JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 18 | June 2018

JONES DAY

GLOBAL PRIVACY & CYBERSECURITY UPDATE

Jones Day Cybersecurity, Privacy & Data Protection Attorney Spotlight: Richard Martinez

Europe's new General Data Protection Regulation ("GDPR") is driving an evolution in corporate privacy practices globally. As businesses address GDPR compliance, they also face a growing array of domestic and international laws and regulations that apply to the collection, use, and transfer of information; aggressive regulatory investigations and enforcement efforts; and private litigation over information usage. Rick Martinez, a Minneapolis-based partner in Jones Day's Cybersecurity, Privacy & Data Protection practice, brings over 25 year of experience as a litigator to advising domestic and international clients on cybersecurity, data privacy, information technology, and intellectual property issues.

Rick represents companies in regulatory investigations, enforcement actions, and litigation. He is experienced in all aspects of breach response, forensic investigations, notification obligations, and working with law enforcement. Additionally, Rick has applied his knowledge and experience to assist clients proactively, advising them on enterprise risk mitigation strategies across a variety of technologies and industries, including information technology, outsourcing services, financial services, industrial technologies, IoT, and the strategic protection of intellectual property.

United States

Regulatory—Policy, Best Practices, and Standards

Coalition of 31 Attorneys General Challenge Federal Bill Preempting State Data Breach Laws
On March 19, 2018, a group of 31 state attorneys general formally opposed legislation in Congress that would preempt state data breach and data security laws requiring notice to consumers and state attorneys general of breaches when they occur.

New York Attorney General Releases Report on

EDITORIAL CONTACTS

Daniel J. McLoon
Los Angeles

Mauricio F. Paez
New York

Jay Johnson
Dallas

Jonathon Little
London

Kevin D. Lyles
Columbus

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

2017 New York Data Breaches
On March 29, 2018, the New York attorney general released a report documenting the record number of data breach notices filed with the New York Attorney General's office in 2017. According to the report, companies and other entities reported 1,583 data breaches to the office in 2017 and reported exposing the personal information of 9.2 million New Yorkers. This was quadruple the number of New Yorkers reportedly affected in 2016.

Congress Targets Robocallers Through Legislation and Advocacy
On April 18, 2018, a group of 15 U.S. senators sent a letter to the Federal Communications Commission ("FCC") chairman asking the FCC to enact consumer safeguards against automated calls and texts. Multiple bills related to robocalls are currently pending in Congress, including the Robocall Enforcement Enhancement Act of 2018 in the Senate and the Repeated Objectionable Bothering of Consumers on Phones "ROBOCOP" Act in the House of Representatives.

Regulatory—Critical Infrastructure

NIST Teams with Florida International University for Cybersecurity Education Outreach
On April 4, 2018, the National Institute of Standards and Technology ("NIST") announced a cooperative agreement with Florida International University to help build national relationships that advance outreach in the cybersecurity education, training and workforce development communities. The collaboration will be managed by NIST's National Initiative for Cybersecurity Education Program.

NIST Announces "Unlinkable Data Challenge"
On May 1, 2018, NIST announced the Unlinkable Data Challenge to help the public conduct research using data gathered with personal digital devices and taken from large databases such as driver's license and health care records. Through the contest, NIST aims to identify ways to effectively "de-identify" personal information while maintaining the data's analytic value. The challenge will have three phases, and $190,000 of total prize money will be split among the winners of the phases.

DHS Focuses Cybersecurity Strategy on Energy Sector
On May 15, 2018, the U.S. Department of Homeland Security ("DHS") released its new Cybersecurity Strategy, which provides the Department with a framework to execute over the next five years to keep up with evolving cyber risks. DHS intends to improve national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure.

Regulatory—Consumer and Retail

Clothing Retailers Confirm Data Breach
In April 2018, two major clothing retailers confirmed that hackers breached the stores' points of sale systems to steal the credit card information of more than a million shoppers. The two retailers notified customers that malware began running on point-of-sale systems across North America as early as July 1, 2017. Hackers claim to have stolen five million credit and debit card numbers.

FTC Launches Campaign to Assist Small Business Cyber Defenses
On April 10, 2018, the Federal Trade Commission ("FTC")

Hack

Brazil's National Monetary Council Issues New Rules on Cybersecurity Policies and Data Processing and Storage Requirements

Article 29 Working Party Sets Forth Cooperation Procedure for Approval of Binding Corporate Rules

China Publishes National Standard for Personal Data Protection

Australian Information Commissioner Releases Quarterly Data Breach Report

RECENT AND PENDING SPEAKING ENGAGEMENTS

The National Technology Security Coalition National CISO Policy Conference, Jones Day, Washington, D.C. (July 2018). **Jones Day Speaker**: **Mauricio Paez**

Cybersecurity Regulation and Enforcement, 2018 Essential Cybersecurity Law, The University of Texas School of Law Continuing Legal Education, Houston, TX (July 2018). **Jones Day Speaker: Jay Johnson**

43rd International Legal and GDPR Event: Global Legal ConfEx and Global GDPR ConfEx, New York, NY (June 2018). **Jones Day Speaker: Mauricio Paez**

