial technology and intellectual property projects. Jonathon helps clients develop data privacy compliance programs, draft data security and privacy policies, implement processing arrangements, and implement international data transfers. He works closely with the EU litigation team on data breach response projects and data subject access requests. He also works on digital marketing and advertising schemes and advises on the issues arising from monitoring the use of systems and communications.

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

Michiru Takahashi
Tokyo

Editor-in-Chief: Anand Varadarajan

Practice Directory

HOT TOPICS IN THIS ISSUE

United States

Regulatory—Policy, Best Practices, and Standards

EU and U.S. Release Terms of Privacy Shield
On February 29, the European Commission ("EC") and U.S. Department of Commerce released the full text of the EU-U.S. Privacy Shield framework. This release follows the February 2 announcement that EU and U.S. officials had reached an agreement to replace the recently invalidated Safe Harbor program ("Safe Harbor") with a more robust and comprehensive transatlantic data transfer scheme. The details of the Privacy Shield were released as part of a 128-page package that includes the enumeration of the Privacy Shield Principles, the terms of the new "Arbitral Model" that will be used to address certain unresolved data protection claims, and letters from various U.S. regulators. The EC also released a draft "adequacy decision" concluding that the Privacy Shield ensures an adequate level of protection for personal data transferred under its ambit and meets the standards of Directive 95/45/EC. In particular, the EC emphasized the strengthened Principles, increased transparency obligations imposed on participating companies, new oversight and recourse mechanisms, and commitments from the United States that surveillance will be limited to what is strictly necessary.

President Obama Establishes Commission on Enhancing National Cybersecurity as Part of Cybersecurity National Action Plan
On February 9, President Obama announced the creation of a Commission on Enhancing National Cybersecurity. Comprising 12 members and led by the Federal Chief Information Security Officer, the Commission "is tasked with making detailed recommendations on actions that can be taken over the next decade to enhance cybersecurity awareness and protections throughout the private sector and at all levels of Government, to protect privacy, to maintain public safety and economic and national security, and to empower Americans to take better control of their digital security." These efforts are part of the President's Cybersecurity National Action Plan—a multifaceted strategy aimed at strengthening federal cybersecurity, improving incident response, and enhancing infrastructure security and resilience.

House Subcommittee Seeks Industry Advice on Cybersecurity
On January 8, cybersecurity professionals testified in a hearing before the House Science, Space and Technology Subcommittee on Research and

RECENT AND PENDING SPEAKING ENGAGEMENTS

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

Practical Tips to Avoid Cyber Risks and Understand the Legal Liability of "Smart" Devices, ABA Webinar (May 3)
Jones Day Speaker: Jay Johnson

Panel discussion on Update on the General Data Protection Regulation, Jones Day, Frankfurt, Germany (Apr. 14)
Jones Day Speakers: Undine von Diemar, Ted Kroke

Securing the Connected Car: Privacy, Security and Self-Regulation, IAPP Global Privacy Summit 2016, Washington, D.C. (Apr. 3–4)
Jones Day Speaker: Mauricio Paez

Latin America Cybersecurity and Privacy Symposium, Jones Day, Miami, Florida (Apr. 1)
Jones Day Speakers: Mauricio Paez, Paloma Bru, Guillermo Larrea, Todd McClelland

Incident Response Forum 2016, Washington, D.C. (Mar. 31)
Jones Day Speaker: Richard DeNatale

Internet of Things (IoT) National Institute, ABA Section of Science & Technology Law, Washington, D.C. (Mar. 30–31)
Jones Day Speakers: Cynthia Cwik, Mauricio Paez

Data Breaches in Healthcare: Responding to Skyrocketing Cyber Attacks, Strafford Webinar (Mar. 24)
Jones Day Speakers: Richard DeNatale, Todd McClelland

EU Privacy Laws and Implications for Implementing Health and Safety Programs, European Union Health, Safety & Environment Forum, Brussels, Belgium (Mar. 24)
Jones Day Speaker: Undine von Diemar

Dealing With Crisis—Cybersecurity and Data Breaches: The Risk of Regulatory Enforcement Actions and Litigation, 2016 Executive Roundtable Series, Jones Day, Washington, D.C. (Feb. 25)
Jones Day Speaker: Jay Johnson

Technology titled *Cybersecurity: What the Federal Government Can Learn from the Private Sector*. Industry representatives urged the federal government to increase spending on cybersecurity and education efforts for policymakers to keep pace with current industry efforts.

Commission Urges Congress to Limit China's Access to U.S. Markets
On November 17, 2015, the U.S.–China Economic and Security Review Commission issued its 2015 Annual Report to Congress. The Commission urged lawmakers to adopt new reciprocal measures restricting Chinese investment and allowing U.S. businesses to "hack back" in response to state-sponsored cyber espionage against U.S. companies and a series of new laws restricting foreign companies' access to China's market.

Regulatory—Critical Infrastructure

NCCoE Asks Vendors to Help Secure Wireless Medical Devices
On January 28, the National Cybersecurity Center of Excellence ("NCCoE") at the National Institute of Standards and Technology ("NIST") invited technology vendors "interested in working on a standards-based example solution, or reference design, to work with the center and to provide commercially available products and services as modules in the end-to-end example solution." Currently, NCCoE is developing example cybersecurity solutions to shield wireless infusion pumps delivering intravenous medication from unintentional errors or unauthorized access. In December 2015, NCCoE released a white paper discussing the challenges and potential solution requirements needed to better secure infusion pumps on an enterprise network.

NIST Seeks Comments on Computer Security Publication on Randomness
On January 27, NIST announced that it is seeking public comment on its latest draft of a publication intended to help computer security experts use randomness to protect sensitive data. The Second Draft of Special Publication (SP) 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, "aims to help security specialists judge whether the source of random numbers they use as part of the data encryption process is sufficiently unpredictable." NIST requests public comments on the draft document by May 9.

