JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 20 | December 2018 JONES DAY

GLOBAL PRIVACY & CYBERSECURITY UPDATE

Jones Day Cybersecurity, Privacy & Data Protection Attorney Spotlight: Elizabeth Cole

Data privacy and cybersecurity are becoming increasing areas of focus in Asia, with divergent approaches from market-driven regulation to protectionist laws that restrict the transfers of both personal and other commercial data. Notable developments in 2018 include the passing of cybersecurity laws in Singapore and Vietnam; the publication of proposed data protection laws in India, Indonesia, and Thailand; and the introduction of the Personal Information Protection Standard in China.

Elizabeth Cole is a partner based in Singapore and Shanghai whose practice encompasses data privacy and cybersecurity issues in Southeast Asia and China. Elizabeth has practiced in Australia, China, Hong Kong, Indonesia, and Singapore for more than 25 years and has represented clients throughout the Asia-Pacific region, including advising and assisting on cybersecurity, personal data privacy issues, and data breach notification obligations.

Elizabeth regularly assists clients in navigating data privacy and cybersecurity laws in the region relating to cross-border mergers and acquisitions, corporate reorganizations, joint ventures, outsourcing of services, and investigations. Elizabeth is also presently assisting a number of clients on compliance with uncertain data localization and cross-border transfer restrictions under China's Cybersecurity Law as they apply to the ongoing operation of their businesses.

United States

PRACTICE DIRECTORY

Daniel J. McLoon, Los Angeles
Mauricio F. Paez, New York
Jay Johnson, Dallas
Jonathon Little, London
Elizabeth A. Robertson, London
Todd S. McClelland, Atlanta
Jeff Rabkin, San Francisco
Lisa M. Ropple, Boston
Adam Salter, Sydney
Michiru Takahashi, Tokyo
Undine von Diemar, Munich
Richard M. Martinez, Minneapolis
Samir C. Jain, Washington
John A. Vogt, Irvine
Edward S. Chang, Irvine
Aaron D. Charfoos, Chicago
Elizabeth Cole, Singapore
Chiang Ling Li, Hong Kong
Richard DeNatale, San Francisco
Olivier Haas, Paris
Jörg Hladjk, Brussels
Guillermo E. Larrea, Mexico City
Todd Kennard, Columbus
Jimmy Kitchen, Pittsburgh
Ryan M. DiSantis, Boston

Editor-in-Chief: Kerianne N. Tobitsch
Partner Lead: Jay Johnson

HOT TOPICS IN THIS ISSUE

Regulatory—Policy, Best Practices, and Standards

NIST Releases Internal Report Regarding IoT Cybersecurity
In September, the National Institute of Standards and Technology ("NIST") released a draft internal report called "Considerations for Managing Internet of Things ("IoT") Cybersecurity and Privacy Risks." The report addresses differences in managing cybersecurity and privacy risks for conventional information technology versus the IoT.

Regulatory—Consumer and Retail

Children's Consumer Protection Watchdog Asks FTC to Investigate Manipulative Preschool Apps
On October 30, the Campaign for a Commercial-Free Childhood ("CCFC") asked the Federal Trade Commission ("FTC") to investigate the market for preschool apps. The CCFC cited a new University of Michigan study that found "a number of troubling advertising practices, including apps that force kids to watch ads or make in-app purchases in order to advance in the game," as well as advertisements disguised as gameplay, and cartoon characters urging children to make purchases.

Retailer Announces Breach of Employee Data
On November 5, a retailer notified employees that some of their personal data may have been compromised in an internal data breach. The company stated that it was investigating an October 9 incident in which a contract worker improperly handled some employee data. Compromised data may have included employees' names, Social Security numbers, payment card numbers, checking and routing account numbers, insurance provider information, salary information, dates of birth, addresses, and phone numbers.

Regulatory—Financial

SEC Orders Cease-and-Desist Proceedings Against Investment Adviser
On September 26, the Securities and Exchange Commission ("SEC") ordered public administrative and cease-and-desist proceedings against a registered broker-dealer and investment adviser for deficient cybersecurity practices. The SEC found that the company violated the Safeguards Rule by failing to adopt written policies and procedures reasonably designed to protect customer records and information. The SEC also found that the company violated the Identity Theft Red Flags Rules by failing to develop and implement a written identity theft prevention program. The SEC imposed a $1 million civil monetary penalty on the company.

SEC Report Recommends Improvements to Internal Accounting Controls to Combat Cyber Fraud
On October 16, the SEC published an investigative report examining the efficacy of internal accounting controls for

Argentinian Agency Sends Personal Data Privacy Bill to Congress

European Commission Publishes Report on Second Annual Review of Functioning of EU-U.S. Privacy Shield

Chinese Ministry Releases Regulation Regarding Cybersecurity Inspections

RECENT AND UPCOMING SPEAKING ENGAGEMENTS

Current Developments in Global Data Privacy and Security, Ethics & Compliance Certificate Program, SMU Dedman School of Law, Dallas, Texas (February 2019). **Jones Day Speaker:** Jay Johnson

Data Privacy—A Discussion of Law and Policy, Federalist Society, Notre Dame Law School, South Bend, Indiana (February 2019). **Jones Day Speaker:** Jay Johnson

Handling a Cybersecurity Investigation: An Interactive Tabletop Exercise Led by a Regulator, a Lawyer, and a Security Expert, Utilities & Energy Compliance & Ethics Conference, SCCE, Houston, Texas (February 2019). **Jones Day Speaker:** Jay Johnson

Privacy by Design and Privacy by Default—on the Ground, IAPP Data Protection Intensive France 2019, Paris, France (February 2019). **Jones Day Speaker:** Olivier Haas

Threat & Vulnerability Management, CISO Executive Network, Dallas, Texas (January 2019). **Jones Day Speaker:** Jay Johnson

Blockchain Technology, Security, and Privacy, ABA Science and Technology Section, Webinar (January 2019). **Jones Day Speaker:** Jay Johnson

2018 Privacy & Data Security Recap, Association of Corporate Counsel, Minneapolis, Minnesota (December 2018). **Jones Day Speaker**: Rick Martinez

International Data Breach Notification: How to Get it Right,

nine public companies that lost millions of dollars as a result of cyber-related fraud. Though public companies are required to implement internal accounting controls designed to safeguard against cyber-related fraud, as required by Section 13(b)(2)(B) of the Securities Exchange Act of 1934, the SEC found that the fraudulent schemes "were not sophisticated in design or the use of technology." The SEC recommended that public companies reassess and calibrate their internal accounting controls to the current cybersecurity risk environment.

