Global Privacy & Cybersecurity Update
Issue 17 | March 2018

JONES DAY

GLOBAL PRIVACY & CYBERSECURITY UPDATE

Jones Day Cybersecurity, Privacy & Data Protection Attorney Spotlight: Adam Salter

The recent introduction of mandatory data breach notification in Australia epitomizes the ever-evolving regulatory landscape and the various data privacy and cybersecurity considerations central to international business expansion. International expertise is critically important.

Adam Salter is a partner based in Sydney who leads Jones Day's Australian Cybersecurity, Privacy & Data Protection Practice. Adam has more than 20 years of experience practicing in Australia and elsewhere in the Asia-Pacific region (including in Hong Kong and Singapore), advising domestic and international clients on cybersecurity, personal data privacy, and security issues.

Adam regularly assists clients with drafting Australian privacy policies and procedures, contractual and statutory data privacy obligations (including the collection and transfer of personal information), and data privacy issues relating to Australian cross-border private treaty mergers and acquisitions, corporate reorganizations, joint ventures, strategic alliances and outsourcing of services. Adam is also presently advising a number of clients on how to comply with obligations under the mandatory data breach notification rules in Australia and on how to respond to data breaches there to minimize legal risk

United States

Regulatory—Policy, Best Practices, and Standards

CFTC and SEC to Coordinate Efforts on Virtual Currency Enforcement Actions
On January 25, Securities and Exchange ("SEC") Chairman Jay Clayton and Commodity Futures Trading Commission ("CFTC") Chairman J. Christopher Giancarlo jointly published an op-ed in *The Wall Street Journal*. The article discusses the combined intention of both regulatory agencies to set and enforce rules that foster innovation while promoting market integrity and confidence for initial

EDITORIAL CONTACTS

Daniel J. McLoon
Los Angeles

Mauricio F. Paez
New York

Jay Johnson
Dallas

Jonathon Little
London

Todd S. McClelland
Atlanta

Jeff Rabkin
San Francisco

Lisa M. Ropple
Boston

Adam Salter
Sydney

Michiru Takahashi
Tokyo

Undine von Diemar
Munich

Olivier Haas
Paris

Jörg Hladjk
Brussels

Editor-in-Chief: Anand Varadarajan

HOT TOPICS IN THIS ISSUE

coin offerings and related cryptocurrency markets. The agencies issued a joint statement on the topic as well.

Regulatory—Critical Infrastructure

NIST Updates Cybersecurity Framework
On December 5, 2017, the National Institute of Standards and Technology ("NIST") published the second draft of the proposed update to the Framework for Improving Critical Infrastructure Cybersecurity. NIST announced that the new draft is intended to clarify, refine, and enhance the Cybersecurity Framework, and anticipates finalizing Cybersecurity Framework version 1.1 in spring 2018.

Regulatory—Consumer and Retail

FTC Hosts a Workshop on Informational Injury to Consumers
On December 12, 2017, the FTC hosted an Informational Injury workshop to discuss injuries consumers suffer when their information is misused. Maureen Ohlhausen, acting FTC Chairman, provided remarks at the workshop about qualitatively and quantitatively measuring these injuries and applicable frameworks for businesses to evaluate the risks leading to these injuries.

Senators Seek to Establish Cybersecurity Office within FTC
On January 10, U.S. Senators Elizabeth Warren (D-Mass.) and Mark Warner (D-Va.) introduced a bill to establish an Office of Cybersecurity within the FTC to supervise data security at consumer reporting agencies. Under the proposed regulation, the Office will issue "regulations establishing standards for effective cybersecurity at consumer reporting agencies" and "impose penalties on credit reporting agencies for cybersecurity breaches that put sensitive consumer data at risk."

Regulatory—Energy/Utilities

Secretary of Energy Forms New Office of Cybersecurity, Energy Security, and Emergency Response
On February 14, U.S. Secretary of Energy Rick Perry announced the creation of the Office of Cybersecurity, Energy Security, and Emergency Response ("CESER") at the U.S. Department of Energy. CESER will be led by an Assistant Secretary, yet to be named, and the office will focus on energy infrastructure security and support the department's newly assigned national security responsibilities.

Regulatory—Financial

SEC Issues Public Statement on Cryptocurrencies and Initial Coin Offerings
On December 11, 2017, SEC Chairman Jay Clayton issued a public statement on cryptocurrencies and initial coin offerings ("ICOs"), listing out considerations for market professionals and main street investors. The statement includes "sample questions" for investors considering an investment opportunity in ICOs or cryptocurrency.

OCC Publishes Semiannual Risk Perspective, Identifies Cybersecurity and Fintech as Key Risk Areas for Banks
On January 18, the U.S. Office of the Comptroller of the Currency ("OCC") released its Semiannual Risk Perspective for Fall 2017 and identified several key data

Brexit on EU Data Protection Law

China Releases Final Personal Information Protection Standard

Australian Data Breach Notification Amendment Takes Effect

RECENT AND PENDING SPEAKING ENGAGEMENTS

Tabletop Exercise: A Breach … Now What?, 2nd Annual Cybersecurity and Data Privacy Law Conference, Plano, TX (Apr. 2018). **Jones Day Speaker: Jay Johnson**

A Gloves Off Discovery Fight, 2nd Annual Cybersecurity and Data Privacy Law Conference, Plano, TX (Apr. 2018). **Jones Day Speaker: Jay Johnson**