NIST Invites Feedback on Cybersecurity Framework Use
On December 10, 2015, NIST issued a Request for Information on its cybersecurity framework, possible changes, and future governance. NIST identified

Legal Cybersecurity Landscape for Oil & Gas Companies: The Potential Coalescence of Best Practices into an Applicable Standard of Care, Utilities & Energy Compliance & Ethics Conference, Society of Corporate Compliance & Ethics, Houston, Texas (Feb. 22)
Jones Day Speaker: Jay Johnson

Cybersecurity in 2016, 38th Annual Conference on Securities and Business Law, The University of Texas School of Law, Dallas, Texas (Feb. 11)
Jones Day Speaker: Jay Johnson

Federal Financial Institutions Examination Council Cybersecurity Assessment Tool Workshop, Jones Day, Washington, D.C. (Jan. 25–26)
Jones Day Speakers: Lisa Ledbetter, Mauricio Paez, Al Rota

Doing More With Less: Preventing & Managing Digital and Financial Fraud in a Down Commodities Market, BDO, Houston, Texas (Dec. 11, 2015)
Jones Day Speaker: Jay Johnson

RECENT AND PENDING PUBLICATIONS

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

The California Attorney General Recommends Minimum Standards for Reasonable Security Measures under California's Data Protection Law, *The Recorder* (Apr.)
Authors: Greg Silberman, Jessica Sawyer

Text Messages: Recovery & Use in Litigation, Dallas Bar Association Headnotes (Mar.)
Author: Jay Johnson

IRS Warns of Phishing Scam Involving Tax-Related Information, Jones Day Publications (Mar.)
Authors: Justin Herdman, Todd McClelland, Jay Johnson

Save Your Data and Your Dollars: Tips to Prevent "Ransomeware" from Holding Your Company Hostage, Jones Day Publications (Feb.)
Authors: Jeff Rabkin, James Dutro, Daniel McLoon, Mauricio Paez, Michael Morgan, Colin Leary, Alexandra McDonald

specific areas for feedback, including how best practices are being shared, the relative value of different parts of the framework, suggested updates, and long-term management of the framework.

NCCoE Seeks Comments on Data Integrity Project
On November 24, 2015, the NCCoE invited comments on a new project to help organizations prepare for and recover from cyber attacks. NIST issued a draft whitepaper describing the project and "the technical challenges of ensuring accurate and complete back-up data when recovering systems after an attack."

Regulatory—Retail

California Attorney General Releases Data Breach Report
On February 16, the California Attorney General released its Data Breach Report, analyzing the 657 data breaches reported to the Attorney General's office from 2012 to 2015. According to the report, the majority of the reported breaches were the result of security failures. *For further discussion on the Data Breach Report, see the* Jones Day Alert*.*

FTC Issues Recommendations to Businesses on Use of Big Data
In January, the Federal Trade Commission ("FTC") reported recommendations to businesses about the fair use of big data. The report, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues, highlights the ways in which businesses can use big data to provide benefits to underserved consumers. However, citing the Fair Credit Reporting Act, the FTC Act, and equal opportunity laws, the FTC also warned against using big data-derived biases or inaccuracies about certain groups to target consumers for unfair business practices like fraud or denial of credit opportunities.

FTC Approves New COPPA Parental Consent Method
On November 19, 2015, the FTC approved the use of "face match to verified photo identification" ("FVMPI") as a method to obtain parental consent for the collection of children's personal information, as required by the Children's Online Privacy Protection Act ("COPPA"). Before allowing use of online services requiring parental consent, the FVMPI method prompts parents to take a photo of themselves. That photo is then analyzed to confirm that it is a live photo and is compared to an identification photo of the parent that has been analyzed for authenticity.

Regulatory—Defense, National Security, and

California Attorney General Releases Data Breach Report, Jones Day Publications (Feb.)
Authors: Daniel McLoon, Jeff Rabkin, Greg Silberman, Michael Morgan, Jessica Sawyer

Data Breaches Are on the Rise in Australia: What if it Happens to You?, Jones Day Publications (Feb.)
Authors: Adam Salter, Peter Brabant, Nicola Walker

"EU-U.S. Privacy Shield" to Replace "Safe Harbor," Jones Day Publications (Feb.)
Authors: Mauricio Paez, Undine von Diemar, Jonathon Little, Elizabeth Robertson, Paloma Bru, Olivier Haas, Laurent De Muyter, Jennifer Everett, Michael La Marca

Interview with Paloma Bru about the Safe Harbor Decision (*La privacidad de los datos de empresas de la UE, en el aire*), Expansión (Jan.)
Jones Day attorney interviewed: Paloma Bru

International Data Transfers under the General Data Protection Regulation—What Can We Expect to Face Then? (*Internationaler Datentransfer unter der Datenschutzgrundverordnung—Was kommt da auf uns zu*?), German Federal Association of Data Protection Officers (*Berufsverband der Datenschutzbeauftragten Deutschlands—BvD*) (Jan.)
Author: Undine von Diemar

Revised DFARS Interim Rule Regarding Cybersecurity Responds to Industry Concerns, Jones Day Publications (Jan.)
Authors: Peter Garvin, Andrew Jackson, Fernand Lavallee, Todd McClelland, Mauricio Paez, Jeff Rabkin, Grant Willis, Grayson Yeargin, Jay Johnson, Chad Dorr

Proposed Cybersecurity Disclosure Act Shows Deep Misunderstanding of the Role of Board of Directors, Jones Day Publications (Dec. 2015)
Authors: Mauricio Paez, Randi Lesnick, Michael La Marca

Agreement Reached on the European Reform of Data Protection, Jones Day Publications (Dec. 2015)
Authors: Mauricio Paez, Undine von Diemar, Jonathon Little, Elizabeth Robertson, Paloma Bru, Olivier Haas, Laurent De Muyter

Economic Espionage

Baseball Executive Pleads Guilty to Hacking Another Team's Computer System
On January 8, a former baseball executive pled guilty to two counts of unauthorized access of a protected computer in violation of 18 U.S.C. §§ (a)(2)(C) and (c)(2)(B)(iii). The executive admitted to using his knowledge of a former coworker's password to gain access to the former coworker's new email account and proprietary database account at the coworker's new baseball team.

Department of Defense Revises DFARS Interim Rule
On December 30, 2015, the Department of Defense ("DOD") revised the Defense Federal Acquisition Regulations Supplement ("DFARS") interim rule on required cybersecurity measures for defense contractors.

As published in August 2015, the revised DFARS clause 252.204-7012 required contractors to provide "Adequate Security" for Covered Defense Information by implementing the security requirements of the NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." After publishing that rule, the DOD issued a class deviation allowing contractors up to nine months for implementation of security requirements. The December 30, 2015, Interim Rule gives contractors additional time to implement the requirements of NIST SP 800-171 and incorporates a number of changes that will affect contractors' cybersecurity compliance policies. *For further discussion on the revised DFARS interim rule, see the* Jones Day Alert*.*

FBI Director Names New Executive Assistant Director of Criminal, Cyber, Response, and Services Branch
On December 1, 2015, the FBI Director named a new Executive Assistant Director of the Criminal, Cyber, Response, and Services Branch, which oversees all of the FBI's cyber investigations.

Assistant Attorney General Discusses CFAA at Law Review Symposium
On November 6, 2015, the Principal Deputy Assistant Attorney General discussed the Department of Justice's use of the Computer Fraud and Abuse Act ("CFAA") at a recent law review symposium, explaining the factors guiding prosecutorial discretion and successful and unsuccessful prosecutions. In response to the unsuccessful prosecutions, he outlined proposed CFAA amendments, such as expanding the definition of "exceeds authorized access" and requiring proof that the hacker obtained information worth at least $5,000.

