Global Privacy & Cybersecurity Update
Issue 14 | May 2017

JONES DAY

GLOBAL PRIVACY & CYBERSECURITY UPDATE

Jones Day Cybersecurity, Privacy & Data Protection Attorney Spotlight: Samir Jain

Sophisticated and evolving cyberattacks, sometimes sponsored by state actors, are a significant risk that enterprises in virtually all industries now face. The legal and policy landscape in which they must manage this risk is evolving rapidly, as courts, regulators, and legislators both in the United States and abroad seek to balance security and public safety, privacy, economic consequences, and other key values.

Samir Jain, a Washington-based partner in Jones Day's Cybersecurity, Privacy & Data Protection Practice, leverages his considerable government and private practice experience to advise companies—including those in critical infrastructure sectors such as communications, energy, and health care—on managing cybersecurity risk, developing cyber incident response plans, and responding to security incidents. He counsels companies on interactions with law enforcement and regulators, defends against government investigations, and advises on the promulgation of regulation and policy. He also focuses on emerging technologies and marketplace trends, including the deployment of Internet of Things products, self-driving cars, and artificial intelligence.

Prior to joining Jones Day, Samir was Senior Director for Cybersecurity Policy for the National Security Council at the White House, where he led the team responsible for cyber incident response and oversight of cyber operations, directed the evaluation of legislative proposals such as reform of the Electronic Communications Privacy Act, and worked closely with international cyber counterparts.

He also previously served as Associate Deputy Attorney

EDITORIAL CONTACTS

Daniel J. McLoon
Los Angeles

Mauricio F. Paez
New York

Jonathon Little
London

Kevin D. Lyles
Columbus

Todd S. McClelland
Atlanta

Jeff Rabkin
San Francisco

Adam Salter
Sydney

Michiru Takahashi
Tokyo

Undine von Diemar
Munich

Paloma Bru
Madrid

Olivier Haas
Paris

Jörg Hladjk
Brussels

Jay Johnson
Dallas

Editor-in-Chief: Anand Varadarajan

Practice Directory

HOT TOPICS IN THIS ISSUE

U.S. Congress Votes to Repeal FCC Broadband Privacy Rules

Mexican INAI Issues Strategic Actions to Implement General Data Protection Law

European Data Protection Supervisor Seeks Stronger Consumer Protections in Digital Content

General in the Department of Justice, where he helped develop proposals to modernize cybercrime laws and represented DOJ in White House cybersecurity policy meetings and international negotiations.

Before his government service, Samir was in private practice for nearly 20 years, during which he represented clients in litigation and regulatory proceedings involving privacy and data security, national security, communications, and internet law issues.

United States

Regulatory—Policy, Best Practices, and Standards

New York Attorney General Announces Record Number of Data Breach Notices in 2016
On March 21, 2017, the New York Attorney General's Office announced that it received 1,300 reported data breaches in 2016—a 60 percent increase from the number received in 2015. The reported breaches exposed personal records of 1.6 million New York residents.

Office of U.S. Trade Representative Reports on Data Residency Laws
On March 31, the Office of U.S. Trade Representative released its annual report analyzing how barriers to trade have played out in dozens of foreign countries. The report highlights two trends: (i) an increasing emergence of data residency laws requiring private-sector companies to store information locally; and (ii) new laws that require government data to be stored locally, such as in China, Indonesia, Canada, and Nigeria.

SEC Reaffirms Commitment to Pursuing Actions over Cyber Reporting
On April 20, in response to a Jones Day moderator at the 2017 IAPP Global Privacy Summit, the Securities and Exchange Commission's ("SEC") Acting Enforcement Director commented on the absence of SEC actions against public companies for failing to report cyber incidents and risks. She noted that the absence should not be mistaken for the agency's unwillingness to bring such actions, but she added that "we [SEC] are not looking to second-guess good-faith disclosure decisions."

Massachusetts Attorney General Educates Law Enforcement on Cyber Crime
On April 26, the Massachusetts Attorney General hosted the sixth annual National Cyber Crime Conference. More than 650 law enforcement officers, prosecutors, and investigators from across the United States and Canada attended the three-day conference. The goal of the conference was to help equip law enforcement officials and prosecutors with the tools and skills to effectively detect and defeat cyber crime.

Regulatory—Critical Infrastructure

Contracts

China Passes Civil Law Relating to Personal Data Protection

Australian Law Requires Telecommunications Service Providers to Retain Metadata

RECENT AND PENDING SPEAKING ENGAGEMENTS

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

2017 Compliance Outreach Program for Broker-Dealers, U.S. Securities & Exchange Commission and Financial Industry Regulatory Authority, Dallas, Texas (July 27). **Jones Day Speaker: Jay Johnson**

Network & System Architecture as a Defense, CISO Executive Network, Houston, Texas (June 22). **Jones Day Speaker: Nicole Perry**

Fully Connected, Fully Liable? Cybersecurity: Risks and Pitfalls—Be Prepared (and Watch Your Smartphones—Live Hacking Demonstration!), Jones Day Client Conference 2017, Frankfurt, Germany (June 12). **Jones Day Speaker: Undine von Diemar**

