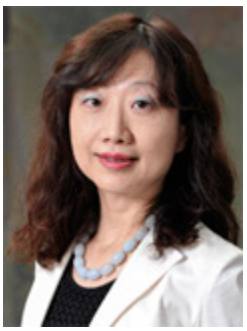
JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 10 | June 2016

JONES DAY

Jones Day Attorney Spotlight: Michiru Takahashi



The complicated fabric of privacy and data security regulations in Asia continues to challenge multinational clients. The last few months have seen significant regulatory changes within Asia—strengthened enforcement measures in many countries, a more robust Japanese Personal Information Protection Act, the creation of a Personal Information Protection Commission in Japan, and others. These changes, coupled with developments in Europe and the Americas, compel businesses with a global footprint to constantly monitor and update their compliance practices.

Michiru Takahashi, a partner based in Tokyo, Japan, assists clients on various privacy issues, including cross-border transfers of personal data, internal compliance programs, and data breach response. She regularly advises Japan-based multinational clients on global data protection issues as well as cross-border data transfers from Europe to the Americas to Asian Pacific nations.

Michiru's experience in these areas makes her a valuable asset for Jones Day's global Cybersecurity, Privacy & Data Protection team as well for clients situated throughout the world.

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

Guillermo E. Larrea
Mexico City

Michiru Takahashi
Tokyo

Adam Salter
Sydney

Editor-in-Chief: Anand Varadarajan

Practice Directory

HOT TOPICS IN THIS ISSUE

United States

Policy, Best Practices, and Standards

FTC Urges FCC to Protect Privacy in New Television Set-Top Box Rulemaking
On April 22, the Federal Trade Commission ("FTC") Bureau of Consumer Protection issued a comment urging the Federal Communications Commission ("FCC"), in its rules expanding commercial availability of television set-top boxes, to require third-party set-top box manufacturers to certify that their products comply with the same privacy regulations applicable to cable and satellite providers. The Director also emphasized the need for third-party set-top box makers to issue consumer-facing statements regarding compliance that would be enforceable by the FTC.

FTC Scrutinizes App Developers' Audio Monitoring Software
On March 17, the FTC issued warning letters to 12 app developers using audio beacon technologies in their apps. The technologies are designed to monitor consumers' television and other video viewing habits for the purpose of facilitating targeted advertising and analytics. The FTC warned companies that obtaining permission to access a device's microphone is not sufficient; apps using these technologies should disclose that audio will be recorded in the background and that viewing habits may be logged.

Critical Infrastructure

NIST Analyzes Feedback from Critical-Infrastructure Leaders
On March 24, the National Institute of Standards and Technology ("NIST") published an analysis of feedback on the voluntary, federally led Cybersecurity Framework received from critical-infrastructure leaders and others. NIST's analysis of the feedback affirms the framework's current uses, recommends refinements, and suggests future directions.

NIST Announces Updates to Guidance on Strengthening Remote-Access Data Security
On March 14, NIST announced upcoming updates to guidance on telework to include the latest technology available to strengthen an organization's remote-access data security. As part of the update, NIST sought comments on two draft publications through April 15.

Financial Services Roundtable Commends NIST

Security Strategy

RECENT AND PENDING SPEAKING ENGAGEMENTS

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

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

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

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

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

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

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

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

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

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

Cybersecurity Framework
On February 25, the Financial Services Roundtable ("FSR") issued a press release praising the NIST Cybersecurity Framework as "the 'Rosetta Stone' of Cross-Sector Cyber Defense for U.S. Companies." The FSR stated that the NIST framework allows a diverse set of industries to easily apply common approaches to assess and prevent cyber attacks. The press release warned against regulation schemes that are not aligned with the NIST framework, which can require organizations to comply with multiple regimes that potentially conflict.

Retail

District Court Finds Online Retailer Not Authorized to Charge for Kids' In-App Purchases
On April 26, the FTC prevailed on summary judgment against an online retailer in the U.S. District Court for the Western District of Washington, alleging that the retailer billed consumers for unauthorized in-app purchases made by children. The court found the retailer's disclosure about the possibility of in-app purchases within otherwise free apps was insufficient to inform consumers about the charges children could incur within the app. The court order seeks further information from the parties regarding out-of-pocket costs to consumers for the unauthorized purchases

Defense, National Security, Economic Espionage, and Other Criminal Matters

Presidential Telecommunications Group Suggests "Good Samaritan" Framework to Promote Data Sharing
On May 11, the President's National Security Telecommunications Advisory Committee met in Silicon Valley and suggested a "Good Samaritan" framework to allow both companies and individuals to provide data to the government following a cyber or terrorist attack or natural disaster without fear of subsequent privacy lawsuits. The framework is part of the Advisory Committee's Report on "Big Data Analytics" and was supported by numerous high-ranking defense officials.