Building a Cybercrime Prosecution: Law Enforcement and Corporate Perspectives (with DOJ and FBI), Massachusetts Institute of Technology Applied Cybersecurity Professional Education Program Cambridge, Boston, MA (June 2018). **Jones Day Speaker: Lisa Ropple**

Latest Developments in Cybersecurity, Licensing Executives Society International Conference, San Diego, CA (May 2018). **Jones Day Speaker: Aaron Charfoos**

Security Innovation, 2018 Dallas Breakfast Roundtable, CISO Executive Network, Dallas, TX (May 2018). **Jones Day Speaker: Jay Johnson**

Cybersecurity, Not Just an IT Problem Anymore, Masters Conference, Chicago, IL (May 2018). **Jones Day Speaker: Aaron Charfoos**

Homeland and National Security in an Internet-Everything World,

issued a press release outlining a "national education campaign to help small businesses strengthen their cyber defenses and protect sensitive data that they store." The plan follows a Staff Perspective report discussing specific materials and steps available for small businesses to implement robust cybersecurity and data privacy protocols.

Regulatory—Energy/Utilities

House Energy and Commerce Committee Approves Cybersecurity Bills to Secure Energy Infrastructure
On May 9, 2018, the House Energy and Commerce Committee approved legislative measures that help to secure the U.S. energy infrastructure from cyberattacks. The Pipeline and LNG Facility Cybersecurity Preparedness Act, the Enhancing Grid Security through Public-Private Partnerships Act, the Cyber Sense Act of 2018, and the Energy Emergency Leadership Act are all bipartisan and will soon go to the House for a vote.

Regulatory—Financial

IRS Announces Cybersecurity to be Key Topic at 2018 IRS Nationwide Tax Forums
On April 26, 2018, the Internal Revenue Service ("IRS") announced that this year's Nationwide Tax Forums will focus on cybersecurity and the risks that cybercriminals pose to tax professionals. The forums will discuss how to craft effective security plans and developments in cybersecurity.

Regulatory—Health Care/HIPAA

Audit Reveals Military Electronic Health Records Compromise
On May 2, 2018, a Department of Defense Inspector General audit of the medical record security systems at the Defense Health Agency ("DHA"), Navy, and Air Force revealed that "[o]fficials from the DHA, Navy, and Air Force did not consistently implement security protocols to protect systems that stored, processed, and transmitted [electronic health records] EHRs and [patient health information] PHI at the locations tested." The audit included several recommendations for the respective agencies to implement, including: (i) configuring systems that process patient health information to lock after 15 minutes of inactivity; (ii) implementing higher standards for password length and complexity; and (iii) developing plans and milestones to mitigate known network vulnerabilities.

HHS to Consider Rule Providing Portion of Civil Penalty to Individuals Harmed by HIPAA Offense
In spring 2018, the Department of Health and Human Services ("HHS") issued an advanced notice of proposed rulemaking titled "HIPAA Enforcement: Distribution of a Percentage of Civil Money Penalties or Monetary Settlements to Harmed Individuals." HHS seeks the "public's views on establishing a methodology under which an individual who is harmed by an offense punishable under HIPAA may receive a percentage of any civil money penalty or monetary settlement collected with respect to the offense."

Regulatory—Defense and National Security

Department of Defense Reveals Types of U.S. Technology Most Targeted by Foreign Intelligence

American Bar Association Internet of Things National Institute, Washington, D.C. (May 2018). **Jones Day Speaker: Rick Martinez**

Devil in the Details: Crafting an Effective Incident Response Plan, Boston Bar Association Privacy & Cybersecurity Conference, Boston, MA (May 2018). **Jones Day Speaker: Lisa Ropple**

Data Protection–GDPR: Hot Topics for the Life Science Industry and Data Risks in China, Jones Day Life Science Seminar, Tokyo, Japan (May 2018). **Jones Day Speakers: Michiru Takahashi, Undine von Diemar, Jerry Ling**

The Life Sciences Industry Meets the Internet of Things & eHealth, Jones Day Life Science Seminar, Tokyo, Japan (May 2018). **Jones Day Speaker: Undine von Diemar**

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:**

in 2017
In April 2018, the Defense Security Service ("DSS") released a summary of the types of U.S. technology most targeted by foreign intelligence agencies in 2017. The most commonly targeted categories include: (i) aeronautic systems; (ii) command, control, communication, and computers; (iii) electronics; (iv) radars; (v) armament and survivability; (vi) optics; and (vii) software. The summary will be followed by DSS's annual "Targeting U.S. Technologies" report, to be published in September 2018.

Department of Defense to Create Joint Artificial Intelligence Center
On April 13, 2018, the Undersecretary of Defense for Research and Engineering stated that the Department of Defense planned to create a "joint artificial intelligence center." The undersecretary described the center as "crosscutting across services in the intelligence community" and explained that he would report to Congress in mid-summer on details such as how the center would be created, where it would be located, and who would be in charge.