Cybersecurity—Handling a Crisis, Symposium on International Law and Global Markets, Institute for Law and Technology, Plano, Texas (June 12). **Jones Day Speaker: Jay Johnson**

Network & System Architecture as a Defense, CISO Executive Network, Atlanta, Georgia (June 7). **Jones Day Speaker: Todd McClelland**

Cyber Security Primer, Plano Bar Association, Plano, Texas (June 2). **Jones Day Speaker: Jay Johnson**

GDPR: What is Going to Change About Data Protection Across the EU, Jones Day Webinar (June 1). **Jones Day Speaker: Giuseppe Mezzapesa**

IAPP Global Update and HR Data Processing Under the GDPR, How Companies Need to Prepare, Munich,

NIST Publishes Report on Robot Cybersecurity Performance Analysis

On April 18, the National Institute of Standards and Technology ("NIST") issued a report titled "Metrics and Key Performance Indicators for Robotic Cybersecurity Performance Analysis." The report follows NIST's construction of a "testbed to measure the performance impact induced by cybersecurity technologies on Industrial Control Systems." The research delves into various manufacturing-related operational methodologies and the effectiveness of defensive measures.

NIST Issues Cyber-Threat Intelligence and Information-Sharing Bulletin

On May 8, NIST published a bulletin titled "Cyber-Threat Intelligence and Information Sharing to discuss the basics of cyber-threat information sharing and building relationships in an information-sharing community. The bulletin discusses security alerts, intelligence reports, and tool configurations, as well as strategies to build and participate in information-sharing networks.

Regulatory—Retail

FTC Penalizes Membership Reward Service for Violating Order

On March 17, the Federal Trade Commission ("FTC") announced a civil penalty against a membership reward service, Upromise, for failing to disclose the extent of its data collection practices. Despite a 2012 order requiring the company to make clear and prominent disclosures, the FTC alleged that the company failed to make appropriate disclosures or to obtain the necessary assessments certifying protection of consumer data. As part of the new order, the company must pay $500,000 and implement the remedial measures prescribed in the 2012 order.

FTC Resolves Allegations that Companies Misrepresented Participation in International Privacy Program

On April 14, the FTC approved final orders with three companies regarding allegations that they deceived consumers by misrepresenting their participation in the Asia-Pacific Cooperation Cross-Border Privacy Rules system. The settlements with a provider of endpoint protection software, a marketer of a private message app, and a distributor of cybersecurity software prohibit the companies from misrepresenting their participation, membership, or certification in any privacy or security program sponsored by a government or self-regulatory or standard-setting organization.

FTC Seeks Comment on Children's Privacy Compliance Oversight Program Proposal

On April 19, the FTC sought comment regarding a private compliance and data security company's proposed change to its self-regulatory guidelines regarding children's privacy. The proposed change adds a requirement that companies in the program annually assess whether third parties collect personal information from children.

Germany (May 31). **Jones Day Speaker: Undine von Diemar**

Network & System Architecture as a Defense, CISO Executive Network, Washington, D.C. (May 25). **Jones Day Speaker: Jennifer C. Everett**

Connected Cars: Privacy & Security Issues, Dallas Bar Association's Science & Technology Section, Dallas, Texas (May 22). **Jones Day Speaker: Jay Johnson**

Jones Day's Second Annual Latin American Privacy & Cybersecurity Symposium in Mexico City (May 17–18). **Jones Day Speakers: Mauricio Paez, Todd McClelland, Richard Martinez, Paloma Bru, Sergio Alvarez-Mena,** and **Guillermo Larrea**

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

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

New Trends on Cyber Security, Conference in the American Chamber of Commerce of Madrid , Madrid, Spain (May 10). **Jones Day Speaker: Paloma Bru**

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

GDPR Workshop: Best Practices for Implementing the EU General Data Protection Regulation, Jones Day Seminar, New York, New York (April 25). **Jones Day Speakers: Undine von Diemar, Mauricio Paez,** and **Jörg Hladjk**

GDPR Workshop: Best Practices for Implementing the EU General Data Protection Regulation, Jones Day Seminar, Washington, D.C. (April 24). **Jones Day Speakers: Undine von Diemar, Jörg Hladjk,** and

FTC Settles Deceptive Online and Mobile Consumer Tracking Practices with Digital Advertiser
In April, the FTC approved a final consent decree with digital advertising technology company Turn. The FTC charged Turn with misrepresenting the extent to which it continued to track consumers, even after the consumers opted out of such tracking through web browser settings, as advised by Turn's privacy policy. The FTC alleged that Turn used unique device identifiers to track tens of millions of mobile phone customers who had blocked or deleted cookies. As part of the order, Turn must provide an effective opt-out mechanism for consumers who do not want their information used for targeted advertising.

Regulatory—Defense and National Security

DOD Announces Cyber Bug Bounty Program
On March 2, the Department of Defense ("DOD") announced that it would invite hackers to test the department's cybersecurity. The pilot program is the first in a series planned to find vulnerabilities in the department's applications, websites, and networks. The pilot was announced as part of an effort to comply with the Administration's Cyber National Action Plan.