Future of Cybersecurity, Stanford Law Cybersecurity Symposium, Palo Alto, CA (Apr. 2018). **Jones Day Speaker: Samir Jain**

Status of the ePrivacy Regulation—Impact on Business GDD International Seminar, GDD-Fachtagung Datenschutz International, Berlin, Germany (Apr. 2018). **Jones Day Speaker: Jörg Hladjk**

Privacy Challenges and Solutions for Blockchain Projects in the Context of GDPR, IAPP Europe Data Protection Intensive 2018, London, England (Apr. 2018). **Jones Day Speaker: Olivier Haas**

Blockchain: Best Practices and Legal Issues, Paris, France (Apr. 2018). **Jones Day Speakers: Philippe Goutay, Olivier Haas**

International Cybersecurity, Stanford University, Palo Alto, CA (Apr. 2018). **Jones Day Speaker: Jeff Rabkin**

GDPR Is Coming: Is Your Company Ready?, ARMA International (Association of Records Managers and Administrators), Chicago, IL (Apr. 2018). **Jones Day Speaker: Aaron Charfoos**

Department of Justice Perspective on Key Surveillance Controversies, IAPP Global Privacy Summit, Washington, D.C. (Mar. 2018). **Jones Day Speaker: Samir Jain**

Artificial Intelligence & Law, Paris Artificial Intelligence, Paris, France (Mar. 2018). **Jones Day Speaker: Olivier Haas**

Legal Issues for Cooperative Responses to Malicious Cyber

and privacy risk areas facing banks and other financial institutions today. The OCC found that the severity of cyber threats has increased and that criminals continue to target personal information in aggressive, innovative new ways. The OCC also warned that institutions' over-reliance on a few third-party servicers creates the risk of "concentrated points of failure" should one of these servicers suffer a data breach or other cyberattack.

SEC Appoints Receiver in Action Involving ICO and Alleged Cryptocurrency Bank
On January 30, the SEC announced its action against an allegedly fraudulent ICO initiated by a cryptocurrency banking platform. The SEC detailed how the company "falsely stated that it purchased an FDIC-insured bank" and failed "to disclose the criminal background of key executives." The SEC obtained an emergency freeze order from the court, which also appointed a receiver to handle and manage all assets of the company, including the digital cryptocurrency assets, while the case is resolved. For more information, see the Jones Day *Alert*.

SEC Office of Compliance Inspections and Examinations Announces 2018 Examination Priorities
On February 7, the SEC's Office of Compliance Inspections and Examinations ("OCIE") announced that cybersecurity was one of its 2018 examination priorities. Each of OCIE's examination programs will prioritize cybersecurity with an emphasis on, among other things, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.

SEC FY 2019 Budget Requests Funds for Additional Cybersecurity Staff, Security Improvements
On February 12, the SEC released its proposed FY 2019 budget. The SEC requested funds for four additional staff positions, all focused on cybersecurity, with particular focus on "incident management and response, advanced threat intelligence monitoring, and enhanced database and system security." The proposal stated that cybersecurity is going to be one of the SEC's top priorities in FY 2019 and that the request will enable the SEC to support increased investment in tools, technologies, and services, including moving the SEC from legacy IT systems to modern platforms with improved security features.

SEC Updates Cybersecurity Guidance
On February 21, the SEC issued new guidance on public company cybersecurity disclosures, and Chairman Clayton provided an accompanying statement emphasizing the SEC's expectations that public companies: (i) implement comprehensive cybersecurity policies that allow them to make accurate and timely disclosure of material cybersecurity risks and events; and (ii) prohibit insider trading based on selective disclosure of cyber risks or incidents. The guidance follows a 2011 release addressing similar topics. For more information, see the Jones Day *Alert*.

Regulatory—Transportation

Department of Transportation Hosts Roundtable on Data for Automated Vehicle Safety
On December 7, 2017, the Department of Transportation ("DOT") hosted the Roundtable on Data for Automated Vehicle Safety. More than 60 participants from businesses, nonprofit organizations, universities, research

Activity Below Use of Force, MIT Cyber Norms 6.0, Cambridge, MA (Mar. 2018). **Jones Day Speaker: Samir Jain**

The Anatomy of a Cyber Attack, Second Annual Boston Conference on Cybersecurity (sponsored by Boston College), Boston, MA (Mar. 2018). **Jones Day Speaker: Lisa Ropple**

Preparing for Cyber Security Incidents, New England Corporate Counsel Association, Waltham, MA (Mar. 2018). **Jones Day Speaker: Lisa Ropple**

Cybersecurity, Litigation Risk, and Disruptive Technology, University of California, Hastings College of the Law, San Francisco, CA (Mar. 2018). **Jones Day Speaker: Jeff Rabkin**

Security Visibility, Monitoring & Incident Response, CISO Executive Network, Dallas, TX (Mar. 2018). **Jones Day Speaker: Jay Johnson**

Security Visibility, Monitoring & Incident Response, CISO Executive Network, Houston, TX (Mar. 2018). **Jones Day Speaker: Nicole Perry**

GDPR Is Coming: Is Your Company Ready?, Jones Day and Navigant Consulting, Chicago, IL (Mar. 2018). **Jones Day Speaker: Aaron Charfoos**

A Picture Is Worth a Thousand Litigations: Current Trends In The Illinois Biometric Information Privacy Act, IAPP Chicago Knowledgnet, Chicago, IL (Mar. 2018). **Jones Day Speakers: Aaron Charfoos, Efrat Schulman**