DHS, FBI, and United Kingdom's National Cyber Security Centre Issue Joint Technical Alert Regarding Russia's Cyber Exploitation of Network Infrastructure Devices
On April 16, 2018, the Department of Homeland Security ("DHS"), the Federal Bureau of Investigation ("FBI"), and the United Kingdom's National Cyber Security Centre issued a joint Technical Alert providing "information on the worldwide cyber exploitation of network infrastructure devices (e.g., router, switch, firewall, Network-based Intrusion Detection System (NIDS) devices) by Russian state-sponsored cyber actors." According to the Alert, this campaign to exploit network devices threatens national safety, security, and economic well-being, and the primary targets are government and private-sector organizations, critical infrastructure providers, and the internet service providers supporting those sectors.

Litigation, Judicial Rulings, and Agency Enforcement Actions

Pennsylvania Attorney General Sues Transportation Services Company Over Data Breach
On March 5, 2018, the Pennsylvania attorney general announced a lawsuit against a rideshare company alleging that it violated Pennsylvania's data breach notification law by not timely disclosing a data breach to 13,500 affected Pennsylvania residents.

District Court Permits Putative Privacy Class Action against Rent-to-Own Retailer
On March 7, 2018, a Pennsylvania federal court allowed a putative class action against a rent-to-own retailer to move forward. A Wyoming couple alleged that the retailer installed spyware on its rented laptops that captured personal identifiable information as well as conversations and computer screenshots. The district court judge recognized that the couple may have a valid claim under an invasion of privacy tort theory.

Texas Federal Court Applying *Spokeo* Finds Plaintiff Failed to Show Injury-in-Fact
On March 30, 2018, a Texas federal court found that, pursuant to the standard laid out in the Supreme Court's *Spokeo* decision, a plaintiff patron of a restaurant did not have standing to bring a claim against the restaurant operator for printing too many digits of his debit card on receipts. The plaintiff argued that he had suffered from unnecessary stress and wasted time resulting from the need to check his credit card statements and credit reports to ensure that he had not fallen victim to identity theft. The district court found that the plaintiff here could not satisfy the injury-in-fact requirement under *Spokeo* and dismissed the action.

Federal Court Dismisses TCPA Class Action Against Charitable Organizations, Insurance Company
In April 2018, a federal court granted a motion to dismiss a TCPA class action against certain charitable organizations and an insurance company. The court found that the plaintiff had provided prior express

Aaron Charfoos

RECENT AND PENDING PUBLICATIONS

U.S. Government Releases Report on IoT Botnets and Other Distributed Attacks (June 2018). **Jones Day Authors**: **Samir Jain**, **Rick Martinez**

DOJ Takes Action Against Sophisticated Botnet Linked to Russian DNC Hackers (May 2018). **Jones Day Authors**: **Jimmy Kitchen**, **Jay Johnson**, **Todd McClelland**, **Jeff Rabkin**

SEC Announces Yahoo Will Pay $35 Million for Failure to Disclose Data Security Incident (May 2018). **Jones Day Authors**: Various

Federal Court Dismisses TCPA Class Action Against Charitable Organizations, Insurance Company (Apr. 2018). **Jones Day Authors**: **Todd Kennard**, **Bill Dolan**, **John Vogt**

Draft EU CLOUD Proposal—Enabling Law Enforcement Access to Overseas Data (Apr. 2018). **Jones Day Authors**: **Laurent De Muyter**, **Jörg Hladjk**

Ninth Circuit Finds Data Breach Customers Have Initial Standing to Sue (Apr. 2018). **Jones Day Authors**: **Todd Kennard**, **Bill Dolan**, **John Vogt**, **Ali Schill**

consent and that the text messages at issue were merely informational, were not advertisements, and did not constitute telemarketing. For more information, see the Jones Day *Alert*.

Seventh Circuit Revives Class Action Security Breach Lawsuit
On April 11, 2018, the Court of Appeals for the Seventh Circuit revived a proposed class action alleging a major book retailer failed to secure customers' financial data during a 2012 security breach. Reversing the lower court's decision, the appellate court found that the customers sufficiently alleged economic damages in the form of security costs and lost time. The ruling follows the district court's earlier ruling granting the defendant company's motion to dismiss on grounds that the class representatives had failed to show economic damages.

Rideshare Company Agrees to Expanded Settlement with the FTC
On April 12, 2018, a major rideshare company agreed to an expanded settlement with the FTC over claims that the company failed to disclose a data breach that occurred in 2016. At the time of the 2016 data breach, the FTC was investigating the company for an earlier 2014 breach. The new settlement requires the company to disclose future breaches to the FTC and provide copies of third-party audits of its privacy program to the FTC.

West Virginia Attorney General Sues Credit Reporting Company Over Data Breach
On April 12, 2018, West Virginia Attorney General Patrick Morrissey announced a lawsuit against a credit reporting company for failing to safeguard consumer information of hundreds of thousands of state residents and for delaying disclosure to the public of a breach that exposed the personal data of about 148 million people. The lawsuit alleges that the company took no action to secure its online dispute portal despite prior warnings of vulnerability.

Major Internet Search Engine to Pay First SEC Penalty over Response to Hack
On April 24, 2018, the SEC announced that Altaba Inc., f/k/a Yahoo, would pay $35 million for misleading investors by waiting nearly two years to acknowledge a computer breach. This is the first such penalty levied against a publicly traded company for failing to disclose a cyberattack. The SEC claims that Yahoo officials learned of the breach days after it happened in December 2014 but failed to disclose to investors that Russian hackers had broken into its database until September 2016. For more information, see our Jones Day *Commentary*.