Regulatory—Financial Services

FINRA Urges Investors to Understand Brokerage Firm's Cybersecurity Practices
On January 14, the Financial Industry Regulatory Authority ("FINRA") issued an investor alert encouraging investors to evaluate the cybersecurity measures protecting their financial accounts. In the alert, FINRA lays out a series of steps that investors can take to protect themselves, including using wireless connections wisely, not responding to emails requesting personal information, and securing confidential documents.

EU Reaches Agreement on Cybersecurity Rules, Jones Day Publications (Dec. 2015)
Authors: Mauricio Paez, Undine von Diemar, Paloma Bru, Jonathon Little, Olivier Haas, Laurent De Muyter

New Decision Raises the Bar for FTC Enforcement Actions Over Data Security Practices, Jones Day Publications (Dec. 2015)
Authors: Michael Morgan, Todd McClelland, Mauricio Paez, Jeff Rabkin, Greg Silberman, Jay Johnson, Jessica Sawyer, Alexandria Ordway

SEC and FINRA Identify Cybersecurity as 2016 Examination Priorities
On January 5, FINRA released its annual Regulatory and Examination Priorities Letter, identifying cybersecurity as one of its enforcement priorities. In light of the "evolving nature of cyber threats," the regulator stated that it would review firms' approaches to cybersecurity risk management, focusing on topics like "governance, risk assessment, technical controls, incident response, vendor management, data loss prevention, and staff training." Likewise, on January 11, the Securities and Exchange Commission ("SEC") Office of Compliance Inspections and Examinations ("OCIE") announced its examination priorities for 2016. As it did in 2015, OCIE listed cybersecurity as a key initiative. The SEC stated that it will continue "to examine broker-dealers' and investment advisers' cybersecurity compliance and controls" by "testing and assessments of firms' implementation of procedures and controls."

SEC Seeks Exemption from Warrant Requirement in Email Privacy Bill
At a December 1, 2015, hearing before the House Judiciary Committee, the SEC advocated for a warrant exemption carve-out in the Email Privacy Act. The proposal provides an update to the 1986 Electronic Communications Privacy Act, which allows the government to use a subpoena, rather than a warrant, to obtain from internet companies electronic communications more than 180 days old.

State Attorneys General Urge PIN Requirement for Chip Cards
On November 16, 2015, the Attorneys General from Connecticut, Illinois, Maine, Massachusetts, New York, Rhode Island, Vermont, Washington, and the District of Columbia joined in a letter to the top officials at several banks and payment card companies urging quick adoption of chip and PIN technology.

New York Financial Regulator Proposes Cybersecurity Rules
On November 9, 2015, former Acting New York Superintendent of Financial Services requested input from federal and state regulators on proposed rules from the New York State Department of Financial Services designed to protect customer account information and financial institutions' information technology systems. The rules would, among other things, require banks and insurers to conduct annual penetration testing and designate a qualified employee to serve as chief information security officer responsible for overseeing, implementing, and enforcing cybersecurity programs and policies. The rules also provide for additional notification requirements in the event of a cybersecurity incident that has a "reasonable likelihood of materially affecting the normal operation" of the company.

Regulatory—Transportation

DOT and Automakers Agree on Proactive Road Safety Principles Affecting Connected Vehicles
On January 15, the Department of Transportation ("DOT"), the National Highway Traffic Safety Administration, and 17 automakers agreed on a set of proactive safety principles for improving vehicle safety and the safety of U.S. roadway users. The Statement of Principles includes a commitment from DOT and automakers to work collaboratively to improve road safety by mitigating automotive cyber threats and enhancing analysis of early warning reporting data collected by motor vehicle and motor vehicle equipment manufacturers.

New York Attorney General Announces Settlement with Transportation Services Company Over Rider Data Security Practices
On January 6, the New York Attorney General announced a settlement with a transportation services company, which requires the transportation ride matching service to enhance protections for its riders' personal information and a $20,000 penalty for separately failing to comply with state breach notification laws. According to the announcement, the company agreed to encrypt rider geo-location data and implement multifactor authentication access controls around sensitive rider personal information. The company will also pay a $20,000 penalty in connection with a data breach that occurred in

September 2014.

DOT Revises Guidance on Automated Vehicles and Announces Plans for Model State Policy
In January, DOT unveiled policy guidance that updates the National Highway Traffic Safety Administration's 2013 preliminary guidance concerning automated cars. Given the widespread deployment of partially and fully automated vehicles, the guidance announces the agency's six-month timeline for working with states to craft "model policy guidance that helps policymakers address issues in both the testing and the wider operational deployment of vehicles at advanced stages of automation and offers a nationally consistent approach to autonomous vehicles."

DOT Launches $50M Smart City Challenge
On December 7, 2015, the DOT announced the Smart City Challenge, which invites cities nationwide to submit bold, data-driven ideas for making transportation safer, easier, and more reliable in a "Smart City." To showcase what is possible when technology is used to connect transportation assets into an interactive network, the agency plans to award up to $40M to one winning mid-sized city (defined as city having population between 200,000 and 850,000) selected through the challenge. The winning city will be announced in June 2016.

Regulatory—Health Care/HIPAA

DHHS Issues Final Rule Regarding HIPAA and the NICS
On January 4, the Department of Health and Human Services ("DHHS") issued a final rule modifying HIPAA's Privacy Rule to expressly permit certain covered entities to disclose to the National Instant Criminal Background Check System ("NICS") the identities of individuals who, for specific mental health reasons, are prohibited by federal law from having a firearm. This permission does not apply to most treating providers but applies to only a small subset of covered entities that: (i) make the mental health determinations that disqualify individuals from having a firearm; or (ii) are designated by their respective states to report such information to NICS. This rule permits a covered entity to report only limited identifying, nondiagnostic, and nonclinical information to the NICS.

Litigation, Judicial Rulings, and Agency Enforcements

Dental Practice Software Provider Settles with the FTC over Protection of Patient Data
On January 25, a leading dental practice software provider settled with the FTC for $250,000 over claims that the provider misled patients that their sensitive personal information would be adequately encrypted. The FTC complaint alleged that the provider incorrectly advertised industry-standard encryption that would meet HIPAA requirements for protection of patient data.

Companies Tackle Biometric Data Privacy Suits Under Illinois BIPA
On December 29, 2015, an Illinois federal court refused to dismiss a putative class action accusing an online image publishing service of unlawfully using facial recognition technology to gather biometric data from users' photographs in an alleged violation of the Illinois Biometric Information Privacy Act ("BIPA"), finding that face geometry scans are not excluded from BIPA. However, on January 21, 2016, an Illinois federal judge dismissed a similar BIPA claim against a social media company, finding the company did not intentionally target Illinois residents in the company's alleged collection of biometric data from photographs posted on the site. The court thus found a lack of specific jurisdiction over the proposed class action.