GDPR Is Coming: Is Your Company Ready?, ISACA (Information Systems Audit and Control Association, Inc.) and IAPP Knowledgenet, Chicago, IL (Mar. 2018). **Jones Day Speaker: Aaron Charfoos**

Challenges for Data Processors under GDPR, EMEA Conferences, Bucharest, Romania (Feb. 2018). **Jones Day Speaker: Jörg Hladjk**

Vulnerability and Threat Management, CISO Executive Network, Washington D.C. (Feb. 2018). **Jones Day Speaker: Samir Jain**

The Regulation of Data, Brussels School of Competition's New Study

centers, and federal, state, and local government attended to provide feedback on the DOT's draft *Guiding Principles on Voluntary Data Exchanges to Accelerate Safe Deployment of Automated Vehicles* and draft *Framework for Voluntary Data Exchanges to Accelerate Safe Deployment of Automated Vehicles*. The participants also identified and discussed the data exchanges they believed were most critical, which included improving cybersecurity for automated vehicles.

Department of Transportation Publishes Automated Vehicle Notices for Public Comment
On January 10, the Department of Transportation published four automated vehicle notices for public comment on its website as part of its efforts to advance the release of Federal Automated Vehicle Policy 3.0, also known as A Vision for Safety 3.0. The published notices included: (i) the Federal Highway Administration's Request for Information (RFI) on Integration of ADS into the Highway Transportation System; (ii) the National Highway Traffic Safety Administration's Request for Comments on Removing Regulatory Barriers for Automated Vehicles; (iii) the Federal Transit Administration's Request for Comments on Automated Transit Buses Research Program; and (iv) the Federal Transit Administration's Request for Comments on Removing Barriers to Transit Bus Automation.

Regulatory—Defense and National Security

Department of Commerce and Department of Homeland Security Release Draft Report on Cybersecurity Threats
On January 5, the Department of Commerce and Department of Homeland Security ("DHS") released a draft report for public comment in response to the May 11, 2017, Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The report, titled "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," identified five goals "that would dramatically reduce the threat of automated, distributed attacks and improve the resilience of the ecosystem." The final report is due to President Trump on May 11.

State Department Announces Proposal to Create New State Department Bureau to Handle Cybersecurity
On February 6, the State Department announced a proposal to create a new cybersecurity bureau. The State Department proposed that the new office be led by a Senate-confirmed assistant secretary, who would "formulate and coordinate a strategic approach necessary to address current and emerging cyber security and digital economic challenges."

Regulatory—Health Care/HIPAA

Bankrupt Document Storage Business Settles with OCR for HIPAA Violations
On February 13, the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") settled alleged HIPAA violations with a company that provided document storage and other services for health care companies. OCR's lengthy investigation began when numerous medical records—constituting unsecured protected health information—were left by company personnel at a recycling facility without any security

Programme on Cognitive Technologies & Artificial Intelligence, Federation of Enterprises in Belgium, Brussels, Belgium (Jan. 2018). **Jones Day Speaker: Laurent De Muyter**

Preparing for Cyber-Security Incidents: What to Expect and How to Reduce Impact, Pittsburgh Speaker Series, Pittsburgh, PA (Jan. 2018). **Jones Day Speaker: Lisa Ropple**

The European Union's General Data Protection Regulation (GDPR), Jones Day MCLE University, San Francisco, CA (Jan. 2018). **Jones Day Speakers: Undine von Diemar, Jörg Hladjk**

The ePrivacy Regulation, Jones Day MCLE University, San Francisco, CA (Jan. 2018). **Jones Day Speakers: Undine von Diemar, Jörg Hladjk**

Cybersecurity: Managing Evolving Risks, Jones Day MCLE University, Irvine, CA (Jan. 2018). **Jones Day Speakers: Undine von Diemar, Jörg Hladjk**

Managing Vulnerabilities and Threats, CISO Executive Network, Houston, TX (Jan. 2018). **Jones Day Speaker: Nicole Perry**

Protecting PII—Balancing Data Security and Global Privacy Laws, cyberSecure, New York, NY (Dec. 2017). **Jones Day Speaker: Jay Johnson**

GDPR Is Coming: Is Your Company Ready?, ARMA International (Association of Records Managers and Administrators), Chicago, IL (Dec. 2017). **Jones Day Speaker: Aaron Charfoos**

Cybersecurity Risk, Association of Corporate Counsel, Boston, MA (Dec. 2017). **Jones Day Speaker: Lisa Ropple**

RECENT AND PENDING PUBLICATIONS

The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues, *New York Law Review* (Apr. 2018). **Jones Day Authors: Mauricio Paez, Kerianne Tobitsch**

New York's Top Court Rules 7–0: "Private" Facebook Posts Subject to Disclosure (Feb. 2018). **Jones Day Authors: Harold Gordon, Rebekah Blake, James Jones**

Data Protection in Business

measures or other precautions. Despite no longer being in business, the company settled with OCR for $100,000 to cover the cost of properly and securely disposing of remaining unsecured medical records in its possession.

Litigation, Judicial Rulings, and Agency Enforcement Actions

Washington State Attorney General Sues Transportation Services Company Over Data Breach
On November 28, 2017, Washington's Attorney General Bob Ferguson announced a lawsuit against a transportation services company for violating the state's data breach notification law. The lawsuit stems from the company's announcement that it had paid hackers $100,000 in late 2016 to destroy data on more than 57 million customers and drivers that had been stolen from the company.