Ninth Circuit Revives Lawsuit Against Shoe Retailer
In April 2018, the Court of Appeals for the Ninth Circuit reversed the lower court's finding that a group of plaintiffs did not have standing to sue regarding a shoe retailer's data breach. The unanimous Ninth Circuit panel determined that the "imminent" risk of identity theft from the breach was enough to establish standing to sue. For more information, see our Jones Day *Commentary*.

Supreme Court to Review Online Search Company's *Cy Pres* Settlement
On April 30, 2018, the U.S. Supreme Court granted certiorari for review of a settlement agreement in which an online search company agreed to pay millions of dollars to third-party privacy nonprofit organizations, while providing nothing to users of the company, to settle allegations of illegal information-sharing with advertisers. The review marks the first instance in which the Supreme Court will consider *cy pres* remedies, where awards in a class action are provided to a non-party in place of providing the award to the plaintiff class.

Second Circuit Upholds Dismissal of Class Action against E-Merchants' Sharing of Data
On May 7, 2018, the Court of Appeals for the Second Circuit upheld the dismissal of a putative class action against a collection of e-merchants. The putative class had alleged that the e-merchants had deceptively enrolled its consumers in rewards programs, which automatically charged monthly fees, when the e-merchants exchanged consumer data between one another. The district court originally dismissed the claim, finding that the plaintiffs had failed to show that they had never consented to the exchange of information.

Eleventh Circuit Finds FTC's Order to Implement Data Security Measures Unenforceable
On June 6, 2018, the Court of Appeals for the Eleventh Circuit vacated the FTC's order directing a laboratory services company to implement a variety of data security measures. The FTC's initial order followed an investigation into the alleged exposure of 9,300 consumers' personal information on a file-sharing site. On appeal, the Eleventh Circuit found the order unenforceable because it "does not enjoin a specific act or practice" and instead mandates a "complete overhaul" of the company's data security program without sufficient specificity.

Legislative—Federal

Congress Passes CLOUD Act
On March 23, 2018, Congress enacted the Clarifying Overseas Use of Data ("CLOUD") Act. Under the new law, U.S. law enforcement authorities may compel production of communications data stored outside the United States, and certain foreign countries may be eligible to enter into executive agreements with the United States that would permit U.S. service providers to respond to certain foreign orders seeking access to communications data. For more information, see our Jones Day *Commentary*.

House Passes Bill to Counter Identity Theft Against Children
On April 17, 2018, the House of Representatives passed the Protecting Children from Identity Theft Act, which authorizes the Social Security Administration to establish a new database so that financial institutions can verify a person's Social Security number, name, and date of birth before reporting it to a credit agency. The legislation seeks to prevent "synthetic identity theft"—mixing a real Social Security number with fake information—perpetuated against children and others with minimal credit history.

Legislative—States

Oregon Amends Data Breach Notification Law
On March 16, 2018, Oregon's governor signed S.B. 1551, which amends Oregon's data breach notification law. The amendment alters the law's notification requirement, such that the entity must now give notification not later than 45 days after discovering or receiving notification of the breach of security. Additionally, if the entity offers to provide credit monitoring services in connection with the notification, it may not condition the provision of services on the consumer providing a credit or debit card number. The law also expands the definition of "personal information" to include any information or combination of information that the entity reasonably knows or should know would permit access to the consumer's financial account.

South Dakota Enacts Data Breach Notification Law
On March 21, 2018, South Dakota's governor signed S.B. 62, the state's first data breach notification law. The law governs data breach notification requirements for entities conducting business in South Dakota and those owning or licensing computerized personal or protected information of South Dakota residents. The bill requires notification to affected consumers not later than 60 days from the discovery or notification of the breach of system security.

Alabama Enacts Data Breach Notification Law
On March 28, 2018, Alabama's governor signed S.B. 318, making Alabama the final state to enact a data breach notification law. The law governs data breach notification requirements for entities acquiring or using sensitive personally identifying information of an Alabama resident. The bill requires notification to affected customers in the event of a breach within 45 days of the entity determining that a breach occurred. The law also provides that covered entities and their agents must implement and maintain reasonable security measures to protect sensitive personally identifying information.

Vermont Adopts Data Broker Legislation
On May 24, 2018, Vermont's attorney general issued a press release discussing a new law establishing a registry and security standards for commercial entities that buy and sell consumer data. As outlined in the release, the law contains four goals: (i) eliminating fees; (ii) protecting consumers from fraud; (iii) clarifying minimum data security requirements; and (iv) providing transparency to consumers.

Canada

OPC Launches Investigation of Social Media Company
On March 20, 2018, the Office of the Privacy Commissioner of Canada ("OPC") opened an investigation concerning recent alleged reports of a major social media company using and accessing user profiles without authorization. The investigation will focus on the company's compliance with the Personal Information Protection and Electronic Documents Act.