Regulatory—Transportation

Office of Unmanned Aircraft Systems Director Testifies on FAA Rules Regarding Privacy
On March 15, the director of the Federal Aviation Administration ("FAA") Office of Unmanned Aircraft Systemstestified before the Senate Committee on Commerce, Science, and Transportation that the FAA has no rules in place regarding what data commercial drones can collect, whether companies can sell such data, and how long companies can retain the information they gather. The director also noted that the FAA is working with the Drone Advisory Committee, which includes several members from the drone industry, to draft regulations.

Regulatory—Financial Services

SEC Proposes Inline XBRL Filing of Tagged Data
On March 1, the SEC proposed amendments to improve the quality and accessibility of data submitted by public companies and mutual funds using eXtensible Business Reporting Language ("XBRL"). The acting chairman noted that "while XBRL technology has made disclosures easier to access for investors, there are legitimate concerns about the burdens smaller companies face when preparing their filings," and the Commission is seeking "a way to streamline this process to ensure usability for the public while keeping compliance costs down."

SWIFT Messaging System to Start Suspicious Payment Alerts to Defend Banks
On April 12, the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") announced measures to defend banks against cyberattacks that target banks' connections to the SWIFT messaging system. Among

Jennifer Everett

Q&A with the SEC on Agency Expectations for Consumer Privacy and Cybersecurity, IAPP Global Privacy Summit, Washington, D.C. (April 20). **Jones Day Speaker: Jay Johnson**

Identity—The Human Factor, CISO Executive Network, Atlanta, Georgia (April 12). **Jones Day Speakers: Frances Forte** and **Mary Alexander Myers**

The Digital Criminal: Cyber Crime Trends and Enforcement with the U.S. Attorney's Cybercrime Unit, Jones Day, and Booz Allen Hamilton, Boston, Massachusetts (April 10). **Jones Day Speaker: Lisa Ropple**

Identity: The Human Factor, CISO Executive Network, Houston, Texas (April 20). **Jones Day Speaker: Nicole Perry**

Data Breaches: Working with Federal Authorities, Third Annual Health Care Cyber Security Symposium, North Texas Crime Commission, Fort Worth, Texas (March 31). **Jones Day Speaker: Jay Johnson**

Legal Issues Specific to Health Care Cyber Security, Third Annual Health Care Cyber Security Symposium, North Texas Crime Commission, Fort Worth, Texas (March 31). **Jones Day Speaker: Anand Varadarajan**

General Data Protection Regulation: The New Tools of the CNPD (Luxembourg Data Protection Authority), Conference of General Counsels in Luxembourg, Banque & Caisse d'Epargne de l'Etat, Luxembourg (March 29). **Jones Day Speaker: Laurent De Muyter**

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

LexisNexis Webinar: UK Cybersecurity Update (March 21). **Jones Day Speakers: Elizabeth Robertson** and **Harriet Territt**

Introduction to the GDPR—Top 10 Implementation Issues for Companies, Jones Day Webinar

other measures, the tools include a payment screening service allowing small member banks to automate the flagging of suspicious payments. SWIFT is an interbank messaging system that hackers used to steal $81 million from Bangladesh last year.

Regulatory—Health Care/HIPAA

HHS Settles with Wireless Health Services Provider Following Theft of Unsecured Laptops
On April 24, the U.S. Department of Health and Human Services ("HHS") publicized a $2.5 million settlement with a wireless health services provider, CardioNet, relating to the disclosure of unsecured patient health information stored on two stolen laptops. Because the investigation revealed that CardioNet "had an insufficient risk analysis and risk management processes in place at the time of the theft," the provider was also ordered to implement a corrective action plan. For more information, see the related Jones Day *Commentary*.

HHS Settles with Hospital Provider for HIPAA Privacy Violations
On May 10, HHS announced a settlement with a hospital system for inadvertently disclosing protected health information ("PHI") in a hospital press release, which reported on a data security incident affecting patient data. Under the settlement, the hospital system must pay $2.4 million and "update its policies and procedures on safeguarding PHI from impermissible uses and disclosures and to train its workforce members."

Litigation, Judicial Rulings, and Agency Enforcement Actions

Illinois Federal Judge Approves $76 Million Settlement in Cruise Robocall Class Action
On March 2, an Illinois federal district court granted final approval of a $76 million settlement resolving a class action accusing several cruise marketing companies of robocalling millions of Americans. The plaintiffs alleged that the cruise marketing companies operated a telemarketing scheme advertising free cruises but actually intending to sell timeshares. The calls went out to at least 900,000 numbers contained in a class list put together from company records. The settlement provides a minimum payout of $135 per call, with most class members receiving more than $400 each.

Clothing Retailer Settles Data Breach Class Action for $1.6 Million
On March 17, a prominent clothing retailer settled a credit card data breach class action affecting approximately 350,000 customers. Although the action was initially dismissed for lack of standing, the Seventh Circuit Court of Appeals found that preventative measures like credit monitoring were sufficient to show standing. As part of the settlement, the company will pay $1.6 million and institute a host of remedial security measures.