FBI Names New Associate Executive Assistant Director for Criminal, Cyber, Response and Services Branch
On April 27, the Federal Bureau of Investigations ("FBI") announced a new associate executive assistant director of the Criminal, Cyber, Response and Services Branch. His responsibilities will include overseeing the development of the FBI's cyber policy and strategy.

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

Digital Media Meets Data Nationalism, Legal Frontiers in Digital Media, Mountain View, CA (May 19)
Jones Day Speaker: Jeff Rabkin

Panel Discussion on the Privacy Shield and Making Sense of International Data Flows, IAPP KnowledgeNet, Washington D.C. (May 12)
Jones Day Speaker: Jennifer Everett

What to Do When … You've Been Hacked, Jones Day (May 12)
Jones Day Speakers: Greg Silberman, Jeff Rabkin, Richard DeNatale

FFIEC Cybersecurity Assessment Tool Deep Dive Workshop, Mortgage Bankers Association, Dallas, TX (May 12)
Jones Day Speakers: Jay Johnson, Lisa Ledbetter, Richard Milone

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

EU/U.S. Privacy Shield and International Data Transfers: Insights from the Regulator, IAPP KnowledgeNet, Munich, Germany (May 3)
Jones Day Speakers: Mauricio Paez, Undine von Diemar

International Data Transfers, Practice Days Data Protection, Cologne, Germany (April 29)
Jones Day Speaker: Undine von Diemar

Panel discussion on Privacy Shield, AmChamSpain, Madrid, Spain (April 28)
Jones Day Speaker: Paloma Bru

Finding Ways to Advance and Improve the Use of Self-Regulatory Approaches, Cybersecurity Regulators Forum for Independent and Executive Branch Regulators (April 21)
Jones Day Speaker: Mauricio Paez

Update on the General Data Protection Regulation, Jones Day, Frankfurt, Germany (April 14)
Jones Day Speaker: Undine von Diemar

SpyEye Malware Hackers Receive Prison Sentences Totaling More Than 24 Years
On April 20, the Department of Justice ("DOJ") announced that the two international hackers who created the SpyEye Trojan malware were sentenced to 15 years and nine-and-a-half years, respectively, in federal prison. From 2010 through 2012, SpyEye was the preeminent banking Trojan that allowed the theft of login information for bank accounts, PINs, and credit card information.

U.S. District Court Sentences Former NRC Employee to 18 Months in Prison for Spear-Phishing Attack
On April 11, the U.S. District Court for the District of Columbia sentenced a former employee of the U.S. Nuclear Regulatory Commission ("NRC") to 18 months in prison after he pleaded guilty to accessing a protected computer without authorization and intentionally damaging it by sending emails to particular Department of Energy employees that would install a virus on their computers upon opening it.

DOJ Announces Indictment of Seven Iranians Accused of Computer Hacking
On March 24, seven Iranian hackers were indicted on computer hacking charges relating to distributed denial of service ("DDoS") attacks directed at 46 U.S. financial sector businesses from 2011 through 2013. The hacks caused tens of millions of dollars in remediation damages and left hundreds of thousands of Americans without access to their online banking accounts.

U.S. Attorney General Addresses RSA Conference on Cybersecurity
On March 1, the U.S. Attorney General addressed the RSA Conference on Cybersecurity and described law enforcement's various efforts to combat cybercrime. Among other things, she touted the recent successful international operation that led to the shuttering of multiple "dark market" websites and discussed ongoing negotiations with the United Kingdom to allow UK authorities to investigate corporate accounts used by non-U.S. citizens or residents.

Financial Services

Credit Union National Association and National Association of State Credit Union Supervisors to Co-Host Cybersecurity Symposium
On August 1–2, the Credit Union National Association and National Association of State Credit Union Supervisors will host a third annual cybersecurity symposium. The event will focus on best practices and procedures that protect credit

Legal Issues Arising from a Data Breach, Experian Credit Industry Law Conference (April 5)
Jones Day Speaker: Dan McLoon

Panel discussion on Privacy and Cybersecurity in Latin America, Jones Day, Miami, FL (April 1)
Jones Day Speakers: Mauricio Paez, Todd McClelland, Guillermo Larrea, Paloma Bru

The World of IoT Policy, Laws, and Regulations (U.S. and International), Internet of Things (IoT) National Institute, Presented by ABA Section of Science and Technology Law (March 31)
Jones Day Speaker: Mauricio Paez

RECENT AND PENDING PUBLICATIONS

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

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

IoT Devices Raise a Host of Privacy Issues, *San Francisco Daily Journal* (May)
Jones Day Authors: Jeff Rabkin, Mike LaMarca

Texas High Court Finds Texas Uniform Trade Secrets Act Can Exclude Opposing Party from Injunction Proceedings, Jones Day Publications (May)
Jones Day Authors: Bob Kantner, Keith Davis, Joe Beauchamp, Thomas Allen, Jay Johnson

Supreme Court Rejects Lawsuits by Plaintiffs Who Cannot Show "Real" Injury, Jones Day Publications (May)
Jones Day Authors: Meir Feder, Dan McLoon, John Vogt, Darren Cottriel, Brian Murray, Joshua Stillman, Rajeev Muttreja

European Antitrust Enforcers Move on Holders of Big Data, Jones Day Publications (May)
Jones Day Authors: Multiple

Fourth Circuit Confirms Coverage for Data Breaches Claims Under Traditional CGL Insurance Policies, Jones Day Publications (April)
Jones Day Authors: Richard DeNatale, Richard Milone, Celia Jackson

unions from the latest cyber threats.