Circuit Court Rules Website User Data is Not Personal Information
On November 29, 2017, the Ninth Circuit ruled that although a sports app user claiming the sports network disclosed his private information to an analytics company had standing to sue, a lower court was right to dismiss his suit because the information was not personally identifiable under the Video Privacy Protection Act. The Ninth Circuit affirmed a Washington federal judge's application of the "ordinary person" standard, which determined that "personally identifiable information" refers to information an ordinary person could use to pinpoint a specific individual's video watching behavior.

FTC Settles Software Privacy Violations with Personal Electronics Manufacturer
On January 2, the FTC settled with a personal electronics manufacturer regarding allegations that the manufacturer preloaded advertising software onto its laptops that interfered with a user's internet browser and seriously compromised the browser's security. The settlement prohibits the manufacturer from misrepresenting any features of software preloaded onto its laptops and requires the manufacturer to implement a comprehensive software security program for most consumer software preloaded onto its laptops for the next 20 years.

Operations in the European Union—Regulatory, book chapter, *Bloomberg Portfolio* (Feb. 2018). **Jones Day Author: Jörg Hladjk**

SEC Releases Guidance on Public Company Cybersecurity Disclosures (Feb. 2018). **Jones Day Authors: Samir Jain, Jay Johnson, David Woodcock, John Tang**

Appellate Court Limits Who May Sue Under Biometric Information Privacy Act (Jan. 2018). **Jones Day Authors: Todd Kennard, Aaron Charfoos, William Dolan, Jackson Lavelle**

How the Distributed Public Ledger Affects Blockchain Litigation, *Banking and Financial Services Policy Report* (Jan. 2018). **Jones Day Author: Aaron Charfoos**

China Cyber Security Law from the Business Perspectives, *J+C Economic Journal,* (Dec. 2017). **Jones Day Authors: Michiru Takahashi, Kadomatsu Shinji**

Japan Legal Update | Vol. 31 (Nov. 2017). **Jones Day Authors: Various**

Legal Issues Related to the Development of Automated, Autonomous, and Connected Cars (Nov. 2017). **Jones Day Authors: Various**

Biometric Data in the Workplace Could Trigger Privacy Litigation Wave (Nov. 2017). **Jones Day Authors: Todd Kennard, Jackson Lavelle**

FTC Settles Violations of Children's Privacy Law Allegations with Electronic Toy Maker
On January 8, the FTC announced that it reached a settlement with an electronic toy maker over allegations that the toy maker violated the Children's Online Privacy Protection Act. According to the complaint, the toy maker collected personal information from children and parents without providing direct notice and obtaining their parents' consent, and failed to take reasonable steps to secure the data collected. As part of the settlement, the company will pay a $650,000 fine and is required to implement a comprehensive data security program, which is subject to independent audit for the next 20 years. The FTC noted that this was its first children's privacy case involving internet-connected toys.

Supreme Court Declines to Revisit *Spokeo*'s Standing Rule
On January 22, the U.S. Supreme Court declined to revisit the Article III standing bar that it had established in its pivotal 2016 *Spokeo* decision. In the 2016 decision, the High Court reviewed whether the plaintiff had established standing for alleged violations of the Fair Credit Reporting Act by the defendant. The Court announced that plaintiffs cannot rely solely on statutory violations to establish Article III standing and remanded the case back to the Ninth Circuit. Seeking to have the Ninth Circuit's decision overruled, the defendant petitioned the Supreme Court, pleading the Court to resolve the "widespread confusion" over what types of intangible injuries are capable of being used to establish standing; however, the Supreme Court declined to hear the case a second time.

Federal Judge Approves Settlement in Case Involving Leaked Tax Data
On January 24, a North Carolina federal judge granted preliminary approval to a proposed settlement between an aircraft maintenance company and its employees, who have accused the company of falling for a phishing scheme and emailing sensitive tax information of at least 3,000 employees to

cybercriminals. In addition to a $250 payment for each affected individual, the proposed settlement requires the company to implement various measures to improve its data security practices.

Legislative—Federal

House Passes Bill to Reorganize DHS's Cybersecurity Efforts
On December 11, 2017, the House of Representatives passed the Cybersecurity and Infrastructure Security Agency Act of 2017, which reorganizes the cybersecurity and infrastructure operations of DHS and adds new leadership positions, including a director responsible for reporting to Congress. The bill seeks to enable U.S. companies to coordinate with DHS during cyber incidents and help streamline DHS's ability to carry out its cybersecurity mission. The legislation awaits a vote in the Senate.

House Bill Seeks to Examine DHS's Cyber Vulnerabilities
On January 9, the House of Representatives passed the Cyber Vulnerability Disclosure Reporting Act, which requires the Secretary of DHS to report to Congress on its policies and procedures for coordinating on cybersecurity vulnerabilities with the private sector and other agencies. The bill has been referred to the Senate Committee on Homeland Security and Government Affairs.

House Passes Cyber Diplomacy Act of 2017
On January 17, the House of Representatives passed the Cyber Diplomacy Act of 2017, a bill that would reestablish an Office of Cyber Issues within the State Department, with a leader appointed by the president and confirmed by the Senate, having the same status and privileges as a United States ambassador. The legislation would also require the Secretary of State to coordinate with other relevant federal departments and agencies to produce a strategy dedicated to the United States' international cyberspace policy. The bill remains without a sponsor in the Senate.