New York Attorney General Announces Settlements with Three Health and Fitness App Providers

(March 15). **Jones Day Speakers: Various**

The Endpoint: How to Protect Vulnerable IoT Devices from Data Attacks, CISO Executive Network, Houston, Texas (March 9). **Jones Day Speaker: Nicole Perry**

The Endpoint: How to Protect Vulnerable IoT Devices from Data Attacks, CISO Executive Network, Dallas, Texas (March 9). **Jones Day Speaker: Jay Johnson**

Governance, Risk Management & Compliance, The First Boston Conference on Cyber Security, Boston, Massachusetts (March 8). **Jones Day Speaker: Lisa Ropple**

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

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

RECENT AND PENDING PUBLICATIONS

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

"WannaCry": The Global Ransomware Attack (May). **Jones Day Authors: Rick Martinez, Mauricio Paez, Lisa Ropple, Jay Johnson**

Personal Data Held by Government Agencies Now Heavily Protected in Mexico (May). **Jones Day Authors: Mauricio Paez, Guillermo Larrea, Mónica Peña Islas**

China's New Cybersecurity Law and Draft Data Localization Measures Expected to Burden Multinational Companies (May). **Jones Day Authors: Chiang Ling Li, Haifeng Huang, Todd McClelland, Mauricio Paez, Jennifer Everett**

$2.5 Million Settlement Reached as HIPAA Crackdown Continues on Unsecured Portable Devices (May).

On March 23, three mobile health app developers agreed to pay $30,000 and revise their advertising and privacy policies to resolve the New York Attorney General's claims that they falsely touted the ability of their apps to measure key vital signs and were unclear about what data the apps collected. The settlement concluded a yearlong investigation by the New York Attorney General into deceptive statements and "irresponsible privacy practices" linked to the developers' health-related apps that promise to accurately measure heart rates and detect fetal heartbeats.

Florida Federal Judge Approves $31 Million FACTA Class Action Settlement

On March 23, a Florida federal judge signed a $31 million class action settlement involving a major fast food chain. The figure comprises the largest settlement in the history of the Fair and Accurate Credit Transactions Act ("FACTA"). The plaintiffs alleged that the food chain violated FACTA through its practice of printing the full expiration dates of customers' credit cards on receipts.

Massachusetts Attorney General Settles with Advertising Company in Geofencing Case

On April 4, the Massachusetts Attorney General entered a settlement prohibiting an advertising company from engaging in certain geofencing practices. Specifically, the "digital advertising company [] was hired to use mobile geofencing technology to target women entering reproductive health facilities." The settlement forbids the advertising company from using geofencing technology near hospital facilities to collect or compile the medical information of any individual.

Jones Day Authors: Alexis Gilroy, Todd Kennard, Kevin Lyles, David Kopans

Japan Legal Update | Vol. 24 (April). **Jones Day Authors: Various**

Data Breach Risks for 401(k) and Retirement Plans (April). **Jones Day Authors: John Vogt, Richard DeNatale, Travis DeHaven, Todd McClelland**

Japan Legal Update Vol. 23 (March). **Jones Day Authors: Various**

What Does the Introduction of Mandatory Data Breach Notification in Australia Mean for You? (March). **Jones Day Authors: Adam Salter, Mauricio Paez, Undine von Diemar, Nicola Walker**

New Mexico On the Brink of Passing Data Breach Notification Law (March). **Jones Day Authors: Mauricio Paez, Lisa Ropple, Jay Johnson, Kerianne Tobitsch**

California Releases Further (Proposed) Regulations Governing Testing and Deployment of Autonomous Vehicles (March). **Jones Day Authors: Paul Rafferty, Jeffrey Jones, Robert Kantner, Todd Kennard**

California Federal Judge Approves $60.5 Million Judgment in Favor of Advertising Company

On April 13, a California federal judge approved an unopposed $60.5 million judgment in favor of a large advertising company against an online real estate rental service in a copyright and computer fraud suit. The advertising company alleged that the real estate rental service unlawfully collected its user data by scraping contact information via a third party. In addition to the monetary penalty, the judgment included an injunction preventing the real estate rental service and any of its officers from reproducing or distributing the advertising company's content themselves or through a scraper, robot, or spider.

Florida Attorney General and FTC File Complaints for "Tech Support" Scams

On May 1, the Florida Attorney General and the FTC filed a complaint against three technical support software companies alleging violations of the Florida Deceptive and Unfair Trade Practices Act. These alleged scams involved pop-up ads disguised as virus alerts that instructed consumers to call a number for help. The companies then sold the consumers unnecessary and costly technical support services or software products.

Legislative—Federal

Congress Votes to Repeal FCC Broadband Privacy Rules

On March 28, the House of Representatives approved a joint resolution repealing the privacy rules for internet service providers ("ISPs") set by the Federal Communications Commission ("FCC") in October 2016. The resolution, which passed the Senate on March 23, was signed by the President on April 3. Among the privacy rules invalidated by this action is a rule that required ISPs to obtain opt-in consent before using or selling consumer data, including web browsing and app usage history. Under the Congressional Review Act, Congress can repeal agency rules through simple majority votes.