Financial Services Sector Coordinating Council Releases Cyber Insurance Purchaser's Guide
On April 14, the Financial Services Sector Coordinating Council published a guide for organizations looking to mitigate the risks of a cybersecurity incident through the purchase of an insurance product. The guide provides an overview of the cyber insurance market and identifies key questions that a potential cyber insurance policyholder should consider.

SEC Brings Enforcement against Broker-Dealer for Failure to Adopt Policies and to Ensure Security of Customer Information
On April 12, the SEC instituted cease-and-desist proceedings against a broker-dealer and two of its principals based on the broker-dealer's "failure to adopt written policies and procedures reasonably designed to insure the security and confidentiality of customer records and information" and "to make and keep certain communications relating to its business." The SEC alleged, in part, that the broker-dealer violated securities laws by using email addresses other than those with its domain name to receive faxes containing sensitive customer information.

SEC Director Acknowledges SEC's Efforts to Bolster Cybersecurity
On March 14, at the Investment Company Institute's 2016 Mutual Funds and Investment Management Conference, the SEC Director for the Division of Investment Management responded to concerns that enhancing the reporting framework for investment companies and advisers would make the SEC a target for cyber criminals. He noted that the SEC was addressing cybersecurity in order to protect the information that it collects. He specifically recounted that the SEC chair had requested "funds from Congress to maintain and enhance the Commission's cyber capabilities" and that the Commission was "implementing certain cybersecurity protocols that are consistent with" recommended standards.

Digital Health Law Update, Vol. II, Issue 2, Jones Day Publications (April)
Jones Day Authors: Richard Milone, Jessica Jardine Wilkes, Laura Koman, Whitney Ehlin, Olaf Hohlefelder

Cybersecurity's Moment and What it Means for Financial Services, Jones Day Publications (March)
Jones Day Authors: Lisa Ledbetter, Todd McClelland, Mauricio Paez, Albert Rota, Hunter Wiggins, Jay Johnson, Eitan Levisohn

SciTech Profile: John Pendergast, Human Rights Activist and Founding Director of the Enough Project, *The SciTech Lawyer* (March)
Jones Day Author: Cynthia Cwik

EU and U.S. Release Terms of Privacy Shield, Jones Day Publications (March)
Jones Day Authors: Mauricio Paez, Undine von Diemar, Jonathon Little, Elizabeth Robertson, Paloma Bru, Olivier Haas, Laurent De Muyter, Jennifer Everett, Michael La Marca

Cyberattacks Are Increasing, Prevention Lagging in Latin America, *Daily Business Review* (AMLAW) (March)
Jones Day Authors: Guillermo Larrea, Paloma Bru

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

Transportation

Department of Homeland Security Notes Continued Deficiencies in TSA's Security Technology Integrated Program
On May 9, the Department of Homeland Security Office of the Inspector General issued the results of an audit into the Transportation Security Administration's ("TSA") Security Technology Integrated Program ("STIP"). The audit assessed the current extent of TSA deficiencies and corrective actions, and provided recommendations to TSA to improve control, security, and functionality of STIP IT assets.

Health Care/HIPAA

FTC Launches New Mobile Health App Interactive Tool
In April, mobile health app developers began using the FTC's new Mobile Health App Interactive Tool to obtain legal guidance regarding issues facing their app. The tool asks developers high-level questions about the health app's function, the data it collects, and the services it provides. The tool then points developers to information about federal laws the app might trigger, including the FTC Act, the FTC's Health Breach Notification Rule, the Health Insurance Portability and Accountability Act ("HIPAA"), and the Federal Food, Drug and Cosmetics Act. The FTC also issued its own Best Practices Guide for Mobile Health App Developers.

OCR Launches Phase 2 of HIPAA Audit Program
On March 21, the Department of Health and Human Services' Office for Civil Rights ("OCR"), the body responsible for enforcing HIPAA, announced that it would begin planning its second phase of audits of covered entities and their business associates. In this phase of audits, the OCR will review policies and procedures that are required by HIPAA to be adopted and followed with respect to HIPAA's Privacy, Security, and Breach Notification Rules.