Congress Renews Foreign Intelligence Surveillance Authority
On January 18, the Senate passed the amended bill to reauthorize Section 702 of the Foreign Intelligence Surveillance Act ("FISA") for six years, now Public Law No. 115-18. The FISA program, which was set to expire on January 19, allows intelligence agencies to collect data on foreign nationals suspected to be national security threats who use American communication services and internet technology. The final version of the legislation did not contain a proposed amendment supported by privacy advocates, called the USA Rights Act, which would have required a warrant for searching the FISA intelligence database for information on Americans. The legislation had already been approved by the House of Representatives.

Legislative—States

House Passes Bill to Reorganize DHS's Cybersecurity Efforts
On December 11, 2017, the House of Representatives passed the Cybersecurity and Infrastructure Security Agency Act of 2017, which reorganizes the cybersecurity and infrastructure operations of DHS and adds new leadership positions, including a director responsible for reporting to Congress. The bill seeks to enable U.S. companies to coordinate with DHS during cyber incidents and help streamline DHS's ability to carry out its cybersecurity mission. The legislation awaits a vote in the Senate.

House Bill Seeks to Examine DHS's Cyber Vulnerabilities
On January 9, the House of Representatives passed the Cyber Vulnerability Disclosure Reporting Act, which requires the Secretary of DHS to report to Congress on its policies and procedures for coordinating on cybersecurity vulnerabilities with the private sector and other agencies. The bill has been referred to the Senate Committee on Homeland Security and Government Affairs.

House Passes Cyber Diplomacy Act of 2017
On January 17, the House of Representatives passed the Cyber Diplomacy Act of 2017, a bill that would reestablish an Office of Cyber Issues within the State Department, with a leader appointed by the president and confirmed by the Senate, having the same status and privileges as a United States ambassador. The legislation would also require the Secretary of State to coordinate with other relevant federal departments and agencies to produce a strategy dedicated to the United States' international cyberspace policy. The bill remains without a sponsor in the Senate.

Congress Renews Foreign Intelligence Surveillance Authority
On January 18, the Senate passed the amended bill to reauthorize Section 702 of the Foreign Intelligence Surveillance Act ("FISA") for six years, now Public Law No. 115-18. The FISA program, which was set to expire on January 19, allows intelligence agencies to collect data on foreign nationals suspected to be national security threats who use American communication services and internet technology. The final version of the legislation did not contain a proposed amendment supported by privacy advocates, called the USA Rights Act, which would have required a warrant for searching the FISA intelligence database for information on Americans. The legislation had already been approved by the House of Representatives.

Canada

OPC Issues Position on Online Reputation
On January 26, Canada's Office of the Privacy Commissioner ("OPC") published a draft position on

reputation and privacy in the online world. The OPC's report, which responds to a public consultation, outlines various considerations and approaches such as de-indexing, source takedown, and other educational efforts needed to fully address the issue.

The following Jones Day lawyers contributed to this section: Jeremy Close, Meredith Collier, David Coogan, Jeff Connell, Jennifer Everett, Chiara Formenti-Ujlaki, Nick Hidalgo, Jay Johnson, Tyson Lies, Laura Lim, Dan McLoon, Mary Alexander Myers, Mauricio Paez, Nicole Perry, Alexa Sendukas, Aaron Tso, and Anand Varadarajan.

[Return to Top]

Latin America

Chile

Superintendent of Banks and Financial Institutions Issues New Regulation
On January 24, the Superintendent of Banks and Financial Institutions (*Superintendencia de Bancos y Instituciones Financieras*) issued (source document in Spanish) a regulation requiring financial entities to incorporate certain cybersecurity steps into managerial policies. The entities must now disclose logical information assets considered critical to the business operation and to the financial system. In addition, the regulation encourages financial institutions to develop secure practices without intervention or mandates from the government.

Colombia

Ministry of Commerce, Industry, and Tourism Amends Database Laws
On January 18, the Ministry of Commerce, Industry, and Tourism published a decree (source document in Spanish) modifying the type of databases that must be registered with the National Registry of Databases (*Registro Nacional de Bases de Datos*). Under the regulation, only databases containing personal data processed by public entities, nonprofit companies, or entities with greater than 100,000 tax value units must be registered.

Mexico

INAI Approves Personal Data Protection Guidelines for Public Sector
On January 26, the Plenum of the National Institute of Transparency, Access to Information, and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* or "INAI") issued a decree (source document in Spanish) approving the Personal Data Protection Guidelines for the Public Sector (*Lineamientos Generales de Protección de Datos Personales para el Sector Público*). The guidelines outline the necessary provisions for applying the General Law on the Protection of Personal Data held by Government Agencies (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados)*.

INAI to Seek Personal Data Protection During Electoral Process
On February 2, INAI President Javier Acuña Llamas announced (source document in Spanish) publicly that INAI, supported by other governmental authorities, will seek to protect personal data of Mexican citizens during the ongoing 2018 electoral process.

The following Jones Day lawyers contributed to this section: Guillermo Larrea, Daniel D'Agostini, and Abigail Ruiz.