OPC Announces New Approach to Privacy Protection
On April 16, 2018, the OPC announced a new Departmental Plan and a new organizational structure to address privacy protection. The OPC's new strategy will inform Canadians of their rights and how to exercise them and will also guide departments and organizations on how to comply with privacy obligations.

OPC Issues New Guidance on Consent
On May 24, 2018, the OPC published two new guidance documents to help organizations comply with privacy obligations. The guidance documents, launched at a conference of the International Association of Privacy Professionals in Toronto, focus on obtaining meaningful consent and on inappropriate data practices.

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, Laura Lim, Dan McLoon, Mary Alexander Myers, Mauricio Paez, Nicole Perry, Alexa Sendukas, Aaron Tso, and Anand Varadarajan.

[Return to Top]

Latin America

Jones Day Hosts Third Latin America and Cybersecurity Symposium
On April 26 and 27, 2018, Jones Day hosted the Third Latin America and Cybersecurity Symposium. The

symposium offered panels on new legal obligations for information and security management in light of updated privacy and cybersecurity legislation in Latin American countries, and discussed best compliance practices. Key takeaways included:

- An increased interest on cybersecurity and technology in Latin America.
- Mexico and Brazil lead the development of financial technology institutions in the region.
- Latin American countries develop privacy and data protection regulations in harmony with EU regulations.
- Latin American countries lean toward a data incident notification to the authority model following the already established obligations in the United States and the European Union.
- The significant presence of cyberattacks in the region.

For more information, see our Jones Day press release.

Argentina

Agency for the Access to Public Information Amends Data Controllers' Personal Data Notice
On March 9, 2018, Argentina's Agency for the Access to Public Information ("*Agencia de Acceso a la Informacion Publica de Argentina*") amended a mandatory notice used by data controllers (source document in Spanish). The notice now covers instances where the data controller collects and processes an individual's image in digital media.

Brazil

Brazil's National Monetary Council Issues Resolution Regulating Credit Financial Technologies
On April 26, 2018, Brazil's National Monetary Council issued Resolution 4,656, regulating credit financial technologies (source document in Portuguese). Under the Resolution, direct credit companies and interpersonal loan companies will be considered financial institutions and entitled to conduct loan and financial operations through electronic platforms. The Resolution also provides certain requirements for obtaining authorization from the Central Bank of Brazil.

Brazil's National Monetary Council Issues New Rules on Cybersecurity Policies and Data Processing and Storage Requirements
On April 26, 2018, Brazil's National Monetary Council issued Resolution 4,658, creating new rules on cybersecurity policies and requirements for data processing and storage (source document in Portuguese). Per the Resolution, institutions authorized to operate by the Central Bank of Brazil must implement a cybersecurity policy in order to ensure confidentiality of data systems. In addition, the Resolution requires that institutions notify the Central Bank of third-party vendor contracts, regardless of the nationality of the corresponding service provider.

Chile

Chilean Senate Considers New Draft Bill for Personal Data Protection
On April 3, 2018, the Chilean Senate debated the data protection draft bill (source document in Spanish). The law, which would regulate private parties and government agencies, sets forth the following purposes: (i) to regulate the processing of personal data; (ii) to create a Personal Data Protection Agency in Chile; (iii) to create the National Registry of Compliance and Sanctions, administered by the Personal Data Protection Agency; (iv) to regulate liability of governmental agencies regarding personal data processing; and (v) to provide sanctions in the case of violations.

Colombia

Industrial Cybersecurity Center Publishes Second Cybersecurity Study
On April 16, 2018, the Industrial Cybersecurity Center published its second cybersecurity study (source document in Spanish). This document presented the results of a study conducted with managers of 35 Colombian industrial companies. Points evaluated include: (i) the organization of industrial cybersecurity; (ii) industrial cybersecurity management; (iii) technical aspects of industrial cybersecurity; and (iv) industrial cybersecurity markets.

Mexico

Mexico Congress Approves Law Regulating Financial Technology Institutions
On March 1, 2018, the Mexican Congress issued a statement approving the Law Regulating Financial Technology Institutions (source document in Spanish). The purpose of the law is to provide a regulatory framework for financial technology institutions, including their operation, functioning, and services.

Ministry of Public Administration Issues 2018 Open Government Guide

On March 23, 2018, the Ministry of the Public Administration issued the 2018 Open Government Guide (source document in Spanish). This guide establishes plans and procedures on transparency and the protection of personal data, including the bases and procedures for the inclusion of information in the federal platform of citizen participation as well as specific measures for agencies of the Federal Public Administration.

Mexico City Approves Law for Protection of Personal Data Held by Government Agencies
On April 10, 2018, the Legislative Assembly of Mexico City approved the Law on the Protection of Personal Data Held by Government Agencies of Mexico City (*Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México*) (source document in Spanish). The law provides the bases, principles, and procedures to guarantee every person's right to request information about the processing and protection of his or her personal data.

Cyberattack Interrupts Banking Activity in Mexico
On April 27, 2018, Banco de Mexico issued a statement that three banks experienced incidents with the Interbank Electronic Payment System ("SPEI") (source document in Spanish). The incidents caused significant interruption and delays in banking transfers but did not affect the infrastructure of the banks.

The following Jones Day lawyers contributed to this section: Guillermo Larrea and Abigail Ruiz.

