JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 19 | October 2018

JONES DAY

GLOBAL PRIVACY & CYBERSECURITY UPDATE

Jones Day Cybersecurity, Privacy & Data Protection Attorney Spotlight: Jeff Rabkin

On the heels of the European Union's General Data Protection law, which went into effect in May 2018, California has enacted the California Consumer Privacy Act ("CCPA")—the result of an 11th-hour compromise between California lawmakers and consumer privacy activists made to avoid a widely criticized data privacy ballot initiative. The law originally passed in June of this year and was amended in September. It goes into effect on January 1, 2020, and is likely to be modified again prior to the effective date.

The key provisions of the law as presently drafted require companies to provide consumers, upon request, with data regarding their personal information that companies collect and sell. In addition, the law requires companies to delete consumer personal information upon request and to allow consumers to opt out of the sale of their personal information. Importantly, the CCPA also provides consumers with a private right of action, and statutory damages, if certain unencrypted or unredacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure because of a company's failure to implement and maintain reasonable security procedures and practices. It provides the California Department of Justice with both rule-making responsibilities and the authority to impose significant penalties for violations of the statute.

Jeff Rabkin, a partner in our San Francisco Office, came to Jones Day in April 2015 from the leadership team of then-California Attorney General Kamala D. Harris. As Special Assistant Attorney General for Law and Technology, Jeff's portfolio included responsibility for oversight of the lawyers tasked with enforcing California's privacy law as well as cybercrime prosecutions throughout the state. He also served as an Assistant U.S. Attorney for eight years in New York and San Francisco, representing the United States in hundreds of federal criminal matters and led numerous high-profile, sensitive investigations and prosecutions involving corporate fraud, public corruption, and other white-collar crime.

Now a leading practitioner in the fields of cybersecurity and privacy, as well as on legal issues and regulatory risk

EDITORIAL CONTACTS

Daniel J. McLoon
Los Angeles

Mauricio F. Paez
New York

Jay Johnson
Dallas

Jonathon Little
London

Todd S. McClelland
Atlanta

Jeff Rabkin
San Francisco

Lisa M. Ropple
Boston

Adam Salter
Sydney

Michiru Takahashi
Tokyo

Undine von Diemar
Munich

Olivier Haas
Paris

Jörg Hladjk
Brussels

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

HOT TOPICS IN THIS ISSUE

arising from disruptive technology, and a key member of Jones Day's team, Jeff represents businesses in all types of government investigations, regulatory proceedings, and private disputes. He also advises in-house counsel, corporate executives, and boards of directors on these topics.

United States

Regulatory—Policy, Best Practices, and Standards

Report Finds 75 Percent of All U.S. Retailers Have Suffered Data Breach
In July, a security company issued a report finding that 75 percent of all U.S. retailers have suffered at least one data breach. Of those breaches, 50 percent occurred within the last year, and 26 percent of retailers have experienced more than one breach. The report revealed that several factors, including third-party weak spots and "frictionless" retail experiences, drove the increase in data breaches. The report also revealed that 84 percent of U.S. retailers planned to increase IT security budgets in 2018.

Regulatory—Critical Infrastructure

NIST Issues Findings on Why Employees Click on Phishing Emails
On June 27, the National Institute of Standards and Technology ("NIST") released a video exploring why people click on phishing emails. According to NIST's study, context plays a critical factor in why users click or do not click on a phishing email, and the more relevant the context of the message seems to a person's life or job responsibilities, the harder it is for that person to recognize it as a phishing attack.

Regulatory—Consumer and Retail

FTC Releases Comment on Internet of Things and Consumer Product Hazards
On June 15, the Federal Trade Commission's ("FTC") Bureau of Consumer Protection ("BCP") issued a comment in response to the Consumer Product Safety Commission's request for comments on potential hazards associated with internet-connected consumer products. The BCP also outlined the FTC's cybersecurity education and enforcement work and encouraged manufacturers to review the FTC's guidelines on how to predict and mitigate privacy and security risks.