Small Business Cybersecurity Bill Proceeds to Senate Floor

On April 5, the Senate Commerce, Science, and Transportation Committee passed the bipartisan MAIN

STREET Cybersecurity Act, which aims to equip small businesses with resources to help them protect against and manage cybersecurity risks, including implementing the NIST's voluntary Cybersecurity Framework. According to a 2012 study by the National Cyber Security Alliance cited by the bill's co-sponsor, around 60 percent of small businesses that suffer a cybersecurity attack go out of business within six months. The legislation, which is backed by the U.S. Chamber of Commerce and National Small Business Association, now awaits full Senate consideration.

President Signs Cybersecurity Executive Order
On May 11, President Trump signed an executive order designed to enhance the cybersecurity capabilities of the federal government. Specifically, the order seeks to improve accountability within federal agencies, augment incident response capabilities, and develop a workforce more capable of tackling cybersecurity issues.

House Approves Revised Modernizing Government Technology Bill
On May 17, the House of Representatives passed the Modernizing Government Technology Act ("MGT Act") by voice vote. The legislation creates a centralized fund for agencies to modernize their technology and allows agencies to put money saved through IT efficiencies into working capital funds that can be accessed for up to three years. According to a May 12Congressional Budget Office estimate, implementing the MGT Act would cost $500 million over five years. A companion bill in the Senate that is identical to the current version awaits committee action.

Legislative—States

Virginia Updates Data Breach Notification Law for Payroll Data
On March 13, the Virginia Governor signed an amendment to Virginia's data breach notification law, adding a requirement that employers or payroll service providers give notice to the Attorney General's office if payroll information is compromised. Notification to the Virginia Attorney General is required if there is an "unauthorized access and acquisition of unencrypted and unredacted computerized data containing a taxpayer identification number in combination with the income tax withheld for that taxpayer" and "the employer or payroll provider reasonably believes [the access or acquisition] has caused, or will cause, identity theft or other fraud." The Virginia amendment was enacted in response to the recent surge of Form W-2 phishing scams and will go into effect on July 1.

Tennessee Clarifies Encryption Exception in Data Breach Notification Law
On April 4, the Tennessee governor signed an amendment to Tennessee's data breach notification law to clarify that companies do not need to notify Tennessee citizens of personal data breaches if the information compromised was encrypted, resolving confusion that was created by a 2016 amendment. The amendment went into effect immediately upon signature by the governor.

New Mexico Becomes 48th State to Enact Data Breach Notification Law
On April 6, New Mexico became the 48th state to enact a data breach notification law—leaving Alabama and South Dakota as the only states without such laws. H.B. 15 governs data breach notification requirements for entities storing and using personal identifying information about New Mexico residents and also establishes requirements for securing and disposing of that information. The bill requires notification to affected consumers in the event of a breach within 45 days of discovery of the breach and will go into effect on June 16. For more information, see the related Jones Day *Commentary*.

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

Latin America

Argentina

Argentina Issues Draft Data Protection Bill
In February, the Argentinean Data Protection Agency (*Dirección Nacional de Protección de Datos Personales*) posted the first draft of a new data protection bill (source document in Spanish) on its website. Argentina's current data protection bill was enacted in December 2000. The draft bill incorporates several changes proposed in a 2016 public consultation as well as the forthcoming EU General Data Protection Regulation.

Chile

Chilean Government Passes New Personal Data Bill

On March 10, the Chilean government enacted a new version (source document in Spanish) of the Law of Protection of Personal Data. The bill incorporates guiding principles issued by the Organization for Economic Cooperation and Development's guidelines, as well as the recognition of data holders' "ARCO rights" and rules regarding special protection for sensitive personal data. The legislation also creates the Personal Data Protection Agency to supervise and enforce data protection matters.

Mexico

INAI Issues Strategic Actions to Implement General Data Protection Law

On March 27, the National Institute for Transparency, Access to Information and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* or "INAI") issued a step-by-step plan (source document in Spanish) for the implementation of the new General Law for the Protection of Personal Data Held by Regulated Subjects (source document in Spanish). The five strategic lines of action suggested by INAI include: (i) evaluation of the local data protection regulatory framework and counseling state congresses on the subject; (ii) development, execution, and evaluation of the Personal Data Protection National Program; (iii) adjustment of existing laws and regulations issued by the National Transparency System; (iv) revisions to the new digital National Transparency Platform; and (v) personnel training on how to handle personal data.

INAI Issues Recommendations for Using Social Media

On April 10, INAI issued recommendations (source document in Spanish) to avoid risks when using personal data in social media. According to one study, by the third trimester of 2016, there were 64.9 million social media users in Mexico, the majority of whom are under 40 years old. Among other measures, INAI's tips for social media users include: (i) avoiding contact with unknown users; (ii) logging out when accessing accounts on a public computer; (iii) creating robust passwords with diverse characters; (iv) selecting adequate privacy and security configurations for social media accounts; and (v) refraining from business transactions on social media.