Bank Announces Data Breach Affecting Some Online Customer Accounts

On November 2, a bank notified customers of unauthorized access to online customer accounts between October 4 and October 14. The bank disclosed that the incident may have exposed customers' full names, dates of birth, email addresses, phone numbers, bank account numbers, balance information, and statement histories. The bank suspended online access to these customers' accounts and offered a subscription to credit monitoring services for affected customers.

Regulatory—Energy/Utilities

Seven Russian Agents Face Charges for Hacking U.S. Nuclear Power Company

On October 4, the U.S. Department of Justice announced an indictment against seven Russian intelligence agents accused of hacking a U.S. nuclear power company that designed nuclear plants and sold nuclear fuel to Ukraine. According to the indictment, the hackers surveyed the company's networks and personnel, created a fake company domain, and sent spear-phishing emails to the work and personal email accounts of the company's employees in an attempt to collect log-in credentials.

Intelligence Report Details Foreign Economic Cyber Threats Against U.S. Industries

In November, the National Counterintelligence and Security Center released its 2018 Report on Foreign Economic Espionage in Cyberspace. The report described the threat of cyber-economic espionage against U.S. industries by foreign nation-state actors that exploit vulnerabilities in next-generation technologies such as artificial intelligence, the IoT, and cloud computing. The report identified the energy, biotechnology, and defense technology industries as among the sectors of highest interest to foreign actors. The report also highlighted emerging cyber threats to U.S. industries, including potential infiltration of supply chain operations.

Regulatory—Transportation

FTC Settles With Ride-Sharing Service for Failure to Disclose Data Breach

On October 26, the FTC gave final approval to a settlement agreement with a ride-sharing service. The FTC alleged that the company had deceived consumers

Roundtable Topic Discussion, IAPP Europe Data Protection Congress 2018, Brussels, Belgium (November 2018). **Jones Day Speaker**: Jörg Hladjk

The EU General Data Protection Regulation, Lecture at the Jones Day Course at Beijing University, Beijing, China (November 2018). **Jones Day Speaker:** Undine von Diemar

GDPR Training for members of China National Enterprise Compliance Committee (CNECC), Beijing, China (November 2018). **Jones Day Speaker:** Undine von Diemar

The Relevance and Context of GDPR for Players, FIFPro (International Federation of Professional Footballers)—Division Europe, General Assembly, Rome, Italy (November 2018). **Jones Day Speaker**: Jörg Hladjk

New Enforcement Powers: What DPAs Can Learn From Competition Law Practice, IAPP Europe Data Protection Congress, Brussels, Belgium (November 2018). **Jones Day Speaker:** Laurent De Muyter

Privacy and Security for Lawyers: Legal and Ethical Guidelines for Managing Evolving Risks, Houston Association of Women Lawyers, Houston, Texas (November 2018). **Jones Day Speaker:** Nicole Perry

Identity and Access Management, CISO Executive Network, Washington, D.C. (November 2018). **Jones Day Speaker:** Jennifer Everett

Identity and Access Management, CISO Executive Network, Dallas, Texas (November 2018). **Jones Day Speaker:** Jay Johnson

Recent California Privacy Regulations, CISO Executive Network, Houston, Texas (November 2018). **Jones Day Speaker:** Nicole Perry

Pizza & Privacy, American Constitution Society, SMU Dedman School of Law, Dallas, Texas

about its privacy and data security practices, such as failing to take reasonable measures to secure consumer data stored in the cloud, resulting in two data breaches. The FTC's Decision and Order requires the company to maintain a comprehensive privacy program, obtain privacy assessments by a third party, report any future data security incidents to the FTC, and submit a compliance report to the FTC.

FCC Commissioner Discusses Development of Smart Cities

On October 30, Michael O'Rielly, a commissioner of the U.S. Federal Communications Commission ("FCC"), made remarks on technological advancements needed to build smart cities, including fiber, spectrum, and the IoT. The commissioner also highlighted data privacy concerns associated with the collection, use, and analysis of individuals' data in a smart city.

Regulatory—Health Care/HIPAA

Health Insurer Agrees to Largest Settlement of a Health Data Breach

On October 15, the U.S. Department of Health and Human Services Office for Civil Rights ("OCR") announced that a health insurance company agreed to pay $16 million and implement a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act ("HIPAA") related to a data breach. The company discovered the breach in January 2015 that may have exposed the electronic protected health information of almost 79 million people between December 2, 2014, and January 27, 2015. The settlement represents the largest settlement paid to OCR, more than doubling the previous highest amount of $5.55 million in 2016.

Regulatory—Defense and National Security

Department of Defense Releases Cyber Strategy

On September 18, the Department of Defense ("DoD") released the "2018 Department of Defense Cyber Strategy," which supersedes the 2015 DoD Cyber Strategy. The Strategy focuses on securing sensitive information and accelerating cyber capabilities for countering malicious cyber actors. The DoD plans to build partnerships with private-sector entities to support the Department's cybersecurity activities and reduce malicious cyber activity targeting critical infrastructure.