Litigation, Judicial Rulings, and Agency Enforcements

Seventh Circuit Overturns Data Breach Dismissal
On April 14, the Seventh Circuit overturned a district court's dismissal of a case against a large national food chain on the grounds that plaintiffs did in fact have standing to bring claims. The case stemmed from a security breach involving restaurant patrons' credit card information. The court found that claims for future injuries, namely, "the increased risk of fraudulent charges and identity theft," constituted injuries for the purpose of Article III standing.

California District Court Consolidates Claims Against TV Manufacturer for Improper Data Sharing
On April 11, the U.S. District Court for the Central District of California consolidated cases brought against a smart-TV manufacturer for improperly sharing users' information. Plaintiffs alleged that the TV manufacturer collected data regarding "the date, time, channel of programs and whether users watch them live or recorded," and shared this information with third parties. This information allowed the third parties to engage in advertising targeted at the specific consumer.

Court Prohibits Defendant from Accessing Private Computer Systems
On April 8, in a claim that arose out of the leakage of patients' private health information, a California district court prevented a national health care organization from accessing plaintiffs' computer systems as part of the discovery process. The health care organization sought this information to negate causation, intending to show that some plaintiffs' identities may have been compromised prior to the breach. However, the court disagreed and found "that the burden of providing access to each plaintiff's computer system greatly outweigh[ed] its likely benefit."

Payment Processor Files Motion to Dismiss Proposed Class Action
On April 8, a payment processor filed a motion to dismiss a class action resulting from a security breach of consumers' email addresses and bank account information in the Northern District of California. The defendants compared the breached bank account information to written checks, arguing that "checks containing names, email addresses, and account information are exchanged in the open amongst people and businesses all the time." They claimed that the court would set an "unparalleled precedent" in permitting the plaintiffs' claims to proceed.

Class Actions Filed Against Cancer Center for Data Breach
In early April, following a security breach of patients' medical records, several class action suits were filed against a large cancer treatment center, alleging financial harm and other

injuries.

FTC Settles with Oracle Regarding Java Security
On March 29, the FTC approved a final consent order with a cloud applications provider related to allegations that the company misrepresented the safety and security of installing a new version of Java software, which left an insecure version of the software intact. Under the terms of the order, Oracle must notify consumers of the risk and give them the option of uninstalling the outdated software, in addition to providing website and social media notification about the issue.

California State Court Approves $39M Settlement in Medical Center Data Breach
In March, a California state court approved a $39M settlement against a medical center in southern California. The case stemmed from a security breach of patients' personal health information, which was made publicly accessible. The medical center notified the approximately 31,000 affected patients, who in turn filed consolidated class actions, alleging negligence and violations of the California Unfair Competition Law and the California Business and Professions Code, among other claims.

Legislative—Federal

House Unanimously Passes Email Privacy Reform Bill
On April 27, the House of Representatives voted 419–0 to pass a bill to amend the 1986 Electronic Communications Privacy Act with regard to emails and documents stored in the cloud. The Email Privacy Act would require the government to obtain probable cause warrants to access digital consumer records maintained by service providers, which are currently obtainable after 180 days via subpoena or court order.

Senate FAA Reauthorization Bill Mandates Cybersecurity Framework for Aviation
On April 19, the Senate passed a Federal Aviation Administration ("FAA") reauthorization bill that makes changes to a number of aviation policies, including a mandate to the FAA to develop a comprehensive cybersecurity framework for U.S. aviation. The bill also: (i) directs the FAA Administrator to develop a threat model and a plan to respond to cyber attacks; (ii) establishes a working group on aircraft systems information security to monitor the rulemaking and make recommendations; and (iii) suggests that cybersecurity for avionics systems be added as a new component of airworthiness certification.

Trade Secrets Bill Creates Private Civil Right of Action for Businesses
On April 4, the Senate passed the Defend Trade Secrets Act, establishing a new federal private right of action under which businesses can sue for trade secret theft in federal court and potentially seize property used to facilitate the theft in "extraordinary circumstances."

Legislative—States

Nebraska Amends Data Breach Notification Statute
On April 13, the Nebraska governor signed into law LB 835, which broadens the definition of "personal information" in the state's data breach notification statute, Neb. Rev. Stat. §§ 87-802 to 87-804, and adds a regulator notification requirement. The amendments take effect on July 20.

Tennessee Amends Data Breach Notification Statute
On March 24, the Tennessee governor signed S.B. 2005, which requires businesses and government agencies in Tennessee to notify state citizens affected by data breaches within 45 days of discovering a breach. The bill also expands state breach notification requirements to cover breaches of personal information regardless of whether the information was encrypted. The bill goes into effect on July 1.

Oregon Enacts Model Digital Assets Law

On March 3, 2016, Oregon enacted legislation providing personal representatives of deceased individuals access to the email and social media accounts of the deceased person. The bill was based on the Uniform Fiduciary Access to Digital Assets Act and will be effective on January 1, 2017.