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

[Return to Top]

Europe

European Union

EDPS Calls for Improvements to EU Border policy

On March 6, the European Data Protection Supervisor ("EDPS") released an opinion on the European Travel Information and Authorization System ("ETIAS"), a border management regulation proposed in late 2016. In the opinion, the EDPS questions the proposed data collection practices envisioned as part of ETIAS and cautions against profiling tools because they raised "serious technical, legal, and ethical questions."

EDPS Announces 2018 International Conference of Data Protection and Privacy Commissioners

On March 13, the EDPS released a press statement announcing the 40th International Conference of Data Protection and Privacy Commissioners to be hosted in Brussels in October 2018. The conference will allow independent regulators on privacy and data protection to adopt high-level resolutions and recommendations addressed to governments and international organizations.

EDPS Seeks Stronger Consumer Protections in Digital Content Contracts

On March 14, the EDPS published an opinion concerning contracts for the supply of digital content. The EDPS highlighted the risk of confusion for consumers and businesses regarding new provisions in EU law that treat personal information as a commodity for exchange in digital contracts. The EDPS also warned of potential legal uncertainty should EU rules inadvertently interfere with the GDPR and forthcoming ePrivacy Regulation.

EU Commissioners Publish Joint Statement on Data Flows with Japan

On March 20, the European Commission issued a press release on the joint statement made by Vice

President Andrus Ansip and Commissioner Věra Jourová on data flows between Japan and the EU. According to the statement, both the Commission and Japan seek "close and regular exchanges between the EU and Japan on the data economy and increased cooperation for the free flow of data between the EU and Japan and ensuring high standards of data protection."

Commissioner Speaks on EU-U.S. Data Flows and Data Protection
On March 31, the European Commission published a commissioner's speech at the Center for Strategic and International Studies in Washington, which covered the Umbrella Agreement, e-evidence, online hate speech, the General Data Protection Regulation ("GDPR"), and the Privacy Shield. In the speech, the commissioner described the evolution of transatlantic data exchanges and commented that the Umbrella Agreement and the Privacy Shield would benefit citizens and businesses provided that they continue to be properly implemented.

Article 29 Working Party Issues Opinion on ePrivacy Regulation
On April 4, the Article 29 Working Party adopted an Opinion on the Proposed Regulation of the European Commission for the ePrivacy Regulation, which is intended to replace the ePrivacy Directive. In its opinion, the Working Party outlines four "grave" concerns that would lower the level of protection in place under the GDPR: (i) the tracking of the location of terminal equipment; (ii) the conditions under which the analysis of content and metadata is allowed; (iii) the default settings of terminal equipment and software; and (iv) tracking walls.

EDPS Issues Necessity Toolkit to Facilitate Policymaking
On April 11, the EDPS published a necessity toolkit designed to help policymakers identify the impact of new laws on the fundamental right to data protection and determine cases in which the limitation of this right is truly necessary. The toolkit provides policymakers with a practical step-by-step checklist, setting out the criteria to be considered by policymakers when they assess the necessity of new legislation and providing examples to illustrate each step. The toolkit is based on decisions issued by the Court of Justice and the European Court of Human Rights, as well as on Opinions published by both the EDPS and the Article 29 Working Party.

European Network and Information Security Agency

ENISA Provides Recommendations on Privacy Enhancing Technologies
On March 9, the European Network and Information Security Agency ("ENISA") published a document providing recommendations on how to build and maintain an online community for Privacy Enhancing Technologies ("PETs") maturity assessments. The community development approach guides developers and individuals with key skills they need to participate actively in the PETs. The document presents four areas to consider when developing the community: hosting and maintenance, dissemination and promotion, content generation and trust building, and continuous improvement.

France

France Further Implements Digital Republic Act
On March 14, the Prime Minister adopted two orders to further implement the Digital Republic Act. The first order (source document in French) provides that data processing decisions based on "algorithmic processing" have to mention: (i) the purpose of such processing; (ii) the right to obtain the processing rules; and (iii) the conditions under which such rights of access can be exercised. The second order (source document in French) relates to the availability of "reference data" and the conditions under which such data can be accessed.

CNIL Issues 2016 Activity Report
On March 31, CNIL issued its 2016 Activity Report (source document in French) describing 430 controls targeting the implementation of CCTV measures and personal data processing. The report also discusses the 7,703 claims it received relating to the online dissemination of personal data, marketing, the Internet of Things, and Wi-Fi tracking. According to the report, the majority of claims aimed to control the user's e-reputation through delisting and the removal of URLs.

France Implements National System of Health Data
On April 10, France launched (source document in French) the National System of Health Data ("SNDS"), a new database that compiles information related to health insurance and various medical records. The SNDS shares health care information to better assess health expenditures, health monitoring, and research in the health care sector. SNDS will be available only to certain public entities, but other private and public structures may request access for public interest purposes.

CNIL Fines Transportation Services Company
On April 13, CNIL fined a transportation services company €15,000 for failure to comply with French data protection laws. After investigating the company's practices, CNIL observed that the company did not follow required retention periods for personal data or appropriately delete payment card information.