Former Employee Sues Retailer Under Illinois's Biometric Data Law
In July, a former employee of a retailer filed suit against the company alleging that the company's use of biometric fingerprint scanners for timekeeping violated Illinois's Biometric Information Privacy Act. The employee alleged that the company never received written consent from employees to collect their biometric data, failed to tell employees why it collected their biometric data or what the data would be used for, and shared employees' biometric data with third parties without employees' permission.

Regulatory—Financial

Bureau of Consumer Financial Protection Finalizes GLBA Amendments
On August 10, the Bureau of Consumer Financial Protection finalized amendments to implement legislation

Regulatory Framework to GDPR

Final Agreement to Establish Framework to Easily Transfer Personal Data between Japan and EU

Australia Extends Deadline to Opt Out of My Health Records

RECENT AND PENDING SPEAKING ENGAGEMENTS

Keynote Address, Advanced Cyber Security Center Annual Conference, Boston, MA (November 2018). **Jones Day Speaker:** Samir Jain

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, TX (October 2018). **Jones Day Speaker:** Jay Johnson

Data Breach Class Actions: Are You Prepared?, Jones Day Webinar (October 2018). **Jones Day Speakers:** Tiffany Lipscomb-Jackson, Lisa Ropple, Jeff Rabkin, John Vogt

Cybersecurity Seminar, Michigan State University, East Lansing, MI (October 2018). **Jones Day Speaker:** Samir Jain

Marketing Under GDPR: Challenges, Experiences, and Solutions, IAPP Brussels KnowledgeNet, Belgium (October 2018). **Jones Day Moderator**: Jörg Hladjk

Wearables in the Context of Data Protection Regulations (Risks & Challenges), FIFA Football Technology & Data Summit 2018, Zurich, Switzerland (October 2018). **Jones Day Speaker**: Jörg Hladjk

Fifth Annual Cybersecurity Conference for Executives, Johns Hopkins University, Baltimore, MD (October 2018). **Jones Day Speaker:** Samir Jain

Handling a Cybersecurity Investigation: An Interactive Tabletop Exercise led by a Regulator, a Lawyer, and a Security Expert, Dallas Regional Compliance & Ethics Conference, Society of Corporate Compliance and Ethics, Dallas, TX (September 2018). **Jones Day Speaker:** Jay Johnson

Keynote Address, 41st Annual Southwest Securities Conference, Dallas, TX (September 2018). **Jones Day Speakers:** Mark Rasmussen,

allowing financial institutions that meet certain criteria to be exempt from the Gramm-Leach-Bliley Act's ("GLBA") annual privacy notice requirement. The annual privacy notice must inform consumers about their right to opt out of some sharing by the financial institution of nonpublic personal information with certain nonaffiliated third parties. The amendments create an exception to this annual privacy notice requirement for financial institutions whose sharing of information does not trigger an opt-out right for consumers under the GLBA, and the institution has not changed its privacy notice since the last one provided to consumers.

New York State Cybersecurity Law Poses Challenge For Insurers

On September 3, another set of New York's cybersecurity regulations under 23 NYCRR 500 went into effect after an 18-month transitional period. The regulations, 23 NYCRR 500, require insurers who write policies in New York to encrypt customers' nonpublic information both in transit and at rest. Insurers also are required to maintain audit trails of all financial transactions that take place on their networks, as well as audit trails to detect and respond to a data breach.

Regulatory—Health Care/HIPAA

OCR Issues Guidance on Unpatched Software Risks to ePHI

In June, the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") issued guidance on reducing risks that software poses to electronic protected health information ("ePHI"), such as installing patches or restricting network access as appropriate on all types of devices that store ePHI, including phones, computers, servers, and routers. The OCR pointed to the United States Computer Emergency Readiness Team and Health Insurance Portability and Accountability Act ("HIPAA") Administrative Safeguards as additional resources.

California Amends CCPA to Include Exemptions for Health Information

On August 31, the California legislature passed a bill to amend the California Consumer Privacy Act of 2018 ("CCPA"). Amendments include exemptions relating to health information by certain entities, including providers and entities covered by HIPAA and related state laws, business associates, and those collecting health information as part of clinical trials.