White House Releases National Cyber Strategy

On September 20, the White House released the "National Cyber Strategy of the United States of America," which outlined how the Administration would protect networks, promote digital economic and domestic innovation, deter malicious cyber activity, and promote an open and secure internet abroad. The Strategy also focuses on ensuring that federal agencies have the necessary legal authorities and resources to combat malicious, transnational

(November 2018). **Jones Day Speaker:** Jay Johnson

Data Protection and Open Banking: Experiences and Expectations, Brussels, Belgium (October 2018). **Jones Day Speaker**: Jörg Hladjk

GDPR and Latin America at the 33rd Annual Financial Cybersecurity Conference, Miami, Florida (October 2018). **Jones Day Speakers:** Rick Martinez and Jennifer Everett

Cybersecurity and the Impact on SEC Filings and Compliance, Dallas Bar Association Securities Law Section, Dallas, Texas (October 2018). **Jones Day Speaker**: Jay Johnson

General Data Protection Regulation "GDPR": Seeking or Supplying Information to or from the EU or EEA After May 25, 2018. Eastern District of Texas 2018 Bench Bar Conference, Plano, Texas (October 2018). **Jones Day Speaker**: Jay Johnson

Data-Centric Security, CISO Executive Network, Dallas, Texas (October 2018). **Jones Day Speaker:** Jay Johnson

Data-Centric Security, CISO Executive Network, Houston, Texas (October 2018). **Jones Day Speaker:** Nicole Perry

Privacy Law, Guest Lecturer at Internet Law Class, University of Houston Law Center, Houston, Texas (October 2018). **Jones Day Speaker:** Nicole Perry

RECENT AND UPCOMING PUBLICATIONS

General Data Protection Regulation, statutory commentary on profiling, security, and data breach notification, Ehmann/Selmayr, Beck Verlag, second edition 2018 (in German, English translation available soon). **Jones Day Author**: Jörg Hladjk

EU GDPR, statutory commentary on international data transfers, including

cybersecurity activity.

Litigation, Judicial Rulings, and Agency Enforcement Actions

New Mexico Attorney General Sues Technology Companies Over Children's Privacy Concerns
On September 12, New Mexico Attorney General Hector Balderas filed a complaint in the District of New Mexico against technology companies and application developers for alleging designing and marketing applications that illegally track children in violation of the Children's Online Privacy Protection Act. The complaint focuses on online game applications that access the geolocation, demographics, and online activities of children without the knowledge and consent of parents for the purpose of targeted advertising.

Attorneys General Reach $148 Million Settlement with Ride-Sharing Company Over Delay in Data Breach Notification
On September 26, attorneys general from all 50 states and the District of Columbia announced a $148 million settlement with a ride-sharing company to address the company's one-year delay in reporting a data breach. The company learned in November 2016 that hackers had gained access to some personal information of about 57 million riders and drivers, including drivers' license information of approximately 600,000 drivers nationwide, but the company did not notify the affected individuals pursuant to state laws until November 2017. The settlement also requires the company to implement certain data security safeguards, incorporate privacy-by-design into its products, and hire a third-party company to audit its data security practices.

Technology Company Strikes $50 Million Settlement in Data Breach Litigation
On October 22, an email service provider agreed to pay $50 million to settle a class action in the Northern District of California related to a trio of data breaches involving unauthorized access to usernames, passwords, and other private data of up to three billion email user accounts worldwide. The settlement still needs to be approved by the district court. The settlement would require the company to establish a $50 million non-reversionary settlement fund and provide at least two years of credit monitoring and identity theft-protection services for all settlement class members.

EU model contracts and Binding Corporate Rules, Auernhammer, Heymann Verlag, second edition 2018 (in German). **Jones Day Author:** Jörg Hladjk

Out of State, Out of Luck: Federal Court Rejects Nationwide TCPA Class Action Claims (November 2018). **Jones Day Authors:** Bill Dolan, Todd Kennard, Brandy Hutton Ranjan

Driverless, Networked Vehicles on the Rise, French Liability Regulations Lag Behind (November 2018). **Jones Day Authors:** Ozan Akyurek, Sophie Hagège, Françoise Labrousse, Olivier Haas

Blockchain for Business (November 2018). **Jones Day Authors:** Various

GDPR's Potential Fines and Other Exposures Raise Cyber Insurance Coverage Questions (November 2018). **Jones Day Authors:** Various

Is Your Insurance Program Ready for California's New Data Privacy Law? (October 2018). **Jones Day Authors:** Rich DeNatale, Ty Childress

California to Regulate Security of IoT Devices (October 2018). **Jones Day Authors:** Todd McClelland, Rick Martinez, Jeff Rabkin, Fran Forte

Italian Data Protection Decree Harmonizes National Law with GDPR Provisions (October 2018). **Jones Day Authors:** Sara Rizzon, Undine von Diemar, Jörg Hladjk

Ohio Adopts Safe Harbor for Businesses Involved in Data Breach (October 2018). **Jones Day Authors:** Adam Hollingsworth, Todd Kennard, Vanessa Healy, Brandy Hutton Ranjan

Ride-Sharing Company Reaches $4 Million Settlement of TCPA Class Action
On November 6, a proposed consumer class requested that the U.S. District Court for the Western District of Washington preliminarily approve its proposed $3.99 million settlement with a ride-sharing company. The class alleges that the company used an automatic telephone dialing system to send unsolicited commercial texts to individuals in violation of the Telephone Consumer Protection Act ("TCPA"). The settlement class includes all Washington residents who, between June 1, 2012, and the date of preliminary

approval, received one or more invitational text messages through the company's "Invite A Friend" program.

Supreme Court to Weigh in on FCC's Interpretation of "Advertisement" Under TCPA
On November 13, the U.S. Supreme Court announced that it would determine whether the Hobbs Act required a district court to accept the FCC's legal interpretation of the TCPA. The FCC maintained that an unsolicited fax sent by a major health information provider regarding offers for a free e-book must have had a commercial goal to be an advertisement under the TCPA. The Supreme Court will consider the standard that lower courts must use to determine "when" and to "what extent" to defer to FCC guidance.