Germany

Bavarian DPA Issues Guidance on Data Protection Impact Assessments
On March 13, the Bavarian Data Protection Authority ("DPA") published a paper (source document in German) on Data Protection Impact Assessments ("DPIA") as described in Art. 35 of the EU GDPR. DPIAs are required when a new technology's data processing might affect the rights and freedoms of natural persons, and the paper provides guidance on how to evaluate whether a DPIA is required and about the comprehensiveness of performing a DPIA.

Italy

DPA Approves DNA Database
On March 9, the Italian DPA approved a draft (source document in Italian) decree to regulate the nation's DNA database. As part of the decree, the DPA required strengthening the integrity of the data in the database, especially regarding the data of individuals acquitted of criminal charges. The DPA also stressed the need to provide data subjects with an adequate information notice.

DPA Fines Money Transfer Companies
On March 10, the Italian DPA fined (source document in Italian) five companies €11 million for operating a money transfer business involving the illicit use of personal data. To avoid tracking money transfers abroad and scrutiny under the anti-money laundering laws, the companies registered the transfers in the names of individuals who were deceased, nonexistent, or otherwise unaware of such transfers. The fines comprise the highest penalty ever issued by the Italian DPA.

Netherlands

Ministry of Security and Justice Publishes Statistics on Cybercrime
On March 1, the Ministry of Security and Justice published the Safetymonitor (source report in Dutch) annual report, which contains crime statistics in the Netherlands. The report includes figures on cybercrime since 2012 and notes that 10.7 percent of the Dutch population was the victim of cybercrime in 2016. Hacking was the most common offense, followed by fraud and cyberbullying.

Netherlands Issues Draft Bills on "UBO-register" and "Central Shareholder-register"
On March 31, the Netherlands published the first draft of a bill (source document in Dutch) aimed at implementing the Fourth Anti-Money Laundering Directive (2015/849/EU), which requires EU Member States to establish an Ultimate Beneficial Owner ("UBO") register. According to the draft bill, the publicly accessible data will contain personal data such as the UBO's name, date of birth, nationality, residence, and the nature and size of his or her stake in the respective organization. Parliament members have also submitted a proposal (source document in Dutch) on the Central Shareholder-register, opting for a register that will not be accessible to the public.

Spain

DPA Provides Guidance on Telecommunications Services Rights
On March 14, the Spanish Data Protection Agency ("DPA") launched a website (source document in Spanish) that provides information on the rights of telecommunications users and guidance on how to assert claims. This effort follows initiatives by the DPA to promote citizen awareness of rights and guarantees under Spanish law.

DPA Holds Ninth Annual Open Session
On May 25,the DPA held its Annual Open Session (source document in Spanish) to address, among other topics, the new GDPR provisions, implementation, the DPA's activities, and changes in Spanish law.

United Kingdom

UK Incorporates EU Data Protection Regulations
In March, the UK government issued a white paper setting out detailed proposals on how the United

Kingdom will leave the European Union following the service of its Article 50 notice. The "Great Repeal Bill" will incorporate existing EU law (including the GDPR) into UK law, effectively opting into the EU data protection regime.

ICO Fines Lawyer for Improper Storage of Client Information
On March 16, the Information Commissioner's Office ("ICO") fined a British barrister £1,000 for keeping records relating to 250 clients on his home computer and having accidentally uploaded the information to an internet directory as part of a software upgrade. Some files contained highly sensitive information related to court proceedings pending before the UK courts.

ICO Issues Draft Guidance on Consent under GDPR
On March 31, ICO issued draft guidance on the requirements for consent under the GDPR. While still subject to consultation, the guidance helps data controllers "decide when to rely on consent for processing and when to look at alternatives" and takes "account of future guidelines issued by relevant European authorities."

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

Asia, Africa, and the Middle East

Hong Kong

Securities and Futures Commission Tightens Cybersecurity Rules
Beginning in April, the Securities and Futures Commission ("SFC") announced efforts to strengthen cybersecurity rules after a series of hacking attacks of brokerage accounts over the past 18 months led to investor losses totaling HK$110 million. As part of these efforts, the SFC will launch a market consultation on proposals requiring brokers to upgrade their cybersecurity systems, which may include two-step authentication and transaction notification requirements.

PCPD Investigates Loss of Voters' Personal Data
On April 11, the Office of the Privacy Commissioner for Personal Data ("PCPD") issued a statement on the reported loss of registered voters' personal data. The PCPD is investigating the loss of two computers belonging to the Registration and Electoral Office to determine if any privacy violations occurred and whether personal data was compromised.

Japan

Cabinet Submits Bill Concerning De-Identified Medical Information
On March 10, the Diet began considering a bill (source document in Japanese) "concerning de-identified medical information to promote research and development in the medical field." The law aims to advance the use of health and medical information, after de-identification, for the purpose of advanced research and development in life sciences while securing the adequate protection of patient privacy.

Personal Information Protection Commission Releases Guidelines for Health Care Sector
On April 14, after a review of public comments, the Personal Information Protection Commission, together with the Ministry of Health, Labor and Welfare, released guidelines (source document in Japanese) concerning the Personal Information Protection Act for the health care sector. The guidelines discuss proper handling of personal information for medical and long-term-care business operators.