New York Court Grants Motion to Dismiss in Data Breach Class Action
On December 28, 2015, the Eastern District of New York dismissed a putative class action against a crafts retailer for lack of standing. The case arose out of a 2014 security breach

in which hackers obtained credit and debit card information. The court found that plaintiffs could not establish out-of-pocket losses. The court also found that, as two years had passed, any risk of identity theft was not immediate.

Software Company to Provide Consumer Notice of Java Software Security Vulnerabilities
On December 21, 2015, upon determining that a software company was aware of significant security issues with its Java SE software and that it failed to inform consumers that installing updates would not remove the older vulnerabilities, the FTC required it to notify consumers and give consumers the ability to uninstall unsecured versions of the software. In addition to issuing consumer notice and appropriate software removal mechanisms, the company is required to post broad notifications on social media and its website.

Identity Protection Company Enters $100M Settlement with FTC over Violation of 2010 Order
On December 17, 2015, the FTC issued its largest monetary award ever. An identity theft protection company, LifeLock, agreed to pay consumers $100M to settle FTC charges that it violated the terms of a 2010 federal court order regarding the security of personal information and deceptive advertising. In the 2015 action, the FTC alleged that LifeLock: (i) failed to comprehensively secure consumer data, as ordered in 2010; (ii) falsely advertised that it had a comprehensive information security program in place; (iii) falsely advertised that it would notify consumers of indications of identity theft; and (iv) failed to abide by recordkeeping requirements.

Two Application Developers Settle FTC Charges of COPPA Violations
On December 17, 2015, two application developers settled a charge to pay a combined$360,000 in civil penalties for noncompliance with 2013 amendments to the COPPA. According to the FTC complaint, the developers allowed third-party advertisers to collect "persistent identifiers" from children without parental consent for collection and use of the information.

California Attorney General Settles Data Disposal Action with Telecommunications Provider for More Than $25M
On December 15, 2015, the California Attorney General and Alameda County District Attorney announced a settlement with a communications company to resolve allegations that the company both unlawfully disposed of hazardous waste and discarded records without first omitting or redacting private customer information. As part of the settlement, the company will pay $25.95M. The complaint alleged that the company disposed of "customer records without shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means," in violation of California Civil Code section 1798.81.

Fitness Center Operator Settles TCPA Claims
On December 2, 2015, a fitness center chain operator obtained final approval from the District of Minnesota to settle class allegations that the chain sent unsolicited commercial text messages in violation of the Telephone Consumer Protection Act ("TCPA"). The fitness operator will pay between $10M and $15M to affected consumers and an additional $2.8M for attorneys' fees and expenses.

Consumers Bring Class Actions against Retailers for Information Exposed on Receipts
On November 18, 2015, a proposed class action was filed in New York federal court against an appliance and electronics retailer under the Fair Accurate Credit Transaction Act ("FACTA") based on the company's printing of card data on receipts. The receipts allegedly exposed customers to fraud and identity theft. On January 5, 2016, a retail chain was accused of exposing too much customer information on receipts in violation of FACTA in Illinois federal court. And on January 14, 2016, a proposed class action was filed in the Southern District of Florida against a pet store chain based on similar violations of FACTA.

Retailer Data Breach Class Action Settlement Receives Approval
On November 17, 2015, a major retailer received approval to pay $10M to settle consumer class actions stemming from a 2013 data breach that compromised millions of payment cards. On January 27, 2016, the Eighth Circuit rejected an appeal related to the settlement. The district court also approved the payment of up to $6.75M in attorneys' fees and expenses in connection with the consumer settlement. On December 2, 2015, the retailer agreed to pay an additional $39M to banks and credit unions for losses from the same breach.

New Decision Raises Bar for FTC Enforcement Actions over Data Security Practices
A November 13, 2015, decision raised the bar for FTC enforcement actions over data security practices. In order for the FTC to maintain an enforcement action under Section 5 of the FTCA, it must show that consumer harm is not only possible, but that it is probable or actual. It is not enough merely to show that a practice led to "significant risk" of harm to consumers; rather, the FTC must show that direct harm to consumers is likely to actually occur or, in fact, has occurred. *For further discussion on the revised DFARS interim rule, see the* Jones Day Alert.

Legislative—Federal

House Representatives Challenge TPP's Electronic Commerce Chapter
In a January 12 letter to senior administration officials, several House Representatives challenged the Trans-Pacific Partnership ("TPP") trade pact's provision that excludes financial services from commitments on cross-border data flows and data localization. According to the letter, the exclusion is a "missed opportunity" to prohibit the increasingly prevalent localization requirements that impair American companies' competitiveness, reduce overall data security, and create inefficiencies. The TPP was signed in February but has not yet been ratified by Congress.

Medical ID Theft Penalty Bill Becomes Law
On December 28, 2015, the President signed into law the Patient Access and Medicare Protection Act of 2015, which establishes new penalties for the theft and use of Medicare and Medicaid numbers. The bill, which passed both houses of Congress on December 18, 2015, provides for a jail sentence of up to 10 years or a fine of up to $500,000 for the unauthorized purchasing, selling, or distributing of Medicare and Medicaid beneficiary numbers.

Cybersecurity Law Passes as Part of Omnibus Spending Bill
On December 18, 2015, the Cybersecurity Information Sharing Act took effect as part of the $1.15 trillion omnibus spending bill for 2016. The bill calls for improved measures to enhance the sharing of information relating to cybersecurity threats affecting the government and technology and manufacturing companies.

House Financial Services Committee Approves Bill to Establish National Data Breach Notification Standards
On December 9, 2015, the House Financial Services Committee approved legislation to establish a national data breach notification standard and preempt notification laws in 47 states and the District of Columbia. Although the bill has the support of banking industry groups, it faces opposition from consumer organizations, which argue that the bill would eliminate stronger existing state protections and prevent further state innovation. As written, the legislation requires covered entities to notify affected individuals of a breach of their sensitive personal information if it poses a "substantial harm" to the individuals.

House Passes Legislation Authorizing DHS Cybercrime Institute
On November 30, 2015, the House of Representatives agreed by voice vote to the Strengthening State and Local Cyber Crime Fighting Act, which formally authorizes the National Computer Forensics Institute ("NCFI") as part of an amendment to the Homeland

Security Act of 2002. The NCFI was established in 2008 and is operated by the Department of Homeland Security ("DHS") to train and equip law enforcement and prosecutors to investigate and prevent fraud, intellectual property theft, and other cybercrime. The legislation also directs the Secret Service to expand its network of electronic crime task forces and requires the NCFI to formally coordinate with the DHS's Federal Law Enforcement Training Center to help improve its training programs on cybercrime.