Consumer Reporting Agency Agrees to $22 Million Settlement of Data Breach Class Action
On December 3, a federal court in the Central District of California granted plaintiffs' request for preliminary approval of a proposed $22 million settlement of class action claims against a consumer reporting agency related to a data breach that affected 15 million individuals in the United States. The breach involved unauthorized access to individuals' names, addresses, dates of births, Social Security numbers, and driver's license numbers. The settlement funds will be used to provide two years of credit monitoring services to class members and cash payments for out-of-pocket costs.

Legislative—Federal

Cybersecurity and Infrastructure Security Agency Act of 2018 Becomes Law
On November 16, the Cybersecurity and Infrastructure Security Agency Act of 2018 was signed into law. The law rebrands the Department of Homeland Security's main cybersecurity unit, the National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency ("CISA"). The law gives CISA the responsibility to protect the United States' critical infrastructure from physical and cyber threats and to coordinate with government and private-sector organizations to do so. It establishes three divisions in the new agency: Cybersecurity, Infrastructure Security, and Emergency Communications.

Legislative—States

California Enacts Legislation Regulating Security of IoT
On September 28, California Governor Jerry Brown signed legislation making California the first state to expressly regulate the security of connective devices, commonly referred to as IoT devices. The new law aims to protect the security of both IoT devices and any information contained on IoT devices. The law requires a manufacturer that sells or offers to sell a connected device in California to equip the device with reasonable security features. The new law goes into effect on January 1, 2020. For more information, please see our *Commentary*.

Ohio Amends Data Breach Notification Law
On November 2, Ohio's amended data breach notification law went into effect. The amended law provides companies with a "safe harbor" against tort actions brought under Ohio law alleging a lack of reasonable information security controls. To qualify for the safe harbor, companies must adopt reasonable cybersecurity measures and ensure that the company's cybersecurity measures "reasonably conform" to certain industry-recognized frameworks. Companies also must tailor the scope of their cybersecurity program to the company's size, complexity, and nature of the company's activities, among other requirements.

Canada

Canada Launches New Canadian Centre for Cyber Security
On October 1, Canada announced the launch of its new Canadian Centre for Cyber Security. The Centre was created in response to Canada's 2016 Cyber Review, which identified a need for more "focused federal management on cyber security." The Centre's mandate is to "make Canada more resilient to cyber incidents and build a stronger cyber security community" within Canada.

Canada's Mandatory Data Breach Notification Law Goes into Effect
On November 1, Canada's Breach of Security Safeguards Regulations went into effect, implementing the Personal Information Protection and Electronic Documents Act, known as "PIPEDA." The regulations provide the requirements for mandatory data breach notification to affected individuals and the Office of the Privacy Commissioner if a breach poses a real risk of significant harm to individuals. Companies also

must maintain a record of every security incident for 24 months. Companies are subject to potential penalties of CAD$100,000 for failure to make notifications or maintain records.

The following Jones Day lawyers contributed to this section: Jeremy Close, Meredith Collier, David Coogan, Jennifer Everett, Levent Hergüner, Jay Johnson, Laura Lim, Christopher Markham, Dan McLoon, Mary Alexander Myers, Kaeley Brown, Mauricio Paez, and Nicole Perry.

[Return to Top]

Latin America

Argentina

Argentinian Agency Sends Personal Data Privacy Bill to Congress

On September 19, the Access to Public Information Agency (*Agencia de Acceso a la Información Pública*) submitted to Congress a bill to update Argentina's personal data privacy legislation (source document in Spanish). The bill proposed restrictions on the use of personal data and additional mechanisms for companies to safeguard sensitive material, including appointment of a data protection officer and expanded individual rights.

Brazil

Brazil Observes Council of Europe's Convention 108 Meeting

On October 18, the Council of Europe announced that Brazil joined the Committee of Convention 108 as an observer. Convention 108 requires signatories to take the necessary steps in their domestic legislation to implement the data protection principles of the Convention. Observers are countries that have not yet become members of the Convention.

Chile

Chilean Congress Proposes New Computer Crimes Law

On October 25, the Ministry of the Interior and Public Security (*Ministerio del Interior y Seguridad Publica*) announced that it referred a new Computer Crimes bill to the National Congress (source document in Spanish). The Computer Crimes bill, part of Chile's National Cybersecurity Strategy, would replace the current regulation promulgated in 1993. The bill proposed to create several types of cybercrimes, including unauthorized access, disruption, or damage to a computer, and improve government coordination and response to cyber incidents.

Chile's Financial Stability Central Bank Warns of Cybersecurity Risks

On November 15, Chile's Central Bank (*Banco Central de Chile*) issued the Financial Stability Report corresponding to the second semester of 2018, which warned about the cybersecurity risks to private financial institutions and the importance of maintaining adequate security systems to prevent data breaches, critical disruptions, and information loss in Chile's financial system (source document in Spanish). No systemic cybersecurity attacks have occurred, although there were some reports of temporary interruptions to bank operations because of attacks on digital platforms.

Colombia

Colombian Superintendence Joins OECD's Global Consumer Awareness Campaign

On November 13, the Superintendence of Industry and Commerce (*Superintendencia de Industria y Comercio*) announced its collaboration with the global consumer awareness campaign on product safety organized by the Organization for Economic Co-operation and Development ("OECD") and the European Commission to raise awareness about the risks involved in the free movement of unsafe products over the internet (source document in Spanish).

Costa Rica

Costa Rica Hosts the Ibero-American Meeting of Data Protection

On September 25, the Data Protection Agency (*Agencia de Protección de Datos de los Habitantes*)

announced that Costa Rica will host the sixth edition of the Ibero-American Data Protection Meeting (source document in Spanish). The purpose of the meeting is to address best practices on data protection issues, identify data protection risks, and address changes to data protection laws at a global level.

Mexico

Convention 108 and its Additional Protocol Enters into Force in Mexico
On October 1, the National Institute of Transparency, Access to Information and Protection of Personal Data (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* or "INAI") announced that Convention 108 of the Council of Europe and its Additional Protocol governing cross-border data flows went into effect in Mexico (source document in Spanish). The Convention requires signatories to take the necessary steps in their domestic legislation to apply the data protection principles of the Convention. The INAI announced that complying with the principles of the Convention would strengthen Mexico's business relations with other signatory countries and establish rules to facilitate data transfers.