[Return to Top]

Europe

European Union

EU Issues Proposal to Allow Law Enforcement Access to Overseas Data
On April 17, 2018, the European Commission proposed a legislative package to allow EU Member State law enforcement and judicial authorities access, directly from service providers, electronic evidence held outside of the European Union or in another EU Member State. The draft Regulation enables authorities to directly request a service provider in another Member State to disclose data about a user within 10 days, or six hours in emergency cases. For more information, see our Jones Day *Commentary*.

EU Considers Whistleblower Protections
On April 23, 2018, the European Commission published a draft law to strengthen whistleblower protections across the European Union. Under the draft legislation, whistleblowers who expose violations of data protection, competition, and public procurement rules will be afforded greater protection from retaliation by companies and public authorities.

Council of the European Union

Bulgarian President Releases Draft ePrivacy Proposal
On May 4, 2018, the Bulgarian president published a new version of the proposed ePrivacy Regulation for the relevant delegations of the Council of the European Union. The draft text will be discussed during committee meetings and is pending adoption by the EU Parliament and the Council.

Article 29 Working Party

Article 29 Working Party Publishes Revised Guidelines on Transparency and Consent under GDPR
On April 11, 2018, the Article 29 Working Party published the last revised version of the Guidelines on Transparency. The revisions cover issues such as the requirement that information be "intelligible" and changes to Article 13 and 14. Similarly, on April 10, 2018, the Article 29 Working Party published the last revised version of the Guidelines on Consent, including consent issues relating to users' continued use of websites.

Article 29 Working Party Sets Forth Cooperation Procedure for Approval of Binding Corporate Rules
On April 11, 2018, the Article 29 Working Party published a Working Document on the procedure for approving binding corporate rules ("BCR") for controllers and processors, and on determining the Lead Supervisory Authority for the BCR. BCR are to be approved by the competent supervisory authority in the relevant jurisdiction in accordance with the consistency mechanism, whereby the European Data Protection Board will issue a nonbinding opinion on the draft decision stemming from the competent Lead Supervisory Authority.

Article 29 Working Party Establishes Social Media Working Group
On April 11, 2018, the Article 29 Working Party announced support for the ongoing investigations run by national privacy authorities into the collection and use of personal data by social media companies. In addition, the Article 29 Working Party will create a Social Media Working Group to develop a long-term strategy on this issue.

Article 29 Working Party Comments on Framework for Interoperability of EU Information Systems
On April 23, 2018, the Article 29 Working Party published its Opinion on the Commission's 2017 proposals for rendering interoperable European information systems in the field of border control, migration, international protection, and police and judicial cooperation. The Opinion recommends against the creation of a Common Identity Repository that contains a cross-matching of various sources for identification consolidated in a new common database.

European Data Protection Supervisor

EDPS Publishes Opinion on International Agreements Relating to Exchange of Data with Non-EU Nations
On March 14, 2018, the European Data Protection Supervisor ("EDPS") Commission issued eight recommendations suggesting the Council authorize negotiations between the European Union and Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia, and Turkey to foster the limited exchange of personal data between Europol and law enforcement authorities of these nations. The executed international agreements would provide the required legal basis for Europol to transfer personal data to these countries' law enforcement authorities. The EDPS made general recommendations to ensure that any agreements include appropriate safeguards within the meaning of the Europol Regulation.

EDPS Publishes 2017 Annual Report
On March 19, 2018, the EDPS published its 2017 annual report. The report underlines key achievements from 2017, including: advising the EU legislator on the upcoming ePrivacy Regulation; launching initiatives related to the Digital Clearinghouse and Digital Ethic; contributing to ongoing discussions on the EU-U.S. Privacy Shield; fostering the free flow of data in trade agreements; and the effective supervision of Europol.

EDPS Issues Opinion on Regulations Relating to EU Large-Scale Information Systems
On April 16, 2018, the EDPS published its Opinion on the European Commission's proposals to launch a process toward the interoperability of existing and future EU large-scale information systems in the fields of migration, asylum, and security.

European Network and Information Security Agency

ENISA Publishes Report on Threat Intelligence Platforms
On March 26, 2018, the European Network and Information Security Agency ("ENISA") published a report on threat intelligence platforms ("TIP") that focuses on limitations of threat information-sharing and the analytical tools currently in use, as well as on the relevant recommendations to overcome these limitations. The report presents an overview of the users of these platforms, the main functional areas of TIPs, and the current landscape of the TIPs used by different teams globally.

ENISA Publishes Position Paper on Online Disinformation
On April 27, 2018, ENISA published its position paper on the problem of online disinformation in the EU from a Network and Information Security ("NIS") perspective. The paper presents a number of recommendations relating to both general NIS measures as well as privacy and data protection measures.

Belgium

Belgian Privacy Commission Comments on Draft Law Relating Processing of Personal Data
On April 11, 2018, the Belgian Privacy Commission published Opinion No. 33/2018 on the draft law relating to the protection of natural persons with respect to the processing of personal data (source document in French). The opinion follows the enactment of the GDPR and the transposition of Directive 2016/680.