Executive Branch—States

New Jersey Governor Establishes Cybersecurity and Communications Integration Cell
On May 20, the New Jersey governor signed Executive Order 178 establishing the New Jersey Cybersecurity and Communications Integration Cell ("NJCCIC") within the Office of Homeland Security and Preparedness, seeking to bridge the information and intelligence divide between New Jersey's public and private sectors. The NJCCIC's efforts, which will involve the New Jersey Attorney General's office and the Office of Information Technology and the State Police, will facilitate information sharing related to cybersecurity risks and provide guidance for both public and private entities.

New York AG Announces 40 Percent Increase in Data Breach Notifications and Unveils New Electronic Submission Form
On May 4, the New York attorney general announced that his office received a more than 40 percent increase in data breach notifications over the previous year. The attorney general also unveiled a new electronic submission form to allow companies to file notice via a web submission. This new reporting is designed to expedite and streamline the reporting process, leading to faster notification and resolution for New York consumers.

[Return to Top]

Canada

Canadian Prime Minister Announces Canada Will Co-Lead Initiatives to Increase Nuclear Facilities' Cybersecurity
On April 1, Prime Minister Justin Trudeau announced that Canada will jointly lead two Nuclear Security Summit ("NSS") "gift baskets." Gift baskets are mechanisms by which NSS participants take action in specific areas. One of these gift baskets, co-led with the United Kingdom, will focus on increasing cybersecurity of industrial control and plant systems at nuclear facilities.

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

[Return to Top]

Latin America

Argentina

Argentina's Data Protection Authority Investigates Uber
On April 22, a Buenos Aires judge ordered the preventive blockage of Uber's webpage (source document in Spanish), digital platforms, and applications offered by the company. Likewise, Argentina's data protection agency (*Dirección Nacional de Protección de Datos Personales*), in order to verify its compliance with the data protection regulation, requested that Uber disclose the data that it collects, the protection and confidentiality measures in place, and the data's destination.

Brazil

Final Report of Cyber Crimes Congressional Hearing Issued
On March 31, a Congressional Hearing (*Comissão Parlamentar de Inquérito*) investigating cyber crimes drafted its Final Report (source document in Portuguese). The report proposed several amendments to the Brazilian Civil Rights Framework for the Internet and Brazilian Cyber Crimes Statute (source documents in Portuguese). These amendments would, among other things, increase liability for internet service providers broadcasting offensive materials, grant IP address permissions to law enforcement personnel, broaden criminal liability for those who unlawfully access computers, and grant cyber crime investigative jurisdiction to the Brazilian Federal Police.

Chile

Court of Santiago Issues Ruling Regarding CCTV
On March 4, the Court of Appeals of Santiago issued a ruling (source document in Spanish) ordering the removal of surveillance aerostatic balloons with a closed-circuit television ("CCTV") system installed by the municipalities of Las Condes and Lo Barnechea after determining that their use violated the privacy right of local citizens. The aerostatic balloons were equipped with high-resolution cameras floating over these communities, even recording inside homes that were under the capture range of the devices.

Mexico

Mexican Voters Registration List Leaks through Online Retailer
On April 22, Mexico's National Electoral Institute ("INE") issued a press release (source document in Spanish) stating that voter registration lists were uploaded to an online retailer's data storage site and subsequently made public. Information on the lists included the names and addresses of approximately 90 million Mexican citizens enrolled in the voter registry. INE filed a criminal complaint with the Special Prosecutor's Office for Electoral Crimes against the person responsible, although there is currently no indication that security systems were breached.

New Mexican General Data Protection Law Moves Forward in Senate
On April 21, the United Commissions of Government and Legislative Studies of the Mexican Senate approved the General Data Protection Law Held by Regulated Subjects (source document in Spanish). The law will regulate the processing of personal data by all agencies of the executive, legislative, and judicial branches of the government that previously did not have a regulatory framework on the processing of personal data. The right to the protection of personal data will be limited only for reasons of national security, public order provisions, public health and safety, or to protect third-party rights.

Mexican Supreme Court Limits Access to Mobile Data
On April 13, Mexico's National Supreme Court declared the constitutionality (source document in Spanish) of article 190 of the Telecommunications and Broadcasting Federal Law, which orders telecommunications service companies to cooperate with authorities in locating mobile communication equipment and to allow authorities to access communication records. Although the law was ruled constitutional, the Supreme Court stated that authorization of a federal court is required for telecommunications companies to deliver the information requested by the authorities.

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

[Return to Top]

Europe

European Union

Commission and European Parliament Announce Final Adoption of General Data Protection Regulation
On April 14, the Commission announced the EU Parliament's adoption of the final text of the new General Data Protection Regulation. Together with the Council's vote on April 8, this concluded the legislative procedure and formalized the political agreement reached on December 15, 2015. The Regulation is expected to be published in the Official Journal in June 2016.