Regulatory—Defense and National Security

NIST Publishes Guidance for Contractors Handling Controlled Unclassified Information

On June 13, NIST published guidance for defense contractors handling controlled unclassified information ("CUI"). Special Publication 800-171A, "Assessing Security Requirements for Controlled Unclassified Information (CUI)," provides a roadmap for conducting cybersecurity assessments in compliance with DFARS 252.204-7012 and NIST Special Publication 800-171. NIST subsequently published a bulletin on July 27 that summarizes the guidance in Special Publication 800-171A.

NCSC Releases 2018 Foreign Economic Espionage in Cyberspace Report

On July 26, the National Counterintelligence and Security Center ("NCSC") released its 2018 Foreign Economic Espionage in Cyberspace report, which highlighted current

Jim Cox, Jay Johnson

What to Do When...California's New Data Privacy Rules Come Into Effect, Jones Day Silicon Valley Office, Palo Alto, CA (September 2018). **Jones Day Speakers:** John Vogt, Ed Chang, Jeff Rabkin

Accommodating Data Subjects When They Exercise Their Rights, IAPP Data Protection Intensive: Deutschland 2108, Munich, Germany (September 2018). **Jones Day Speaker:** Undine von Diemar

Cybersecurity: The Latest Strategies for Responding to Ransomware and Other Cybersecurity Incidents, 5th Annual Government Enforcement Institute, Dallas, TX (September 2018). **Jones Day Speaker:** Jay Johnson

Keynote at the IAPP Data Protection Intensive: Deutschland 2018, Munich, Germany (September 2018). **Jones Day Speaker:** Undine von Diemar

The DPO's Place in the Organization, IAPP Data Protection Intensive: Deutschland 2108, Munich, Germany (September 2018). **Jones Day Speaker:** Undine von Diemar

Cybersecurity Issues in Commercial Contracting, Waltham, MA (August 2018). **Jones Day Speakers:** Lisa Ropple, Todd McClelland

Summit on Digital Health Law, Cybersecurity, Chicago, IL (July 2018). **Jones Day Speaker:** Samir Jain

Data Breaches and Cyber Attacks—What You Should and Should Not Do, IAPP KnowledgeNet, Munich, Germany (July 2018). **Jones Day Speaker:** Undine von Diemar

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

RECENT AND PENDING PUBLICATIONS

Belgium Publishes Data Protection Laws Implementing GDPR (September 2018). **Jones Day Authors**: Laurent De Muyter, Jörg Hladjk

Catch Up With the California Consumer Privacy Act, *Daily Journal* (September 2018). **Jones Day Authors**: John Vogt, Jeff Rabkin,

threats and trends in foreign intelligence efforts to steal U.S. intellectual property, trade secrets, and proprietary information through cyberspace. The report noted that next-generation technology, such as artificial intelligence, introduces new vulnerabilities to U.S. networks. It also identified the industries and technologies that foreign threat actors are most likely to target.

Litigation, Judicial Rulings, and Agency Enforcement Actions

Eleventh Circuit Throws Out FTC Order to Clinical Laboratory

On June 6, the Eleventh Circuit Court of Appeals threw out a cease-and-desist order the Federal Trade Commission ("FTC") issued against a clinical laboratory. The order had directed the company to overhaul its data security program pursuant to the FTC's authority to regulate unfair acts or practices under Section 5(a) of the FTC Act. Even assuming that the company's alleged failure constituted an unfair act or practice, the Eleventh Circuit nevertheless found that the cease-and-desist order exceeded the FTC's authority by failing to enjoin any specific act or practice, instead mandating a complete overhaul of the company's data protection program.

Eighth Circuit Approves $10 Million Settlement in 2013 Data Breach Case Against Retailer

On June 14, an Eighth Circuit panel affirmed a $10 million settlement that concluded a multidistrict litigation against a retailer over its 2013 data breach. This comes after the district court, on remand, recertified a class of shoppers comprising those with and without documented losses, and approved the proposed settlement.

Sixth Circuit Affirms IRS Immunity in Financial Privacy Case

On July 5, the Sixth Circuit Court of Appeals affirmed a district court decision from the Eastern District of Michigan regarding a "John Doe" summons the Internal Revenue Service ("IRS") issued seeking financial records related to the bank accounts of two companies pursuant to the Financial Right to Privacy Act ("FRPA"). While the district court determined that the IRS had failed to adhere to its own regulations in issuing the summons as "John Doe" without first seeking district court approval, the court nonetheless found that the IRS was entitled to sovereign immunity because it issued the summons to companies rather than individuals, and the waiver of sovereign immunity under the FRPA protects only individuals.