Panama

Panamanian Congress Passes Bill to Protect Personal Data
On October 24, the Panamanian Congress (*Asamblea Nacional de Panamá*) passed bill No. 665 to safeguard and guarantee citizens' constitutional right to the protection of personal data (source document in Spanish). The bill appoints the Data Transparency and Access to Information Authority (*Autoridad Nacional de Transparencia y Acceso a la Información*) as the governmental agency with authority to protect personal data in connection with information and communication technologies.

Uruguay

Data Control Unit Issues Guidelines on Data Protection
On October 29, the Regulatory and Personal Data Control Unit (*Unidad Reguladora y de Control de Datos Personales*) announced the authorization of new guidelines on data protection issues (source document in Spanish). The guidelines provide recommendations for protecting personal data in three areas: (i) use of online cookies; (ii) implementation of Bring Your Own Device policies; and (iii) operation of drones.

The following Jones Day lawyers contributed to this section: Guillermo Larrea, Daniel D'Agostini, and Juan Carlos Quinzaños.

[Return to Top]

Europe

European Court of Justice

European Court of Justice Conducts Hearing on Privacy Case Referred by French Court
On September 11, the Court of Justice of the European Union ("CJEU") conducted a hearing to obtain evidence for a case brought by the French Data Protection Authority ("CNIL") in August 2017 against a U.S. technology company involving the right to be forgotten (source document in French). The CJEU obtained evidence from the technology company, the CNIL, a number of EU countries representatives, and other privacy advocates. The CJEU will have to decide whether the right to be forgotten should apply to all of the domain names used by a search engine worldwide, regardless of the place from where the search was initiated, or whether this right should apply only to searches initiated on domain names associated with the EU Member States where the search was initiated. The CJEU's decision is expected sometime next year.

European Court of Justice Rules on Access to Personal Data in Context of Criminal Investigation
On October 2, the CJEU adopted a judgment in Case C–207/16 confirming the conditions for public authorities to access personal data retained by providers of electronic communications services to conduct criminal investigations. The CJEU stated that the access by public authorities to identification data (such as first name, last name, or address) of the holder of a SIM card activated for a stolen mobile telephone is not a "serious interference" with the fundamental rights of the persons whose data is concerned. The CJEU

stated that such access is justified by the need to prevent, investigate, detect, and prosecute criminal offenses, even if those offenses are not defined as "serious."

European Parliament

Members of European Parliament Issue Resolution Calling for Investigation of Social Media Company

On October 25, members of the European Parliament announced a resolution urging a social media company to allow EU bodies to carry out a full audit to assess data protection and the security of users' personal data. This announcement arises out of alleged misuse of users' personal data on the social media platform by a third party. The members suggested that EU Member States conduct investigations in conjunction with the European Union's Judicial Cooperation Unit, known as Eurojust, whose mission is to promote and strengthen coordination and cooperation among national authorities to combat serious cross-border crime. The members also called for EU Member States to consider implementing rules to prevent political and electoral interference via social media.

European Commission

European Commission Publishes Report on Second Annual Review of Functioning of EU-U.S. Privacy Shield

On December 19, the European Commission published its report on the second annual review of the functioning of the EU-U.S. Privacy Shield. The report demonstrates that the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the European Union to self-certified companies in the United States. Since the last report, U.S. authorities have taken significant measures to implement the recommendations made by the European Commission and have therefore improved the functioning of the framework. The European Commission, however, is waiting for U.S. authorities to appoint a permanent Ombudsperson by February 28, 2019. The Ombudsperson is an important mechanism under the Privacy Shield to ensure that complaints by data subjects concerning access to personal data by U.S. authorities are properly addressed.

European Data Protection Board

EDPB Adopts 22 Opinions Listing Common Criteria for DPIAs

On September 25, the European Data Protection Board ("EDPB") adopted 22 Opinions listing the common criteria for the types of processing activities that require a data protection impact assessment ("DPIA"). A DPIA is a process to identify and mitigate data protection risks that could affect the rights and freedoms of individuals. The EDPB received lists from the national data protection authorities of 22 EU Member States regarding the types of operations that are likely to result in a high risk to individuals and may trigger a DPIA.

EDPB Adopts Opinion on Proposed e-Evidence Regulation

On September 25, the EDPB adopted an Opinion on the European Commission's proposed e-Evidence regulation of April 2018. The Board determined that the proposed new rules providing for the collection of electronic evidence should sufficiently safeguard the data protection rights of data subjects and be more consistent with EU data protection law.

EDPB Discusses EU-Japan Draft Adequacy Decision

On November 16, the EDPB met for its fourth plenary session and discussed work on the EU-Japan draft adequacy decision. The EDPB reiterated the importance of guaranteeing the continuity and high level of protection for data transfers from the European Union.

EDPB Adopts Draft Guidelines on Territorial Scope of GDPR

On November 16, the EDPB adopted draft Guidelines on the territorial scope of the GDPR and further clarification on the application of the GDPR in various situations, particularly the designation of a representative where the data controller or processor is established outside of the European Union. The Guidelines will be subject to a public consultation.

European Data Protection Supervisor

EDPS Publishes Opinion on Consumer Legislation

On October 5, the European Data Protection Supervisor ("EDPS") issued an Opinion outlining its position on the legislative package titled "A New Deal for Consumers." The package contains the Proposal for a Directive regarding better enforcement and modernization of EU consumer protection rules. It also contains the Proposal for a Directive on representative actions for the protection of the collective interests of consumers.

EDPS Calls for Closer Alignment Between Consumer Law and Data Protection Rules
On October 8, the EDPS released a statement calling for greater cooperation between regulators of Europe's consumer law and data protection rules to prevent legal uncertainty and develop a "big-picture approach" to addressing systemic harms to individuals in digital markets. In particular, the EDPS noted that it is "problematic" for consumers to pay for the supply of digital content or services with their personal data.