[Return to Top]

Europe

European Union

European Commission Files Amicus Brief in U.S. Supreme Court Case *Microsoft Inc. v. the United States*
In December 2017, the European Commission filed an amicus brief asking the U.S. Supreme Court to respect the principles of international comity and territoriality when interpreting U.S. law. The case raises the question of whether the United States can oblige Microsoft to hand over information stored on a server owned by one of Microsoft's EU subsidiaries and physically located in Ireland.

Article 29 Working Party

Article 29 Working Party Issues Joint Review of the EU–U.S. Privacy Shield
On November 28, 2017, the Article 29 Working Party published the *EU–U.S. Privacy Shield—First Annual Joint Review*, which assesses the commercial aspects of the Privacy Shield, the government access to

personal data transferred from the European Union, and the legal remedies available to EU citizens.

Article 29 Working Party Releases Draft Guidelines on Consent and Transparency Under GDPR
On November 28, 2017, the Article 29 Working Party adopted draft *Guidelines on Consent under Regulation 2016/679 (GDPR).* The draft Guidelines focus on the changes under the General Data Protection Regulation ("GDPR"), providing practical guidance to ensure compliance with the GDPR and building upon the existing Article 29 Working Party's Opinion 15/2011 on consent. On the same day, the Article 29 Working Party also adopted draft *Guidelines on Transparency under Regulation 2016/679 (GDPR)*. They provide guidance and interpretative assistance on the new obligation of transparency concerning the processing of personal data under the GDPR.

Article 29 Working Party Updates Guidance on Adequacy Decisions for Personal Data Transfers
On November 28, 2017, the Article 29 Working Party released (source document requires sign-in) the *Working Document on Adequacy Referential (update of Chapter One of WP12)*, which updates its previous guidance on transfers of personal data to countries outside the European Union. The document addresses how to assess the level of data protection in other countries by establishing the core data protection principles that have to be present in the country's legal framework.

Article 29 Working Party Adopts Working Documents on Binding Corporate Rules for Controllers and Processors
On November 29, 2017**,** the Article 29 Working Party adopted two Working Documents (source document requires sign-in) on binding corporate rules for controllers and processors. The documents aim to facilitate the use of binding corporate rules by corporate groups engaged in a joint economic activity for international transfers from organizations established in the European Union to organizations within the same group established outside the European Union.

Austrian Data Protection Chief Elected Article 29 Working Party Chairperson
On February 7, the European data protection authorities elected Andrea Jelinek as the new chairperson of the Article 29 Working Party. Jelinek was previously the data protection chief in Austria, and she will oversee the Article 29 Working Party's transition to the European Data Protection Board under the GDPR in the coming months.

European Data Protection Supervisor

EDPS Adopts Opinion on Proposal for Regulation on ECRIS-TCN
On December 12, 2017, the European Data Protection Supervisor ("EDPS") adopted *Opinion 11/2017 on the Proposal for a Regulation on ECRIS-TCN*. The opinion recommends that ECRIS (a system for sharing information about criminal convictions in the context of judicial cooperation) and ECRIS-TCN (the ECRIS system used for non-EU country nationals) follow the data protection principle of purpose limitation. As such, the opinion suggests that any access by EU bodies be necessary, proportionate, and strictly limited to relevant tasks within the mandate of those EU bodies.

EDPS Ethics Advisory Group Publishes Report on Digital Ethics
In January, EDPS's Ethics Advisory Group issued a report on digital ethics that focuses on terms and concepts regarding the future of ethics in a full-fledged digital society. The report previews the 40th International Conference of Data Protection and Privacy Commissioners, which the EDPS will co-host in October 2018.

EDPS Organizes Workshops on New Data Regulation
On May 25, the GDPR will replace the current Regulation (EC) No. 45/2001. To raise awareness on the current and new data protection rules, EDPS organized a series of workshops in Luxembourg, which are also available online.

European Network and Information Security Agency

ENISA Releases Study on Privacy and Data Protection in Mobile Applications
On January 29, the European Network and Information Security Agency ("ENISA") published a report on *Privacy and Data Protection in Mobile Applications—A Study on the App Development Ecosystem and the Technical Implementation of GDPR.* The report provides a meta-study on privacy and data protection in mobile apps by analyzing the features of the app development environment that affect privacy and security, as well as defining relevant best practices, open issues, and gaps in the field.

ENISA Publishes Report on Developing Cybersecurity Culture within Organizations
On February 6, ENISA published the *Cybersecurity Culture in Organizations* report to better understand the dynamics of how cybersecurity culture can be developed and shaped within organizations. The report includes experiences gathered from existing cybersecurity programs implemented within organizations and contains good practices, methodological tools, and step-by-step guidance for those seeking to enhance their organization's own cybersecurity culture.

Belgium

Belgian Data Protection Authority to Replace Belgian Privacy Commission
On January 10, the *Belgian Official Gazette* published (source document in French and Dutch) the law establishing the Belgian Data Protection Authority, which will supplant the Privacy Commission. The law adapts the Belgian institutional framework to the GDPR because the current Belgian Privacy Commission has limited prosecutorial powers and no direct sanctioning powers.

France

ANSSI and ACPR to Cooperate on Cyber Threats in Financial Sector
On January 17, the French Network and Information Security Agency ("ANSSI") and the Prudential Supervisory Authority ("ACPR") signed a letter of intent (source document in French) promising to coordinate cyber-threat response efforts. In particular, the agencies plan to engage in regular information -sharing to minimize disruption to the banking and financial services industry.