Legislative—States

States Introduce Data Breach Notification Legislation
Several state legislatures introduced measures in early 2016 to strengthen their respective state data breach notification requirements.

- On January 14, H.B. No. 1631 was introduced in Tennessee to redefine the time period within which a business must notify a consumer if the consumer's personal information was obtained by an unauthorized person and to identify employees of a business who use sensitive information unlawfully as "unauthorized persons."
- On January 13, S.B. No. 29 was introduced in Maryland to expand the definition of "personal information" to include state identification card numbers, passport numbers, and other identification numbers issued by the federal, state, or local government.
- On January 12, H.B. No. 1033 was introduced in Florida to require notice to the Agency for State Technology as well as the Florida Department of Legal Affairs in the event that 500 or more Florida residents have to be notified of a security breach.
- On January 12, H.B. No. 1357 was introduced in Indiana to: (i) specify that the data breach notification statute is not limited to breaches of computerized data; (ii) amend or define the terms "data owner," "data collector," and "data user," and to replace the term "personal information" with "sensitive personal information" and make conforming amendments; (iii) require a data user to post certain information concerning the data user's privacy practices on the data user's website; (iv) increase the amount of the civil penalty that a court may impose in an action by the attorney general under certain circumstances; (v) identify certain information that a data owner must include in a disclosure of a security breach; and (vi) specify the applicability of different enforcement procedures available to the attorney general under the statute.
- On January 8, L.B. No. 835 was introduced in Nebraska to amend the definition of "personal information" to include a user name or email address in combination with a password or security question and answer, and to require notice to the Nebraska Attorney General in the event of a breach of security.

Amendments to California and Oregon Data Breach Notification Statutes Take Effect
On January 1, amendments to the California and Oregon data breach notification laws took effect. For the third time in the past three years, California passed legislation updating California's data breach notification statute. The California amendments require a new breach notice format, define "encryption," expand the definition of "personal information," and clarify the substitute notice requirements. Among other updates, the Oregon amendments expand the definition of "personal information" and provide new threshold requirements and new exemptions for data breach notifications.

[Return to Top]

Canada

Canadian Business Organization Forms Exchange to Share Information about Cybersecurity Threats

On December 11, 2015, the Canadian Council of Chief Executives, a not-for-profit organization composed of CEOs from Canadian companies, announced plans to establish a not-for-profit organization called the Canadian Cyber Threat Exchange ("CCTX"). CCTX will aim to help businesses and consumers guard against cyber attacks by allowing companies, the government, and research institutions to share information about cyber threats and vulnerabilities. It also will provide members and the general public with analysis on cybersecurity issues.

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, Jeremy Close, and Anand Varadarajan.

[Return to Top]

Latin America

Brazil

Brazilian Judge Freezes Social Media Messenger Application for 48 Hours
On December 17, 2015, São Paulo prosecutors filed a claim against Facebook Brazil to have its messaging application WhatsApp suspended after Facebook refused to disclose certain users' personal information in connection with a criminal case. A state judge took down the application for 48 hours when Facebook failed to comply with the order. Facebook immediately appealed and had the order reversed within 12 hours of the service suspension.

Right of Reply Bill Takes Effect
On November 12, 2015, Brazil's right of reply legislation (source document in Portuguese) took effect. Under the law, if a publication allegedly harms the reputation of an individual or organization, media companies must publish the affected person's written reply to the offense, published at no cost and with equal proportion. The affected person has 60 days to exercise the right of reply following the date of the publication.

Colombia

Colombia Initiates National Database Registration Process
On November 3, 2015, the Colombian Superintendence of Industry and Commerce (*Superintendencia de Industria y Comercio*) enacted a regulation (source document in Spanish) ordering private companies listed with local chambers of commerce and state-owned companies to register their databases with the National Database Registry (*Registro Nacional de Base de Datos* or "RNDB"). The agency, which oversees data protection in Colombia, mandated that covered entities disclose to RNDB their database content, information security policies, sources of personal data, information regarding national and international transfer of personal data, complaints reported by users, and cases involving data breach.

Mexico

INAI Publishes Guidelines on Posting Privacy Notices on INAI's Website
On January 18, the Mexican data protection authority (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* or "INAI") set forth guidelines for data controllers (source document in Spanish) on using INAI's website as a compensatory measure to deliver privacy notices to data owners. Data controllers may use compensatory measures when it is impossible to deliver privacy notices directly to data owners or if such delivery involves disproportionate efforts. Under the guidelines, a data controller may use INAI's website to publish a privacy notice if: (i) the data controller is authorized by INAI to implement a compensatory measure or is exempted from obtaining such authorization; (ii) does not have a website of its own; and (iii) the

privacy notice complies with all legal requirements.

INAI Presents Recommendations to Prevent Identity Theft
On January 17, INAI published its recommendations to prevent identity theft (source document in Spanish). According to the report, most offenses are committed via data theft from emails, mobile phones, and electronic tablets. As such, INAI recommends safeguarding all personal documents, passwords, or access codes; limiting the amount of personal information published on or shared through social networks; and avoiding the use of public computers to carry out bank transactions or online shopping.

Mexico's Data Protection Authority Issues Guidelines for Conducting Administrative Procedures
On December 9, 2015, Mexico issued the Guidelines for Rights Protection, Investigation and Verification, and Sanctioning Procedures (source document in Spanish) in Mexico's Official Federal Gazette (*Diario Oficial de la Federación*). The Guidelines outline rules on notices, admission of complaints, and evidence for a variety of INAI data privacy and protection matters. Although the Guidelines became effective on December 10, 2015, unresolved and pending investigations will still be subject to the procedures of the Mexican data protection law (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*).

INAI and SAT Agree to Information Exchange
On November 9, 2015, the INAI and the Mexican tax authority (*Servicio de Administración Tributaria* or "SAT") entered into a collaboration agreement (source document in Spanish) to exchange tax information of data privacy offenders. Per the agreement, SAT will provide INAI the tax returns of individuals and entities that violate data protection laws in order for INAI to know their economic capacity and impose relevant fines.

Peru

District of San Isidro in Lima Regulates Use of Drones
On November 9, 2015, the District of San Isidro in Lima enacted a regulation (source document in Spanish) governing the use of drones. As set forth in the regulation, drones may fly only in open, nonresidential areas and may be operated only by an adult or adult-supervised child. Offenders may be fined up to $1,900 Peruvian soles for violations. The regulation does not apply to the use of drones by public entities for government or public safety activities.

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 Commission Launches Public Consultation on Public–Private Partnership on Cybersecurity
On December 18, 2015, the EU Commission issued a public consultation seeking "stakeholders' views on the areas of work of the future cybersecurity public–private partnership as well as on potential additional policy measures that could stimulate the European cybersecurity industry."