France

CNIL Issues 2018 Priorities and Concerns
On March 10, 2018, the French Data Protection Authority ("CNIL") set out its main priorities and concerns for 2018 (source document in French). CNIL announced that it will continue its work on the ethical and legal framework relating to artificial intelligence and broaden the debate on artificial intelligence governance. CNIL also discussed blockchain technology and potential concerns about compatibility with the GDPR.

ANSSI and EPSF Strengthen Cooperation in Digital Security
On March 20, 2018, the French Network and Information Security Agency ("ANSSI") and the French Railway Safety Authority ("EPSF") signed a letter of intent to protect the railway sector from cyberattacks (source document in French). ANSSI highlighted the digitalization of the sector and potential vulnerabilities facing the industry.

CNIL Provides Guidance on Personal Data Processing by Third-Party Applications

On March 21, 2018, CNIL provided guidance to data subjects on third-party applications' personal data processing activities (source document in French). CNIL recommended that data subjects stay vigilant when using any third-party applications and gave practical advice, including app deletion, on limiting access to personal data.

CNIL Allows for Online Appointment of Data Protection Officers
On March 28, 2018, CNIL provided an online service allowing for the designation of data protection officers ("DPO") (source document in French). Appointed DPOs must monitor a company's compliance with the applicable legal framework relating to cybersecurity and data privacy.

CNIL Advises on GPDR Compliance and Implementation
On April 10, 2018, CNIL stated that it would issue benchmarks that specify GDPR principles and provide guidance on how to ensure compliance with the GDPR (source document in French). CNIL also expressed an intention to monitor organizations' compliance with the GDPR moving forward.

ANSSI Raises Digital Security Concerns in Annual Report
On April 17, 2018, the ANSSI released its annual report on 2017 cyberattacks and the commitment to preventing these attacks in the future (source document in French). ANSSI identified the domestic and EU-wide priorities for 2018 to enhance digital security.

CNIL Address Protection of Biometric Data
On April 18, 2018, CNIL outlined its policy on biometric data (source document in French). According to the policy, the following conditions are required: (i) the processing of such data must be necessary for the purposes of the process; (ii) the data subject must be free to choose between biometric technology and an alternative authentication process; and (iii) biometric data must remain under the exclusive control of the data subject.

Germany

Bavarian DPA Publishes Information for Small Businesses and Associations
On March 22, 2018, the Bavarian Data Protection Authority ("DPA") published guidance on essential requirements under the GDPR for small businesses. The guidance addresses entities such as car repair shops, craft businesses, tax consultants, doctor practices, privately owned property managements, production operations, credit cooperatives, bakeries, online shops, accommodation services, and retailers (source document in German).

Insurance Study Finds Small and Medium-Sized Enterprises Unprepared for GDPR
On April 18, 2018, the Association of the German Insurance Industry published the results of a survey conducted by the polling institute Forsa (source document in German). According to the survey, the majority of small and medium-sized enterprises in Germany are not equipped to handle the GDPR, with only 22 percent having adopted requisite measures.

DPAs Post Online Forms to Contact Data Protection Officers
On April 24, 2018, the Bavarian DPA issued a press release discussing a new online form to contact the data protection officer of the DPA (source document in German). The DPAs of other states in Germany have also made such forms available, including Baden-Württemberg and Mecklenburg-Western Pomerania (source documents in German).

DSK Issues Guidance on Online Tracking Mechanisms
On April 26, 2018, the German Data Protection Commission (*Datenschutzkonferenz*, "DSK"), published a paper addressing the legal requirements pertaining to online tracking mechanisms (source document in German). The DSK guidance, formed through consensus of all German DPAs, discusses how to obtain informed consent under the GDPR, including prior to placing cookies or collecting information stored on the user's terminal.

Italy

Italian DPA to Enforce GDPR Sanctions without Delay
On April 19, 2018, the Italian DPA clarified that it would enforce the GDPR and sanctions under the GDPR without any waiting period or delay. The GDPR went into effect on May 25, 2018.

The Netherlands

DDPA Requires Online Registration of Data Protection Officers
On April 3, 2018, the Dutch Data Protection Authority ("DDPA") began requiring organizations to re-register their data protection officer via an online registration form (source document in Dutch).

House of Representatives Considers Dutch Cyber Security Agenda
On April 20, 2018, the House of Representatives received the Cyber Security Agenda, which sets out the framework for accomplishing the nation's cybersecurity priorities (source document in Dutch). Specifically, the agenda contemplates various public, private, national, and international measures available to the

country to accomplish these goals.

DDPA Presents 2017 Annual Report
On April 24, 2018, the DDPA presented its 2017 Annual Report titled "More Attention for Privacy" (source document in Dutch). The report discloses the following about 2017: (i) 10,009 data breaches were notified to the DDPA; (ii) the DDPA finalized 200 investigations, including investigations into data breaches; (iii) the DDPA performed 217 "alternative interventions"; (iv) the DDPA advised on draft bills 28 times; (v) the DDPA imposed 20 measures under threat of penalty; and (vi) the DDPA imposed no fines.