Commission Seeks Stakeholders' Input on ePrivacy Directive
On April 11, the Commission launched a public consultation on the ePrivacy Directive (Directive 2002/58) to align it with the General Data Protection Regulation and ensure the security of digital services, confidentiality and privacy of sensitive data, and consistent regulatory enforcement. The consultation will remain open until July 5.

European Data Protection Supervisor Publishes Guidance Relating to Personal Data Processing Security
On March 21, the European Data Protection Supervisor ("EDPS") released guidance on information security risk management, which issues recommendations on how European institutions can enforce and enhance a secure digital environment. The guidance accounts for the General Data Protection Regulation recently approved by the EU and includes a multidisciplinary assessment that covers several functions within an organization, such as Data Protection Officer and Information Technology.

Article 29 Working Party

Article 29 WP Issues Opinion on EU-U.S. Privacy Shield Draft Adequacy Decision
On April 13, the Article 29 Working Party ("WP") adopted an opinion on the new EU-U.S. Privacy Shield framework for transatlantic exchanges of personal data for commercial purposes. As summarized in its press release, the Article 29 WP welcomes the improvements over the invalidated Safe Harbor framework but expresses concerns over the commercial aspects and access by public authorities.

Article 29 WP Publishes Working Document on Justified Surveillance Measures When Transferring Personal Data
On April 13, the Article 29 WP issued a Working Document assessing how the invalidation of the Safe Harbor framework affected data transfers to the United States. Specifically, the document analyzes the Court of Justice case law related to Articles 7, 8, and 47 of the Charter of Fundamental Rights and the jurisprudence of the European Court of Human Rights related to Article 8 of the European Convention on Human Rights.

Article 29 WP Issues Statement on 2016 Action Plan for Implementation
On February 2, the Article 29 WP released a statement on the guidelines, tools, and procedures to implement the General Data Protection Regulation by the first quarter of 2018. The action plan is structured around four pillars: administration structure, consistency mechanisms, guidance for processors and controllers, and strengthened communication.

European Network and Information Security Agency

ENISA Publishes Report on Common Practices of EU-Level Crisis Management and Applicability to Cyber Crises
On April 4, the European Network and Information Security Agency ("ENISA") issued a report providing a series of key recommendations regarding EU-level priorities to alter the outcome of the next cyber crisis. The report discusses legal framework strategies, training coordination, and information sharing.

ENISA Releases Report Relating to Big Data Security
On March 8, ENISA published a study that identifies the key security challenges facing

companies implementing big data solutions, from infrastructures to analytics applications, and how those challenges may be mitigated.

France

CNIL 2015 Report Shows Record Number of Complaints
On April 8, the *Commission Nationale de l'Informatique et des Libertés* ("CNIL") issued its annual report for 2015 (source document in French). CNIL recorded 7,908 complaints relating to the protection of e-reputation and 5,980 requests for indirect access to the judicial registers following the issuance of search warrants, security measures, and permit withdrawals. CNIL also carried out 501 online controls, issued 93 formal notices, and levied 10 sanctions, including three pecuniary sanctions.

CNIL Audits Wireless Network Devices
In April, CNIL announced (source document in French) that, together with the Article 29 WP, it will carry out an online audit in May to assess the impact of wireless network devices on users' private lives. The audit will target home automation devices and health-related devices, assessing the quality of information delivered, the security levels implemented, and data subject control over personal data. The audit results will be published this fall.

CNIL Launches Compliance Package for Connected Vehicles
On March 23, CNIL launched (source document in French) the process to define the sixth compliance package relating to connected vehicles. This process will involve automotive operators, insurance and telecoms innovative companies, and public authorities. The compliance package is aimed at establishing guidelines to ensure personal data protection and encourage innovation in the automotive sector.

CNIL Imposes €100,000 Fine on Internet Search Engine for Failure to Comply with Right To Be Forgotten
On March 10, CNIL summoned an internet search engine to comply with the requests to delist internet links from the web search results within a certain frame. The internet search engine proposed to delist within a specific geography and to implement a region filter, but CNIL still levied a €100,000 fine because the company failed to comply within the required time frame. According to CNIL's opinion, the right to privacy is a universal right requiring full delisting regardless of the user's geographic region.

ANSSI Issues New Security Guidelines for Integration and Maintenance Providers of Industrial Systems
On March 9, the working group on the cybersecurity of the industrial systems ("CT CSI"), led by the French National Agency for Information Systems Security ("ANSSI"), identified integration and maintenance providers as key cybersecurity actors because of their constant role in the system's life cycle. The working group issued new guidelines (source document in French) relating to the security requirements to be taken by both the providers and the beneficiaries.

Germany

Conference of German Data Protection Authorities Views Privacy Shield as Insufficient
On April 20, the Conference of the Independent German Federal and State Data Protection Authorities (*Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*) ("Conference") issued a resolution (source document in German) holding the current version of the EU-U.S. Privacy Shield as insufficient to ensure adequate protection for data transfers to the United States. In the resolution, the Conference also requested the legislature provide for an independent right of action enabling data protection authorities to challenge adequacy decisions of the EU Commission before national courts.