ANSSI Announces Focus on Digital Security
On January 23, the ANSSI stated (source document in French) that it will focus throughout 2018 on reinforcing European digital security and supporting the European Union's ability to regulate the cyberspace and raising awareness on cybersecurity issues.

CNIL and INRIA Award Privacy Protection Price to European Research Team
On January 26, the French National Institute for Research in Computer Science and Control ("INRIA") and the French Data Protection Authority (*Commission nationale de l'informatique et des libertés*) ("CNIL") awarded (source document in French) the European prize to the authors of an article titled "Engineering Privacy by Design Reloaded." The prize promotes scientific research on privacy protection, GDPR requirements, Privacy by Design, and accountability. The wining article analyzes methods used by engineers to apply strategies of Privacy by Design by highlighting different strategies of minimization and providing guidelines to reduce the amount processed by data controllers or data processors.

CNIL Releases Privacy Impact Assessment Software
On January 29, CNIL launched a beta version of its privacy impact assessment ("PIA") software, as required by the GDPR. The new version includes new languages, a revised workflow, and bug corrections. The PIA software is published under a free license and may be updated by anyone in the community.

ANSSI Warns of Specific Security Threats
In January, ANSSI warned that specific threats known as "Meltdown" and "Spectre" (source document in French) may give unauthorized access to protected information.

Germany

Bavarian DPA Publishes Synopsis on ePrivacy Regulation
On January 29, the Bavarian Data Protection Authority ("DPA") published a synopsis (source document in German) of the legislative procedure of the ePrivacy Regulation. The ePrivacy Regulation is the upcoming legal framework for data processing, especially as it relates to electronic communications and over-the-top services. The DPA announced that it would update the synopsis once the European Council publishes its legislative proposal.

DSK Issues Comprehensive Data Privacy Guidance
In January, the German Data Protection Conference (*Datenschutzkonferenz* ("DSK")) published guidance on CCTV systems, commissioned data processing, processing of employee data, and the data protection officer (source documents in German). The guidance, which incorporates GDPR mandates, follows a meeting and consensus of the various German data protection authorities.

Italy

Italian Data Protection Authority Authorizes System for Remote Monitoring of Phone Traffic

In January, the Italian Data Protection Authority authorized a project submitted by a multinational company. The project will allow the company to process personal data from mobile phones assigned to the company's employees in order to reduce business costs and evaluate the adequacy of the agreement with the telephone service provider. However, the company must still reach agreements with labor unions in order to achieve compliance with applicable labor laws.

The Netherlands

Online Vacation Services Company Ends Processing of National Identity Numbers
On December 15, 2017, the Dutch Data Protection Authority ("DDPA") announced (source document in Dutch) that an American online vacation services company ended the processing of Dutch national identity numbers ("BSN"), per the order of the DDPA. The company now immediately and automatically deletes the BSN from all digital copies of Dutch identity documents and has deleted all previously collected national identity numbers.

DDPA Advises on Implementation of Second Payment Services Directive
On December 20, 2017, at the request of the Minister of Finance, the DDPA issued a statement (source document in Dutch) on the draft of the Implementation Decree Revised Directive on Payment Services (*Implementatiebesluit herziene richtlijn betaaldiensten*). The statement discusses specific steps and actions that must be taken to bring the Directive in line with GDPR requirements.

House of Representatives Examines Bill Implementing GDPR
In December 2017, the Dutch Implementation Act GDPR (*Uitvoeringswet Algemene Verordening Gegevensbescherming*) ("UAVG") (source document in Dutch) was submitted to the House of Representatives for review. The UAVG will take effect along with the GDPR on May 25, 2018, and contains a specific regulation for the processing of biometric data.

DDPA Begins GDPR Education
In January, the DDPA initiated an information campaign (source document in Dutch) to educate the public about the GDPR. Aleid Wolfsen, chairman of the DDPA, kicked off the campaign with a privacy lesson at a primary school. The campaign aims to make people more aware of their privacy rights and offers organizations practical help with compliance with the law.

Spain

Spanish DPA and SFMP Collaborate on GDPR Principles
On December 4, 2017, the Spanish Data Protection Agency ("DPA") and the Spanish Federation of Municipalities and Provinces ("SFMP") agreed (source document in Spanish) to jointly educate the public regarding the GDPR. The agreement aims to provide tools, guidelines, trainings, and publications to help local entities with the transition to the GDPR.

AUTOCONTROL and Spanish DPA Implement Voluntary Mediation System
On January 9, AUTOCONTROL, the independent advertising self-regulatory organization in Spain, announced (source document in Spanish) the implementation of a new voluntary mediation system developed in collaboration with the Spanish DPA. The optional mediation system addresses claims related to data protection issues, such as the reception of spam, phishing, and data processing complaints. The system took effect on January 1.

Spanish DPA Issues First Provisional Authorization to Certify Data Protection Officers
On January 16, the Spanish DPA announced that it had authorized a certification body to provisionally certify data protection officers pursuant to the certification scheme developed together with the National Accreditation Entity. The accreditation (source document in Spanish) process would be finalized once the National Accreditation Entity provides certification as well.

United Kingdom

EU Commission Advises on Effects of Brexit on EU Data Protection law
On January 9, the EU Commission issued a notice on the potential implications of Brexit for transfers of personal data to the United Kingdom. From the date of Brexit, the United Kingdom will become a "third country," and the adequacy of its protections for personal data will need to be assessed by the EU Commission. However, the notice states that even if an adequacy decision is not granted, data flows need not be unnecessarily interrupted, as other options (such as model clauses, binding corporate rules, and exceptions such as contractual necessity) will remain available.