ENISA Publishes Annual Security Incidents Report
On October 8, the European Union Agency for Network and Information Security ("ENISA") published its annual report on security incidents for trust services in 2017. Electronic trust services relate to digital signatures, digital certificates, and other mechanisms used to secure electronic transactions. ENISA is required to publish the annual report pursuant to Article 19 of the Electronic Identification, Authentication and Trust Services ("eIDAS") Regulation. This is ENISA's first full-year report since the eIDAS Regulation went into effect.

ENISA Publishes Good Practices for Security of IoT for Smart Manufacturing
On November 19, ENISA published its study on security for IoT in the context of smart manufacturing. This ENISA study addressed the security and privacy challenges related to the evolution of industrial systems and services precipitated by the introduction of IoT innovations. The study discussed good practices to ensure security of IoT in the context of Industry 4.0/Smart Manufacturing, and mapped the relevant security and privacy challenges, threats, risks, and attack scenarios.

Belgium

Belgium Establishes "Information Security Committee"
On September 10, the official journal published a law establishing the "Information Security Committee" to perform specific tasks regarding processing by public bodies and in the field of social security and health (source documents in French and in Dutch).

Belgium Publishes Law Implementing GDPR
On September 5, the official journal published the Belgian law implementing the GDPR (source documents in French and in Dutch). The Parliament had voted to pass the draft in July. For more information, please see our *Alert*.

Belgian Data Protection Authority Issues Six-Month Post-GDPR Implementation Status
On November 23, the Belgian Data Protection Authority ("DPA") published a status report on GDPR implementation (source documents in French and in Dutch). According to the report, there have been 317 data breach notifications (versus 13 in 2017), 3,599 information requests (versus 2,145 in 2017), 148 complaints/requests (versus 76 in 2017), 137 opinion requests (versus 44 in 2017), and 3,540 notifications of data protection officers. The report also mentions that the first dawn raids took place, although no file has yet been transmitted to the dispute body.

France

CNIL Reports on Effective Implementation of GDPR in France and Europe
On September 25, the French Data Protection Authority ("CNIL") published an article reporting progress on GDPR implementation (source document in French). For instance, 24,500 organizations have appointed a Data Protection Officer, as compared to only 5,000 prior to the GDPR. The article also reported that individuals have become more aware of their right to personal data protection since GDPR entered into force. For example, the number of complaints received by the CNIL has increased by 64 percent since May 25, 2018. Finally, the CNIL declared that new regulatory tools will be adopted soon to further encourage the effective implementation of the GDPR.

CNIL Issues Decision on Data Processing That Requires DPIA

On October 11, the CNIL issued Decision No. 2018-327 adopting a list of several types of data processing operations that require the implementation of a DPIA (source document in French). The list includes, for instance, the processing of health data by medical and social entities for patient care, biometric data of persons who are considered "vulnerable" (such as students, elderly persons, and patients), and personal data for the purpose of regularly monitoring employee activity.

CNIL Adopts New Guidelines Regarding DPIAs

On October 11, the CNIL adopted new guidelines on conducting DPIAs under the GDPR (source document in French). The guidelines supplement the requirements set out in Article 35(1) of the GDPR and the list of nine criteria defining high-risk data processing, adopted on October 4, 2017, by the Working Party 29 ("WP29"). In line with the WP29, the CNIL requires a DPIA for any data processing that meets at least two of the nine criteria. However, the CNIL exempts data controllers from conducting a DPIA if they provide a documented explanation that the processing does not create a "high risk." Where applicable, the explanation must include the opinion of the Data Protection Officer.

CNIL Issues Guidance on Measuring and Aggregating Audience Data

On October 17, the CNIL provided guidance on using devices to measure audiences and track attendance or flows of visitors in public spaces (source document in French). The CNIL explained that such rules do not apply to devices that do not collect personal data. The CNIL provided examples of scenarios for anonymizing and pseudonymizing this data and provided guidance on the need for a DPIA.

CNIL Issues Guidance on DPIAs

On November 6, the CNIL provided further guidance on conducting DPIAs (source document in French). The CNIL mentioned that a DPIA should: (i) precisely describe the data processing; (ii) provide a legal assessment of whether or not such processing is necessary and proportional to the fundamental rights concerned; and (iii) provide an evaluation of the technical risks in terms of data security. The CNIL explained that DPIAs are mandatory when using a type of processing that the CNIL already stated requires a DPIA (*see* CNIL's Decision n° 2018-327 of October 10, 2018) and whenever the processing meets at least two of the nine criteria mentioned under the G29 Guidelines (*see* Decision n° 2018-326 of October 10, 2018).

Cigref Publishes New Report on Cybersecurity

In October, the French Association Cigref, a large network of companies and public administration entities, published its latest report on cybersecurity (source document in French). The report provides private companies and public entities with guidelines and information about the security of their information technologies so that companies can identify, assess, and manage the risks of using those technologies. In its report, Cigref explained that cybersecurity issues should be governed internally by a manager, who would be responsible for raising awareness among other managers within the company on the impact that cyberattacks may have on the company's activity and assets.

Germany

Data Protection Authority Issues First German Fine under GDPR

On November 21, the Data Protection Authority of Baden-Württemberg issued the first fine under the GDPR in Germany against a social media provider for violating data security requirements (source document in German). The company had notified the authority of a data breach after becoming aware that the personal data of 330,000 users, including email addresses and passwords, had been stolen during a hack. The authority determined that the company violated data security obligations under Article 32 of the GDPR, for example by storing the passwords in clear text. The authority imposed a modest fine of €20,000 and took into account mitigating factors such as the company's willingness to cooperate with the authority.

Bavarian Administrative Court Decides Targeted Advertising Case

On September 26, the Bavarian Administrative Court decided that a social media company's custom audience feature for targeted advertising violated applicable data protection law in the absence of consent from social media users (source document in German). The Bavarian Administrative Court confirmed in its decision an order of the Bavarian Data Protection Authority ("BayLDA") prohibiting a Bavarian online shop from using the custom audience feature (source document in German).