Ministry of Internal Affairs and Communications Amends Telecommunications Guidelines
On April 18, after a review of public comments, the Ministry of Internal Affairs and Communications released Guidelines Concerning Personal Information Protection in the Telecommunication Business and the accompanying commentary for these guidelines (source documents in Japanese). The guidelines specifically apply to telecommunication carriers.

People's Republic of China

China Passes Civil Law Relating to Personal Data Protection

On March 15, China passed the General Provisions of the Civil Law (source document in Chinese). The General Provisions, which will take effect on October 1, lay out various measures to protect the security and integrity of personal data.

CAC Issues Data Localization Requirements
On April 11, the Cyberspace Administration of China ("CAC") published a draft (source document in Chinese) on proposed "Measures for the Security Assessment of Outbound Transmission of Personal Information and Critical Data." The draft requires operators of key information infrastructure to keep within China critical data and personal information that they collect or generate in the course of operating their businesses. Under these measures, critical data or information can be released outside of China only if it passes a "security assessment." For more information, see the related Jones Day *Commentary*.

Singapore

PDPC Updates Anonymization Guidelines
On March 28, the Personal Data Protection Commission ("PDPC") announced updates to Chapter 3 of its Advisory Guidelines on the Personal Data Protection Act ("PDPA") for Selected Topics. The revisions "provide further clarity for organizations using and disclosing anonymized data, including further information on the considerations for assessing and managing the risks of re-identification from anonymized data."

PDPC Fines IT Services Company for PDPA Violations
On April 6, the PDPC ordered a $10,000 fine against a data intermediary IT services company for "failing to make reasonable security arrangements to prevent unauthorized access and unauthorized modification of [] customers' personal data"—violations under the PDPA.

Israel

Israel Passes Data Security and Data Breach Notification Requirements
On March 21, Israeli lawmakers enacted (unofficial translation) mandatory data security and data breach notification requirements on companies doing business in Israel. The new regulations apply to all data collected, processed, or held by public or private entities in Israel and govern information collected by multinational companies with a presence in Israel. The regulations allow courts to apply sanctions for data security breaches caused by negligence, adding criminal sanctions for some willful violations. The regulations are effective March 2018.

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

Australia

Law Requires Telecommunications Service Providers to Retain Metadata
Beginning on April 13, telecommunications service providers in Australia must collect and retain telecommunications data for a minimum period of two years. Metadata that must be retained includes the source, destination, date, time, duration, type of communication, and location of equipment or line used in connection with the communication. In addition, retained data must be encrypted and protected from unauthorized interference or access. Per a ruling from the Attorney General, civil litigants will not be allowed access to retained telecommunications data.

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

Jones Day Cybersecurity, Privacy, and Data Protection Lawyers

Emmanuel G. Baud Paris	Edward S. Chang Irvine	Po-Chien Chen Taipei	Richard DeNatale San Francisco
Joshua L. Fuchs Houston	Michael B. Hazzard Washington	Karen P. Hewitt San Diego	John E. Iole Pittsburgh

Jay Johnson
Dallas

Jeffrey L. Kapp
Cleveland

J. Todd Kennard
Columbus

Ted-Philip Kroke
Frankfurt

Jonathan Little
London

Kevin D. Lyles
Columbus

Richard M. Martinez
Minneapolis

Todd S. McClelland
Atlanta

Kristen P. McDonald
Atlanta

Daniel McLoon
Los Angeles

Nicole M. Perry
Houston

Jeff Rabkin
San Francisco

Elizabeth A. Robertson
London

Adam Salter
Sidney

Michiru Takahashi
Tokyo

Rhys Thomas
London

Michael W. Vella
Shanghai

John A. Vogt
Irvine

Sergei Volfson
Moscow

Undine von Diemar
Munich

Toru Yamada
Tokyo

Sidney R. Brown
Atlanta

Paloma Bru
Madrid

Laurent De Muyter
Brussels

Olivier Haas
Paris

Jörg Hladjk
Brussels

Celia Jackson
San Francisco

Guillermo E. Larrea
Mexico City

Christopher J. Lopata
New York

Giuseppe Mezzapesa
Milan

Laura Baldisserra
Milan

Peter T. Brabant
Sydney

Jeremy S. Close
Irvine

Daniel C. D'Agostini
São Paulo

Jennifer C. Everett
Washington

Marina Foncuberta
Milan

Chiara B.L. Formenti-Ujlaki
New York

Frances P. Forte
Atlanta

Bastiaan K. Kout
Amsterdam

Martin Lotz
Munich

Alexandra A. McDonald
San Francisco

Mary Alexander Myers
Atlanta

Kelly M. Ozurovich
Los Angeles

Mónica Peña Islas
Mexco City

Brandy H. Ranjan
Columbus

Ann T. Rossum
Irvine

Jessica M. Sawyer
Los Angeles

Alexa L. Sendukas
Houston

Kerianne N. Tobitsch
New York

Anand Varadarajan
Dallas

Nicola Walker
Sydney

Follow us on:

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