The following Jones Day lawyers contributed to this section: Laurent De Muyter, Undine von Diemar, Daniel Echeverria Gonzales, Olivier Haas, Jörg Hladjk, Bastiaan Kout, Matthijs Lagas, Jonathon Little, Martin Lotz, Hatziri Minaudier, Selma Olthof, Audrey Paquet, Elizabeth Robertson, Lucia Stoican, and Rhys Thomas.

[Return to Top]

Asia

Hong Kong

PCPD Issues Guiding Principles for Small and Medium Enterprises
In December 2017, the Privacy Commissioner for Personal Data ("PCPD") issued guidance titled *Data Protection & Business Facilitation—Guiding Principles for Small and Medium Enterprises* ("Guiding Principles") to assist small and medium enterprises. The Guiding Principles cover a number of areas, including: (i) collecting customers' personal data; (ii) use of customers' personal data; (iii) safeguarding customers' personal data; (iv) operating online businesses or services; (v) operating businesses outside Hong Kong; (vi) marketing of products or services; (vii) recruitment; (viii) installing CCTV for security purpose; (ix) collecting employees' personal data for monitoring; (x) outsourcing the processing of personal data; and (xi) handling data access and data correction requests.

PCPD Reiterates Privacy Issues Relating to Drones

On December 4, 2017, PCPD noted the issues of personal data privacy arising from the use of drones. PCPD cautioned that the use of drones should comply with the requirements of the Personal Data Privacy Ordinance as well as the Data Protection Principles if collection of personal data is involved.

PCPD Examines Privacy Issues in Industry Reports
On December 18, 2017, PCPD released the 2017 Study Report on User Control over Personal Data in Customer Loyalty and Reward Programs and a study titled Inspection Report: Personal Data System of an Estate Agency in Hong Kong. The Loyalty Programs Report examined 30 customer loyalty and reward programs from various industries and discussed the lack of transparency in such programs. The Estate Agency Report, however, concluded that the Estate Agency made reasonably good efforts to ensure proper management of clients' data.

PCPD Fines Grocery Chain for Direct Marketing Violations
On January 2, PCPD fined a large grocery chain HK$3,000 for using customers' personal data in direct marketing campaigns without obtaining prior consent, in violation of section 35E(1) of the Personal Data Ordinance. In its ruling, the Privacy Commissioner noted that "[a]ppropriate training must be provided to its staff members to ensure their awareness of and compliance with the direct marketing provisions under the Ordinance."

Japan

Personal Information Protection Commission Releases Draft Amendment to Regulations Regarding Adequacy Requirements

On December 7, 2017, the Personal Information Protection Commission released a draft amendment to the Enforcement Regulation of Personal Information Protection Act (source document in Japanese) for public comments. The amendment sets forth adequacy requirements for a foreign country in order to allow the cross-border transfer of personal data outside Japan without the data subjects' advance consent. The public comment period closed on January 5, 2018.

People's Republic of China

Domain Name Authentication Rules Take Effect
On January 1, the Ministry of Industry and Information Technology's Notice (source document in Chinese) on the use of domain names by internet information services took effect. The Notice requires domain name registration authorities and domain name registration service agencies to authenticate the identity information of domain names before providing related services. Internet access providers are also required to authenticate the identity information of internet service providers and domain name registrants before providing services to internet service providers.

China Releases Final Personal Information Protection Standard
On January 2, the National Information Security Standardization Technical Committee released the final version of the "GB/T 35273-2017 Information Security Technology—Personal Information Security Specification" (source document in Chinese). The Personal Information Security Specification sets out best practices for enforcing China's data protection rules and applies to "personal data controllers" and those with the right to decide the purpose and method of processing personal information. The Personal Information Security Specification also protects "personal sensitive information," defined as information that may lead to bodily harm, property damage, reputational damage, harm to personal heath, or discriminative treatment if such data is disclosed, unlawfully provided, or abused. The law will take effect on May 1.

Singapore

PDPC Publishes Anonymization Guide
On January 25, the Personal Data Protection Commission issued a new anonymization guide. The guide "gives a general introduction to the technical aspects of anonymization" and "provides information and examples on the concepts and techniques that could be applied to anonymizing personal data."

TThe following Jones Day lawyers contributed to this section: Michiru Takahashi, Sharon Yiu, and Grace Zhang.

[Return to Top]

Australia

Eligible Data Breach Scheme Resources Available
On December 15, 2017, the Commissioner finalized the online resources for the eligible data breach ("EDB") scheme. The resources cover which entities must comply with the EDB scheme, how to identify an EDB, exceptions to notification obligations, how to notify affected individuals and the Commissioner of an EDB, and the role of the Commissioner in the EDB scheme.

Data Breach Notification Amendment Takes Effect

On February 22, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) ("Amendment Act") came into effect. Under the Amendment Act, entities regulated by the *Privacy Act 1988* (Cth) must notify the Office of the Australian Information Commissioner and affected individuals if there has been an EDB. The Amendment discusses two types of EDBs: (i) when there has been unauthorized disclosure or access to personal information that would likely result in harm; and (ii) when unauthorized disclosure or access to personal information is likely to occur and would result in harm.

The following Jones Day lawyers contributed to this section: Adam Salter and Katharine Booth.

[Return to Top]