EU Parliament and Council Agree on EU Data Protection Reform
On December 15, 2015, the EU Parliament and the Council agreed to terms on the EU Data Protection reform. This reform consists of two instruments: the General Data Protection Regulation ("GDPR") to "enable people to better control their data" and the

Data Protection Directive for "the police and criminal justice sector." The Commission also published questions and answers on December 21, 2015, to highlight the key changes instituted by the reform. *For further discussion on the GDPR, see the* Jones Day Alert*.*

EU Parliament and Council Reach Agreement on NIS Directive
On December 7, 2015, the European Parliament and the Council reached an agreement on common rules to strengthen network and information security across the EU. The new network and information security Directive ("NIS Directive") constitutes the first step for the development of an EU harmonized framework for cybersecurity. *For further discussion on the NIS Directive, see the* Jones Day Alert*.*

EU Commission Issues Guidance on Transatlantic Data Transfers
On November 6, 2015, the Commission issued guidance on transatlantic data transfers following invalidation of the safe harbor scheme by the *Schrems* ruling of the Court of Justice. The guidance analyzes the consequences of the judgment and sets out the alternative mechanisms for transfers of personal data to the United States.

Article 29 Working Party

Article 29 Working Party Issues Guidelines on Personal Data Exchange for Tax Purposes
On December 16, 2015, the Article 29 Working Party published data protection guidelines regarding the automatic exchange of personal data for tax purposes. The guidelines, which are addressed to Member States, discuss data protection safeguards in three different settings: (i) exchange of personal data between EU Member States; (ii) exchange of personal data between an EU Member State and a third country that has been the subject of an adequacy decision by the EU Commission, and (iii) exchange of personal data between an EU Member State and a third country that has not been the subject of an adequacy decision by the EU Commission.

Article 29 Working Party Updates Opinion 8/2010 on Applicable Law
On December 16, 2015, the Article 29 Working Party amended its Opinion 8/2010 on applicable law to discuss the EU Court of Justice's May 2014 ruling as it relates to the "inextricable link" between advertising activities and data processing, the lack of "one-stop shops" within the EU, and the applicability of EU law to companies located outside the EU.

Article 29 Working Party Issues an Opinion on the Draft Protection Directive
On December 1, 2015, the Article 29 Working Party adopted an opinion (*see* corresponding cover letter) containing specific comments on the text of the future Data Protection Directive. The opinion includes recommendations for adhering to the principles of the Charter of Fundamental Rights and ensuring consistency with the GDPR.

European Data Protection Supervisor (EDPS)

EDPS Warns Against Intrusive Surveillance
On December 15, 2015, EDPS released an opinion on the dissemination and use of intrusive surveillance technologies. In the opinion, EDPS assessed existing EU standards and discussed updated and consistent policies to mitigate the risks posed by the unregulated growing market for the selling, distribution, and (dual) use of spyware.

EDPS Discusses Support for EU Legislator
On December 10, 2015, EDPS announced its support for the EU legislator on security matters but recommended rethinking the EU Passenger Name Record in favor of "new approaches on data gathering, analysis, cross border cooperation information sharing and use of existing systems among law enforcement bodies."

EDPS Encourages New Debate on Big Data

On November 19, 2015, EDPS issued a report titled Meeting the Challenges of Big Data. In it, EDPS states its intent to launch an open discussion with legislators, regulators, industry, IT experts, academics, and citizens to explore the social benefits of Big Data and the challenges of protecting fundamental rights and individual freedoms.

European Network and Information Security Agency (ENISA)

ENISA Issues Guidelines for National and Governmental CSIRTs
On January 11, ENISA published a report focusing on the maturity of national and governmental Computer Security and Incident Response Teams ("CSIRTs") and the Trusted Introducer1 certification scheme for CSIRTs as an indicator of the maturity level of teams.

ENISA Publishes Statement on Privacy in Big Data
On December 17, 2015, ENISA issued a report titled Privacy by Design in Big Data. The report stresses the limits of big data processing and encourages the integration of appropriate data protection safeguards in the core of the analytics value chain.

ENISA Releases Report Relating to Cloud Computing in Finance Sector
On December 7, 2015, ENISA released a report outlining recommendations to financial institutions, regulators, and cloud service providers on the secure adoption of cloud services in the finance sector. ENISA identified the most pressing short-term issues for promoting adoption of cloud services as "reducing the information gap, [] providing clearer and fit for purpose regulatory guidance, [and] simplifying and streamlining compliance."

Belgium

Privacy Commission Supports Real-Time Access to CCTV Railway Images by Railway Police
On December 16, 2015, the Privacy Commission issued a statement (source document in French) supporting draft legislation providing for real-time access to CCTV images of railways by railway police officers.

Privacy Commission Provides Opinion on Draft Legislation on Electronic Mortgage and Life Insurance Data
On December 16, 2015, the Privacy Commission adopted an opinion (source document in French) supporting draft legislation regulating the electronic exchange of data relating to mortgages and individual life insurance.

Privacy Commission Provides Opinion on PNR Draft Legislation
On December 16, 2015, the Privacy Commission adopted an opinion (source document in French) on passenger names recording ("PNR"). The Commission commended the guarantees and lack of extensive profiling but criticized the extension of data collection to migration control and the five-year retention period.

Privacy Commission Comments on Draft Legislation Introducing Electronic Communications in Judicial Procedure
On December 16, 2015, the Privacy Commission issued an opinion (source document in French) on draft legislation establishing electronic communications in judicial procedures. The Privacy Commission proposed modifications such as enhanced security via encryption, more clarity on controllers, and the establishment of data retention periods.

Belgian Court Decides on Website Plug-ins
On November 9, 2015, a Belgian Tribunal ordered a social media company to cease recording the internet navigation habits of Belgian web users and issued a €250,000 fine for each day of noncompliance. The Privacy Commission also issued a press release (source document in French) summarizing the case and the main arguments. On

December 4, 2015, a contact group composed of the Belgian, Dutch, French, and Spanish data protection authorities published a common statement (source document in French) requesting the company to comply with this judgment throughout the EU territory.

France

Draft Legislation Contemplates Raising Penalty Amounts
On January 22, the French National Assembly finished its first review of the draft law for a Digital Republic (source document in French). In the legislation, representatives proposed to raise penalties to a maximum of €20M or 4 percent of a company's profits for violations of applicable law.

French Consumers Association Sues Toy Manufacturer Following Data Breach
On December 23, 2015, a French consumers association announced (source document in French) that it would file a complaint against a toy manufacturer for system vulnerabilities that allegedly led to a large-scale data breach. The manufacturer sold connected toys that allegedly collected data as children accessed the internet, and more than one million users' data was affected by the breach.