Spain

SDPA and SCA Enact Protocol to Assist Data Protection Officers
On March 13, 2018, the Spanish Data Protection Agency ("SDPA") announced a protocol with the Spanish Compliance Association ("SCA") to assist the nation's data protection officers (source document in Spanish). Per the arrangement, the SDPA will provide the SCA with tools, guides, and publications, including the Risk Assessment Guide and Impact Assessment Guide, to help data processors and data protection officers achieve compliance under the GDPR.

SDPA Approves Online Notification of Appointment of Data Protection Officers
On April 10, 2018, the Spanish Data Protection Agency announced that public administrations and companies required to appoint a data protection officer could communicate their appointment via an online form.

SDPA Issues Checklist to Assist with GDPR Compliance
On April 13, 2018, the Spanish Data Protection Agency issued a document to help data controllers and processors identify and verify the minimum requirements set out by the GDPR (source document in Spanish). The document is divided into 29 blocks, including information transparency, data subjects' rights, records of processing activities, technical and organizational measures, and transfers of data to non-EU countries.

United Kingdom

ICO Publishes Finalized Guidance on Consent Under GDPR
On March 22, 2018, the Information Commissioners' Office ("ICO") published its final guidance on consent for UK organizations under the GDPR. The ICO guidance explains the features of valid consent and describes when organization may rely on consent and how to obtain consent under the GDPR.

ICO Consults Public on Powers Following GDPR Implementation
On May 4, 2018, the ICO invited comments on a draft Regulatory Action for an eight-week period. The draft Regulatory Action grants authority to the ICO to: (i) carry out no-notice inspections; and (ii) compel people and organizations to provide requested information.

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

[Return to Top]

Asia

Hong Kong

PCPD Considers Do-Not-Call Registry
On May 3, 2018, the Office of the Privacy Commissioner for Personal Data ("PCPD") explained that a statutory do-not-call registry will provide protections against unwanted telemarketing campaigns (source document in Chinese). While discussing the benefits of the registry, the Privacy Commissioner also emphasized the value of telemarketing to the economy and recommended that the government appoint the privacy commissioner as the managing authority for the registry.

PCPD Responds to Intrusion into Broadband Network's Customer Database
On April 18, 2018, a broadband internet provider reported an intrusion into its ex-customer database (source document in Chinese). The PCPD began an investigation and review of the matter given size of the database and number of individuals involved.

Hong Kong Businesses Prepare for GDPR Compliance
In March 2018, the PCPD issued the European Union General Data Protection Regulation (GDPR) 2016 booklet. The publication discusses how organizations and businesses in Hong Kong can comply with the new regulatory framework in the European Union and highlights key differences between the GDPR and domestic regulations and laws.

Japan

Personal Information Protection Commission Releases Draft Guidelines on Personal Data Transfers

On April 25, 2018, the Personal Information Protection Commission released draft guidelines on the processing of personal data transferred from the European Union for public comments (source document in Japanese). Under the draft guidelines, legally binding rules that will apply to the personal data transferred from the European Union to Japan based upon the European Union's adequacy decision.

People's Republic of China

Travel Booking Website to Share Guest Data with Chinese Authorities

On March 29, 2018, a website dedicated to renting personal homes to travelers informed its Chinese hosts that it will begin sharing user data with Chinese government agencies to comply with the country's regulation (source document in Chinese). China requires all hotels to report guest information to the police, and travelers staying in private homes are supposed to register that information within 24 hours of arriving in the country.

China Publishes National Standard for Personal Data Protection

On May 1, 2018, China implemented a national standard for personal information protection: the Information Security Technology—Personal Information Security Specification (source document in Chinese). The standard provides detailed guidance for corporations on establishing and maintaining information governance systems.

Singapore

PDPC Calls for Assessment Bodies for Data Protection Trustmark Certification

On March 14, 2018, the Personal Data Protection Commission ("PDPC") invited interested and suitable companies to participate as assessment bodies for the Data Protection ("DP") Trustmark Certification. The DP Trustmark Certification allows organizations to demonstrate compliance with the Personal Data Protection Act ("PDPA") and show adequate management of personal data.

PDPC Issues Advisory Guidelines on In-Vehicle Recordings by Transport Services for Hire

On April 9, 2018, the PDPC issued new advisory guidelines on in-vehicle recordings by transport services for hire. The guidelines were developed in consultation with the Land Transport Authority and provide guidance for compliance with the Data Protection Provisions when in-vehicle recording devices are used.

PDPC Fines Health Care Company Following Data Breach

On April 19, 2018, the PDPC fined a health care company for failing to meet its obligation to make reasonable security arrangements for the protection of personal data under Section 24 of the PDPA. The Commissioner determined that the company disclosed sensitive, medical-related personal data without authorization and failed to adequately safeguard such data.

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

[Return to Top]

Australia

Information Commissioner Releases Quarterly Data Breach Report

On April 11, 2018, the Office of the Australian Information Commissioner published its first quarterly report on data breach notifications received pursuant to the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth). The report discusses the 63 notifications received by the Commissioner during the first quarter of 2018 and provides detailed information regarding: (i) the industries affected by the data breaches; (ii) the type of data compromised; (iii) the technical and nontechnical reasons for the data compromises; and (iv) the number of individuals compromised in each breach.

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

[Return to Top]