Data Protection Authority Increases GDPR Compliance Audits of Bavarian Companies
On November 7, the BayLDA announced that it increased its auditing activities of Bavarian companies (source document in German). The audits focus on the secure operation of online shops, protection against ransomware in medical practices, compliance with the accountability obligations of large corporations and medium-sized companies, and implementation of information obligations in application procedures.

Data Protection Authority Warns of Scam
On October 2, the State Commissioner for Data Protection in Schleswig-Holstein ("ULD") warned companies of a fax sent by a fake authority going by the name "*Datenschutzauskunft-Zentrale*" falsely informing companies of a requirement to fill out a form to comply with data protection legal obligations (source document in German). The ULD stated that the "*Datenschutzauskunft-Zentrale*" is not an official authority.

Data Protection Authority Announces Guide for Website Operators
On October 12, representatives of the BayLDA announced a new book containing a summary of requirements for data protection on websites (source document in German). The document contains guidance and checklists for website operators to comply with the GDPR, as well as the anticipated ePrivacy Regulation.

Italy

Italian DPA Issues Opinion on Consent to Fundraising Text Messages
On November 15, the Italian DPA issued an opinion on the use of donor identification data by nonprofit organizations for the purpose of fundraising campaigns via SMS and telephone calls (source document in Italian). According to the DPA, data subjects who made donations to nonprofit organizations via SMS or phone calls may be informed of the outcome of the fundraising campaigns to which they participated. However, if these nonprofit organizations wish to contact the donors for a new campaign, the entities must obtain the donor's consent, which may be given by sending a text message or by pressing a button on the phone when making the donation.

Italian DPA Identifies Types of Processing Subject to DPIA Requirement
On November 15, the Italian DPA published the list of processing activities that require a DPIA (source document in Italian). The list prepared by the Italian DPA includes large-scale evaluation or scoring activities, automatic processing operations with a significant impact on individuals, systematic processing of biometric data and genetic data, and use of IoT and artificial intelligence technologies. Data controllers are also required to carry out a DPIA when at least two of the criteria set forth in the Working Party 29 Guidelines on DPIA are met or whenever the data controller deems that the specific processing requires a DPIA.

The Netherlands

Dutch DPA Provides Status Update on DPO Audits
On October 5, the Dutch DPA ("DDPA") completed its audit of hospitals and health insurers and determined that all 91 hospitals and 33 health insurers have registered a Data Protection Officer ("DPO") (source document in Dutch). On November 20, the DDPA announced that it is auditing 45 banks and 93 insurers on compliance with requirements to appoint a DPO (source document in Dutch). The first review showed that six banks and nine insurers have not registered a DPO with the DDPA.

DDPA Provides Guidance on Consent Requirements Under PSD2 to Payment Service Providers
On October 18, the DDPA issued notice to payment service providers about requirements for access to consumers' personal data under the second Payment Services Directive (source document in Dutch). One of those requirements is that payment service providers need the explicit consent of consumers before gaining access to personal data. The DDPA clarified that "explicit consent" means: the consent request must be separated from other parts of the agreement (for instance, through a pop-up or a separate checkbox in a dialogue screen), consent must be given freely and be unequivocal, informed, and specific. Consumers must be able to refuse or revoke consent without suffering adverse consequences.

DDPA Penalizes Agency for Insufficient Data Security
On October 30, the DDPA published a decision imposing a penalty on the Employee Insurance Agency

("UWV") (a Dutch quasi-governmental organization) for insufficient security of its web portal (source document in Dutch). The portal is used by employers and labor organizations to log employee absences due to illness. The DDPA determined that the UWV failed to maintain sufficient security measures because multifactor security is needed to secure health data.

Spain

SDPA Recommends Security Measures for Social Media Users
On October 3, the Spanish Data Protection Agency ("SDPA") issued recommendations to social media users in light of a security breach that could have exposed information of 50 million users (source document in Spanish). Although social media companies as data controllers are responsible for the privacy and security of users' personal data, the SDPA stated that users can also play an active role in the protection of their own personal data. The SDPA recommended that users follow basic security measures, such as managing their security settings, closing their sessions when finished with the site, and re-entering their credentials when they seek to access the site again.

Spanish Authorities Offer Recommendations to Promote Safe Online Shopping
On November 19, the SDPA, the General Directorate of Commercial Policy and Competitiveness, and the Directorate General of Consumer Affairs made recommendations to encourage safe online shopping (source document in Spanish). They advised that consumers use official or trusted pages, use robust passwords, avoid the use of public Wi-Fi networks, close sessions after completing purchases, use one credit card exclusively for online payments, and review website privacy policies, among other recommendations. The authorities also advised consumers who purchase connected toys for minors to check the types of data the toy collects, consider who and what the toy will be used for, and assess privacy configuration options.

Spanish Senate Approves New Data Protection Law and Guarantee of Digital Rights
On November 21, the Spanish Senate approved the Organic Law on Data Protection and Guarantee of Digital Rights and published it in the Official Spanish Gazette on December 6 (source document in Spanish). The law is designed to complement the GDPR. It also introduces new privacy rights in a digital environment, including the right to universal access to the internet, right to privacy with use of digital devices in the workplace, and right to privacy from video surveillance at work.

United Kingdom

ICO Fines Companies for Telemarketing Violations
On October 31, the Information Commissioner's Office ("ICO") announced fines of £220,000 against two companies that made 600,000 nuisance calls to individuals who opted out of telemarketing calls by registering with the Telephone Preference Service. The ICO stated that the fines are meant to deter marketing companies from violating consumers' privacy by contacting them without valid consent.