German Federal Constitutional Court Declares Federal Criminal Police Office Act Partly Unconstitutional
On April 20, the German Federal Constitutional ruled (source document in German) that the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz*) is partly unconstitutional as a disproportionate intervention into private life. The court criticized the provisions on secret surveillance measures, such as the surveillance of telecommunication and online searches and the rules for disclosing data to foreign security authorities and domestic intelligence services.

Italy

Italian DPA Adopts a *Vademecum* for Setting Guidelines for Credit Collection
On April 18, the Italian Data Protection Authority published the *vademecum* for credit collection (source document in Italian), summarizing general principles to be applied when creditors carry out activities aimed at collecting amounts due from debtors. The handbook does not introduce material changes to the existing regime but pinpoints the rights of debtors in the case of direct contacts from credit collectors.

Spain

SDPA Publishes Identity Theft Guidelines
On March 14, the Spanish Data Protection Agency ("SDPA") and the Council of Consumers and Users released basic guidelines (source document in Spanish) on protecting against identity theft in telecommunications services. Through these guidelines, citizens can learn about their legal rights relating to privacy and data protection in Spain.

Spanish Constitutional Court Allows Employers to Record Employees Without Disclosure
On March 3, the Spanish Constitutional Court issued a decision (source document in Italian) allowing employers to use video surveillance systems to record their employees without prior disclosure. In this case, the video surveillance system was introduced after a suspected employee was taking money from the cash register.

The Netherlands

DDPA Finds Web Forms Need More Secure Connections
On March 15, the Dutch Data Protection Agency ("DDPA") wrote a letter to the Royal Dutch Society for Physiotherapy (source document in Dutch) regarding earlier questions concerning the security of patient contact forms. The DDPA responded that sensitive personal data submitted through web applications needs to be presented through a secure, https connection.

DDPA Approves Processing of Personal Data by BREIN Foundation on BitTorrent Users
On March 14, the DDPA published a decision (source document in Dutch) approving BREIN's intention to process the personal data of BitTorrent users. The BREIN foundation, a joint antipiracy program of authors and artists, seeks to track users who infringe on the copyright of BREIN's affiliated parties. The personal data to be processed includes IP addresses and user names, and the scope of the investigation is limited to productions of parties affiliated with the BREIN foundation and to Dutch users of the BitTorrent network.

DDPA Declares Processing of Personal Health Data of Employees Unlawful
On March 8, the DDPA issued a press release (source document in Dutch) on two companies that provided activity trackers to their employees to monitor their physical exercise. One of the employers also monitored the sleep patterns of its employees. Although the employees gave their consent to the monitoring, and participation was voluntary, the DDPA found that the data gathered was "sensitive personal data" regarding

personal health, which employers are not allowed to process.

United Kingdom

ICO States that Data Protection Rules Required Regardless of Brexit Vote
On April 19, the ICO issued a statement that the UK will continue to need clear and effective data protection laws, whether or not it remains in the EU. The statement emphasizes the increased need for effective practices in light of the growing digital economy.

ICO Brings Prosecution Against Former Employee for Attempt to Obtain Personal Data
On April 8, the ICO prosecuted a former employee for attempting to obtain personal data. The ICO has stressed that stealing personal information is a crime in the UK. The prosecution stemmed from a recent initiative for stricter penalties for data thieves.

ICO Issues Updated Guidance on Direct Marketing
On March 24, the ICO updated its guidance on online marketing. There is now a greater emphasis on the application of the marketing rules to the not-for-profit sector and direction regarding third-party consent.

ICO Publishes Guidance on the Use of Encryption
On March 3, the ICO issued guidance on the use of encryption to protect personal data. The guidance stressed key areas such as the use of USB memory sticks and the risk of sending personal data to the wrong recipient.

The following Jones Day attorneys contributed to this section: Paloma Bru, Laurent De Muyter, Olivier Haas, Jörg Hladjk, Bastiaan Kout, Jonathon Little, Guiseppe Mezzapesa, and Undine von Diemar.

[Return to Top]

Asia

People's Republic of China

Ministry of Commerce Publishes Draft Specifications for Mobile and Cross-Border Commodity e-Commence
On March 22, the Ministry of Commerce of the People's Republic of China published drafts of the Business Services Specification for Mobile Commodity E-commerce and Business Services Specification for Cross-border Commodity E-commerce (source documents in Chinese), which contain provisions that require e-commerce service providers to take measures to ensure the security of operational data and service platforms. Under the draft specifications, any collection and processing of personal or transaction information requires the authorization of the data subject or parties to the transaction, and such information may not be directly used for commercial purposes unless it has been desensitized.