French Constitutional Council Approves International Electronic Communications Surveillance Act
On November 26, 2015, the Constitutional Council approved (source document in French) Article 1 of the Act on International Electronic Communications Surveillance. Article 1 modified Articles L. 854-1, L. 854-2, L. 854-5, and L. 854-9 of the French Public Security Code and amended key provisions of the Intelligence Act, which previously had been rejected by the Constitutional Council.

French Conseil d'Etat Approves CNIL Sentence Issued Against Software Company
On November 8, 2015, the Conseil d'Etat approved the penalty issued by the French Data Protection Authority ("CNIL") against a consulting company for two years of noncompliance with French data protection regulations (source documents in French). CNIL concluded that the company's video surveillance measures were not justified by the nature of the employees' work. CNIL further concluded that the company failed to adequately disclose surveillance information to its employees or implement measures to secure access to the video recordings.

CNIL Sanctions Eyewear Store for Failing to Comply with Summons
On November 5, 2015, CNIL issued (source document in French) a €50,000 fine against a company for failing to comply with data protection regulations. CNIL summoned the company to provide information on its data protection practices, and after monitoring the company for several weeks, found that it failed to implement adequate measures to protect consumer data.

Germany

German Parliament Adopts Bill Strengthening Consumer Data Protection Rights
On December 17, 2015, the German Parliament adopted legislation (source document in German) allowing civil claimants to enforce violations of data protection provisions protecting consumer rights (*Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts*). Under the proposed legislation, consumer associations and other defined associations would be allowed bring collective actions for data protection violations. The new law awaits adoption by the Federal Council before taking effect.

German Data Protection Authorities Audit Dating Portals
On December 11, 2015, the German Data Protection Authorities of Bavaria, Baden-Württemberg, Berlin, and Hamburg published (source document in German) the results of

a joint audit of various dating portals. The report identifies areas for data security improvements in the sites' login procedures, handling of information requests, transparency of privacy policies, user identification and age verification, and access to user communication.

German Court Holds Email Provider Subject to Telecommunications Law
On November 11, 2015, the Administrative Court of Cologne ruled (source document in German) that an email provider was subject to notification obligations under the nation's telecommunications law. The court concluded that because the provider offered a telecommunications service, it must send specific notifications to the Federal Network Agency (*Bundesnetzagentur*).

Italy

Italian Data Protection Authority Approves Electronic Register for Last Will and Testament
On November 25, 2015, the Italian data protection authority ("DPA") issued an opinion (source document in Italian) approving the communication of data to the Electronic Register for Last Will and Testament. The Ministry of Justice is charged with establishing technical rules for the transmission of last will data to ensure that adequate safeguards are provided to testators and that such data remains secret until the death of the testator.

Italian Data Protection Authority Orders E-Commerce Company to Cease Illicit Customer Profiling
On November 18, 2015, the DPA issued a decision (source document in Italian) ordering an e-commerce company to cease its illicit use of personal data belonging to more than 300,000 people. The company profiled customers' online habits, preferences, and purchase history in order to send them personalized newsletters. The DPA stated that such activity will be deemed lawful only if the company sends prior notification to the DPA and sets forth a limited retention period for the data.

The Netherlands

DDPA Revokes Penalty Imposed on Social Media Company
On January 14, the Dutch Data Protection Authority ("DDPA") revoked the penalty (source document in Dutch) imposed on a social media company for refusing to provide the DDPA with sufficient information to assist the DDPA's investigation into the applicability of the Data Protection Act.

Amsterdam District Court Approves Search Engine's Refusal to Delete Search Results
On January 7, an Amsterdam District Court denied (source document in Dutch) a journalist's request to order an internet search engine to delete a search result showing a newspaper article on plagiarism committed by the journalist. In its opinion, the Court reasoned that: (i) the journalist is still active; (ii) the information in the article is relevant for the journalist's target audience; and (iii) prospective employers should be able to judge the severity of the offense committed by the journalist.

Amendments to Dutch Data Protection Act Take Effect
On January 1, key amendments to the Dutch Data Protection Act took effect. These amendments included: (i) an obligation to notify the DDPA of data breaches and (ii) an increase in the amount of the fines (source document in Dutch) the DDPA may impose. The DDPA's final policy rules (source document in Dutch) explain the parameter of the new notification obligations and how the DDPA will use its authority to impose fines for violations of the Act.

Dutch House of Representatives Examines New Computer Crime Act
On December 28, 2015, the House of Representatives began considering a bill for a third

computer crime act (source document in Dutch). The draft legislation authorizes investigation officers to hack computers under special circumstances, allows communication service providers to render certain data inaccessible, and criminalizes the handling of data acquired through illegal wiretapping. The bill awaits approval from both the Dutch House of Representatives and Senate before taking effect.

DDPA Investigates Dutch Healthcare Authority's Diagnosis Information System
On December 17, 2015, the DDPA began investigating (source document in Dutch) the Dutch Healthcare Authority's ("DHA") Diagnosis Information System's compliance with the data privacy requirements set forth by the DDPA. According to the DDPA, because the DHA processes sensitive personal data, it must take effective measures to reduce the linkability of a dataset with the original identity of a data subject. The DHA announced that it will stop providing data from the DIS to third parties while the investigation is ongoing.

DDPA Finds WiFi-Tracking Practice Unlawful
On December 1, 2015, the DDPA concluded (source document in Dutch) that a company violated data protection regulations by gathering excessive WiFi-tracking location data from mobile devices of store visitors without consent. Following the investigation's results, the company stated it had taken measures to mitigate the excessive data collection.

Spain

SDPA Updates European DPAs on Search Engine's Development of Privacy Policies
On January 11, the Spanish Data Protection Agency ("SDPA") informed (source document in Spanish) other European data protection authorities about the changes a search engine has implemented to its privacy policies. In light of recent actions against the search engine, the SDPA has been monitoring the search engine's policies with respect to individual information, consent, and exercise of privacy rights.

SDPA to Collaborate with Counsels of Consumers and Users
On December 14, 2015, the SDPA and the Council of Consumers and Users signed a collaboration agreement (source document in Spanish) establishing protocols for the processing of personal data used in irregular services contracting.

SDPA Publishes Report on Video Surveillance in Schools
On December 11, 2015, the SDPA released a report (source document in Spanish) issuing recommendations on the use of video surveillance in school centers. The SDPA discussed the need for video surveillance for security purposes but recommended limitations such as a 10-day preservation period, restricted access policies, and alignment with the Spanish data protection regulations.

SDPA Comments on Right to Be Forgotten
In December 2015, the SDPA published recommendations (source document in Spanish) on the right to be forgotten. The SDPA noted the right to limit the universal distribution of general search engines when the information is obsolete or has no relevance or public interest, even if the original publication is legitimate.