ICO Issues Maximum Fine Against Social Media Company
On October 31, the ICO announced that it issued the maximum fine possible under the Data Protection Act 1998 against a social media company for serious data protection violations. The ICO determined that between 2007 and 2014, the social media company allowed application developers to use personal information without sufficiently clear and informed consent. It also found that the company lacked adequate data security measures, which allowed third parties to harvest the personal information of 87 million individuals worldwide, including one million users in the United Kingdom.

The following Jones Day lawyers contributed to this section: Laurent De Muyter, Undine von Diemar, Olivier Haas, Jörg Hladjk, Bastiaan Kout, Jonathon Little, Martin Lotz, Hatziri Minaudier, Selma Olthof, Audrey Paquet, Sara Rizzon, Irene Robledo, Elizabeth Robertson, and Rhys Thomas.

[Return to Top]

Asia

Hong Kong

Privacy Commissioner Initiates Investigation into Hacking of Social Media Accounts

On September 29, the Privacy Commissioner for Personal Data ("Privacy Commissioner") initiated a compliance review to investigate the hacking of social media user accounts (source document in Chinese). The Privacy Commissioner emphasized that social media platforms should implement effective security measures to protect personal data of users from unauthorized or accidental access, processing, or use of personal data. The Privacy Commissioner suggested steps that social media users can take to protect their personal data, including changing passwords to social media accounts, activating two-factor authentication for account login, and checking privacy settings.

Privacy Commissioner Releases Report Regarding Ethical Processing of Personal Data
On October 24, the Privacy Commissioner released a report on the ethical and fair processing of personal data at the 40th International Conference of Data Protection and Privacy Commissioners held in Brussels, Belgium. In particular, the report addresses the processing of personal data through advanced technologies, such as artificial intelligence and machine learning, and seeks to balance the interests of all stakeholders.

Privacy Commissioner Announces Investigation of Airline Data Breach
On November 9, the Privacy Commissioner announced that it would initiate a compliance investigation of a data breach against an airline carrier pursuant to section 38(b) of the Personal Data Privacy Ordinance ("PDPO"). The Privacy Commissioner previously expressed concern that the breach might have compromised the personal data of local and foreign citizens, including names, dates of birth, passport numbers, Hong Kong Identity Card numbers, and credit card numbers. The Privacy Commissioner will examine the company's security measures to safeguard its customers' personal data and its data retention policies and practices.

Privacy Commissioner Announces Periodic Review of Data Protection Law
On November 14, the Privacy Commissioner issued a statement to inform the public it will review data protection issues as part of its statutory obligation to periodically review the PDPO. The Privacy Commissioner will focus on issues of recent importance, including mandatory breach notification requirements, sanctions for noncompliance, and regulation of data processors.

Japan

Personal Information Protection Commission Issues Guidance to Social Media Company
On October 22, the Personal Information Protection Commission of Japan announced that it provided guidance to a social media company to address the Commission's concerns about recent data breaches (source document in Japanese). The guidance includes a request for the company to report to the Commission regarding notice to data subjects and measures to prevent future breaches, among other requests.

Singapore

PDPC Announces Rule Prohibiting Collection of National Identification Numbers
On November 13, Singapore's Personal Data Protection Commission ("PDPC") announced that organizations are not allowed to collect National Identity Registration Card ("NRIC") numbers or other national identification numbers, unless it is required by law or necessary to verify an individual's identity. This rule goes into effect on September 1, 2019.

PDPC Fines Financial Company for Website Security Vulnerabilities
On December 13, the PDPC imposed a $30,000 penalty on a financial company for failing to make reasonable security arrangements to prevent the unauthorized disclosure of personal data. The website that individuals used to register for an account contained a vulnerability that exposed the personal data of other users, including customer identification numbers, national identification numbers, and bank account numbers.

People's Republic of China

Ministry Releases Regulation Regarding Cybersecurity Inspections
On September 15, China's Ministry of Public Security released the Regulation on the Internet Security Supervision and Inspection by Public Security Organs, which became effective on November 1 (source document in Chinese). The Regulation sets forth detailed procedures describing how Public Security

Bureaus conduct cybersecurity inspections of companies that provide internet services or network-using entities in China. Public Security Bureaus have a wide range of power and discretion to inspect internet service providers, such as physically entering the companies' premises, reviewing and copying materials related to internet security, and inspecting the companies by remote access. Public Security Bureaus may authorize cybersecurity service providers to conduct the inspections.

Cyberspace Administration Releases Draft Regulation on Blockchain Information Services
On October 19, the Cyberspace Administration of China released the draft Regulation on Blockchain Information Services (source document in Chinese). The draft Regulation was available for public consultation until November 2. It would require blockchain service providers to register certain information with the Cyberspace Administration of China, including the types of services provided, scope of application, and server address. Before launching any new products, applications, or functions, the providers must undergo a security assessment with the Cyberspace Administration. The draft Regulation also would require users of blockchain services to provide their ID card number and mobile phone number for identity verification. Providers may refuse blockchain services to users who refuse to disclose their real identity and may restrict or close accounts of users who have violated the Regulation or blockchain services agreement.

Chinese Authorities Release Regulation Governing Internet Information Service Providers
On November 15, the Cyberspace Administration of China and the Public Security Bureau jointly released the Regulation of Security Evaluation for Internet Information Service Providers ("IISP") that impact public opinion or social mobilization (source document in Chinese). The Regulation is designed to supervise and guide IISPs to fulfill the obligation of safety management, maintain online information security and order stability, and prevent the spread of rumors and false information. A new IISP must voluntarily conduct security evaluations before going online.

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

[Return to Top]

Australia

OAIC Examines Privacy Protection Proposals for Digital Platforms
On December 10, the Office of the Australian Information Commissioner ("OAIC") announced that it is examining proposals in a preliminary report issued by the Australian Competition and Consumer Commission ("ACCC") to strengthen privacy protections for individuals on digital platforms. The preliminary report addresses concerns regarding the collection of consumer data and targeted advertising. The OAIC will issue its response to the ACCC's proposals in February.

The following Jones Day lawyers contributed to this section: Adam Salter and Samantha Sisomphou.

[Return to Top]