Hong Kong

PCPD Sanctions Insurance Agent for Using Personal Data without Consent
On April 25, the Privacy Commissioner for Personal Data ("PCPD") released a media statement revealing that an insurance agent was convicted of two offenses under the Personal Data (Privacy) Ordinance for using personal data in direct marketing without taking specified actions and obtaining the data subject's consent, and for failing to inform the data subject of his opt-out right when using his personal data in direct marketing. A Community Service Order of 80 hours was imposed by the court on the convicted insurance agent.

PCPD Joins Global Sweep Exercise
On April 15, PCPD announced that it had joined the Global Privacy Enforcement Network to conduct a privacy sweep from April 11, examining data privacy issues relating to Internet of Things devices such as smart electricity meters and internet-connected thermostats. PCPD had chosen to examine fitness bands produced in Hong Kong for the sweep exercise as well. The results of the sweep will be published in the third quarter of 2016.

Japan

Diet Passes Amending Bill to Set New Rules to Utilize Personal Information Held by Administrative Organs
On March 8, the Cabinet submitted a bill (source document in Japanese) to the Diet to amend the law protecting personal information held by administrative institutions. These amendments mirror recent amendments affecting personal information held by the private sector under the Personal Information Protection Act and set new rules for private entities to utilize personal information held by administrative institutions through an anonymization process. The bill passed the Diet on May 20 and will take effect before September 2017.

Singapore

PDPC Issues Enforcement Guidelines
On April 21, the Personal Data Protection Commission ("PDPC") issued Advisory Guidelines on Enforcement for Data Protection Provisions. These guidelines outline the agency's enforcement procedures as they relate to alternative dispute resolutions, investigations, appellate rights, and rights of private action.

PDPC Releases List of Enforcement Actions
On April 21, PDPC released a list of enforcement actions brought by the agency over the past year. The list details the facts and circumstances surrounding 10 data breach-related actions in which organizations were breached or disclosed consumer data without consent. The list also discusses the penalties levied against these organizations.

Taiwan

The Executive Yuan Announces Effective Date of Amendments to Personal Information Protection Act
On February 25, the Executive Yuan announced (source document in Chinese) that the December 30, 2015 amendments to the Personal Information Protection Act will take effect on March 15. After the amendments take effect, personal data collection no longer requires consent unless the information relates to sensitive data, such as medical records, medical treatment, genetic information, health examinations, and criminal records.

The following Jones Day attorneys contributed to this section: Chiang Ling Li, Michiru Takahashi, and Richard Zeng.

[Return to Top]

Australia

Australian Privacy Awareness Week Held
Beginning May 15, the Office of the Australian Information Commissioner held its Privacy Awareness Week. The week's events were highlighted by a visit from the United Nations Special Rapporteur on the Right to Privacy, who hosted a Business Breakfast in Sydney and a public lecture on privacy in Canberra.

Australian Prime Minister Announces Cyber Security Strategy

On April 21, the Prime Minister of Australia announced the Australian Cyber Security Strategy for the next four years. Under the Strategy, the federal government proposes to spend A$230M for initiatives to: (i) strengthen defenses to cybersecurity threats, including increasing the capacity of Australia's Computer Emergency Response Team and the Australian Cyber Security Center; (ii) appoint a Cyber Ambassador to represent Australia in international cyber issues; (iii) establish a Cyber Security Growth Center for cybersecurity research and development; and (iv) establish a fund for cybersecurity education.

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

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

Chiang Ling Li
Hong Kong

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

John A. Vogt
Irvine

Undine von Diemar
Munich

Toru Yamada
Tokyo

Sidney R. Brown
Atlanta

Paloma Bru
Madrid

Jörg Hladjk
Brussels

Jay Johnson
Dallas

Guillermo E. Larrea
Mexico City

Christopher J. Lopata
New York

Margaret I. Lyle
Dallas

Giuseppe Mezzapesa
Milan

Sergei Volfson
Moscow

Olivier Haas
Paris

Peter Brabant
Sydney

Po-Chien Chen
Taipei

Nigel Chin
Singapore

Jeremy S. Close
Irvine

Daniel C. D'Agostini
São Paulo

Laurent De Muyter
Brussels

Adrian Garcia
Dallas

Steven G. Gersten
Dallas

Bart Green
Irvine

Joshua Grossman
New York

Aaron M. Healey
Columbus

Bastiaan K. Kout
Amsterdam

Colin Leary
San Francisco

Tyson M. Lies
Dallas

Alexandra A. McDonald
San Francisco

Kelly M. Ozurovich
Los Angeles

Mónica Peña Islas
Mexico City

Nicole M. Perry
Houston

Scott B. Poteet
Dallas

Brandy H. Ranjan
Columbus

Jessica M. Sawyer
Los Angeles

Alexa L. Sendukas
Houston

Elie J. Sherique
São Paulo

John T. Sullivan
Dallas

Raquel Travesí
Madrid

Anand Varadarajan
Dallas

Nicola Walker
Sydney

Natalie Williams
Atlanta

Richard Zeng
Hong Kong

Follow us on:

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