SDPA Publishes 2015–2019 Strategic Plan
On November 20, 2015, the SDPA published its Strategic Plan 2015–2019 (source document in Spanish), which targeted efficiency and optimization of data protection frameworks, alignment with the new European data protection regulations, and annual publications of compliance.

Spanish Supreme Court Rules on Right to Be Forgotten
On November 15, 2015, the Spanish Supreme Court ordered (source document in Spanish) a search engine to take down certain search results of two persons convicted for smuggling in 1985. Because the first search yielded an old newspaper article about the

crime, the Court ruled that the data was no longer adequate for its original purpose and infringed on privacy rights. The Court also distinguished the duties of newspaper libraries, which do not have the duty to remove any information but do have a duty to prevent such information from appearing on search engines.

Spanish Court Rejects Blacklisting of Workers
On November 12, 2015, the Spanish Supreme Court prohibited (source document in Spanish) the maintenance and transfer of files blacklisting workers. The Court explained that transfers of such data among employers would infringe on the fundamental privacy rights of employees because the data would be shared without their consent and without any applicable legal exceptions.

United Kingdom

UK Government Proposes Crackdown on Nuisance Calls
On January 12, the UK government initiated a consultation period for proposals to require direct marketing companies to implement call line identification for marketing calls.

ICO Calls for Stricter Sentences for Data Thieves
On January 11, the Information Commissioner ("ICO") issued a statement calling for tougher sentences against people convicted of stealing personal data. Citing an incident in which a car rental employee sold almost 28,000 customers' records for £5,000 and was fined only £1,000, the ICO stated that he would like to "see the courts given more options: suspended sentences, community service, and even prison in the most serious cases."

ICO Signals More Fines for Companies Making Nuisance Calls
In 2015, the ICO, in response to more than 170,000 complaints, imposed more than a million pounds in penalties on companies making nuisance calls and text messages. The ICO has indicated that he will take a similarly active approach to enforcement in 2016.

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

China Passes Anti-Terrorism Law with Cybersecurity Provisions
On December 27, 2015, China's legislature adopted a new anti-terrorism law with several data privacy and cybersecurity provisions. Notably, in connection with state terrorism investigations, internet service providers must provide their encryption keys to state authorities and must require the real name registration of all users of their websites. The law also provides for stricter oversight of Chinese internet sites with content monitoring and reporting obligations.

Hong Kong

PCPD Reports Need for Stronger Protection and Enforcement in 2016
On January 26, the Office of the Privacy Commissioner for Personal Data ("PCPD") reported that it received a record number of complaints in 2015. Although the number of enforcement actions dropped in 2015 compared to 2014, several more cases were referred to the police for criminal investigation and prosecution. In the report, the PCPD Commissioner urged "all businesses and organizations to ensure the proper handling and disposal of personal data collected, and to take all practical steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use."

Hong Kong Court Convicts and Fines Individual for Providing Data for Use in Direct Marketing
On December 30, 2015, the PCPD reported the convictions and fines against an individual who gave personal data to a third party for direct marketing purposes. According to the complaint initially filed with PCPD, the defendant obtained the complainant's information at a social function and handed it to a third party who later attempted to sell insurance services to the complainant. The individual was fined HK$5,000.

PCPD Investigates Security Vulnerability of Town Website
On December 23, 2015, the PCPD announced an investigation into SanrioTown website's security vulnerability that could have exposed the personal data of up to 3.3 million people. Compromised data includes name, email address, date of birth, and encrypted password.

PCPD Investigates Data Leakage Incident
On December 1, 2015, the PCPD initiated an investigation into a data leakage incident involving a children's toy company. Although not required to report data leaks, the company voluntarily disclosed the incident to the PCPD and informed the agency that it may have exposed five million customer accounts. The PCPD is still investigating whether the company had adequate safeguards in place.

Japan

Japan Amends Personal Information Protection Act and Reorganizes Specific Personal Information Protection Commission
On January 1, the amendments (source document in Japanese) to the Law to Amend Personal Information Protection Act and the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure partially took effect. Effective the same day, the Specific Personal Information Protection Commission was reorganized and renamed the Personal Information Protection Commission ("PIPC"). Once the amendments take full effect in 2018, the PIPC will function as the Privacy Commissioner responsible for enforcing the My Number Act (Japanese social security number law) and implementing the various guidelines implemented by the amendment.

Japanese Government Issues Cybersecurity Guidelines
On December 28, 2015, the Ministry of Economy, Trade and Industry of Japan ("METI"), in collaboration with Information-Technology Promotion Agency, published the Cybersecurity Management Guidelines (source document in Japanese). In response to growing concerns about cyber attacks against private companies, METI prepared guidance for company management on establishing security measures and investing in IT security systems. The guidelines set forth three principles and 10 important items, including the appointment of a Chief Information Security Officer and the creation of a security and disclosure policy in the event of a data breach.

Taiwan

Taiwan Office of President Amends Personal Information Protection Act
On December 30, 2015, Taiwan's Office of the President set forth amendments (source document in Mandarin) to the nation's Personal Information Protection Act. These changes include additional consent and protection rules for collecting and processing "special" personal information, modification to the notification requirements for data processors, and the removal of imprisonment as a potential penalty for violations. The changes will take effect before April 2016.

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

[Return to Top]

Australia

Mandatory Data Breach Notification Bill Open for Public Comment
In early 2016, the Australian government invited submissions on proposed legislation that would require mandatory notification of a data breach to the Office of the Australian Information Commissioner ("OAIC"). Currently, data breach notification to the OAIC is voluntary except for special circumstances, such as breaches involving medical records. As proposed, the legislation would require notification in any instance of a loss or misuse of personal information creating a risk of serious harm to affected individuals.

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

[Return to Top]

Jones Day Cybersecurity, Privacy, and Data Protection Lawyers

Emmanuel G. Baud
Paris

Wolfgang G. Buchner
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

Jonathan Little
London

Kevin D. Lyles
Columbus

John M. Majoras
Columbus/Washington

Todd S. McClelland
Atlanta

Kristen P. McDonald
Atlanta

Jason McDonell
San Francisco

Carmen G. McLean
Washington

Daniel J. McLoon
Los Angeles

Janine C. 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

Michael G. Morgan
Los Angeles

Sergei Volfson
Moscow

Olivier Haas
Paris

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 Gutiérrez Ponce
Madrid

Aaron M. Healey
Columbus

Elaine Ho
Singapore

Nandini Iyer
Silicon Valley

Bastiaan K. Kout
Amsterdam

Colin Leary
San Francisco

Nicole M. Perry
Houston

Scott B. Poteet
Dallas

Brandy H. Ranjan
Columbus

Jessica M. Sawyer
Los Angeles

Raquel Travesí
Madrid

Anand Varadarajan
Dallas

Natalie 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].