Media Company Settles Video Privacy Class Action for $7.4 Million

On July 5, a federal judge granted initial approval for a $7.4 million settlement deal between a class of subscribers and a media company. The complaint alleged that the company had violated the Michigan Video Rental Privacy Act by disclosing subscribers' personal data. The proposed settlement will net class members between $25 and $50 each.

Retailer Reaches Settlement in Data Breach Class Action

On July 16, plaintiffs in a putative class action filed a motion for preliminary approval of their settlement agreement with a video game and electronics retailer over a data breach that occurred between August 2016 and February 2017. The complaint, filed in September 2017, alleged that a security breach of the company's servers compromised customer credit and debit card information. The proposed settlement would provide reimbursements for the estimated 1.3 million credit and debit cards that were compromised during the breach. Under the proposed settlement, class members would be reimbursed $15 per hour spent replacing cards and $22 per card on which documented fraudulent charges occurred.

Laura Lim

Royal Decree-Law Approved to Ensure Application of GDPR in Spain (September 2018). **Jones Day Authors**: Irene Robledo, Undine von Diemar, Mauricio Paez, Olivier Haas

Blockchain for Business Lawyers, multiple authors and editors, American Bar Association, September 2018. **Jones Day Authors**: Various

Be Wary of Warranties for Software Design (August 2018). **Jones Day Authors**: Chuck Moellenberg, Bob Kantner

Brazil Enacts General Data Protection Law (August 2018). **Jones Day Authors**: Mauricio Paez, Artur Badra, Guillermo Larrea

The Perils of Well-Intentioned Deception: Insider Trading Case Highlights Challenges Facing Public Companies (July 2018). **Jones Day Authors**: Various

French Data Protection Authority Confirms Enforcement Trend on Security Obligations for Data Controllers (July 2018). **Jones Day Authors**: Olivier Haas, Undine von Diemar, Dan McLoon, Mauricio Paez

California Adopts Sweeping Consumer Privacy Law (July 2018). **Jones Day Authors**: Various

Privacy and Cybersecurity Developments in Latin America (June 2018). **Jones Day Authors**: Guillermo Larrea, Mauricio Paez, Todd McClelland, Rick Martinez

Vietnam Passes Sweeping Cybersecurity Law (June 2018). **Jones Day Authors**: Various

DOJ's Business Email Compromise Takedown Illustrates Pervasiveness of Internet Fraud Schemes (June 2018). **Jones Day Authors**: Jimmy Kitchen, Mauricio Paez, Lisa Ropple, Aaron Charfoos

Retailer Settles TCPA Class Action for $1.4 Million
On July 17, a class of consumers filed a motion for preliminary approval of their settlement agreement with a retailer over alleged violations of the Telephone Consumer Protection Act ("TCPA") regarding unsolicited text messages. The complaint, filed in June 2015, alleged that customers who signed up for the company's Loyalist program were not informed that they would receive promotional text messages via cellphone. A federal court granted preliminary approval for the proposed settlement, which calls for a fund of $750,000 in cash and $650,000 in vouchers for the company's merchandise. Under the proposed settlement, class members would be able to decide between a $25 check or a $50 voucher for goods.

Weight Loss Company Settles TCPA Class Action for $3 Million
On August 7, a class of consumer plaintiffs filed a motion for preliminary approval of a settlement agreement with a weight loss company. The complaint, filed in May, alleged that the company sent text messages through the use of an automatic telephone dialing system without permission and in violation of the TCPA. The proposed national class consists of 628,610 individuals who received a text message from the company without their express written consent since May 7, 2014. The proposed settlement would require the company to pay $3 million.

Judge Approves $115 Million Data Breach Settlement Against Health Insurer
On August 15, a federal judge in California issued an order giving final approval for a $115 million settlement that ends a consumer class action against a health insurance company. The complaint alleged that a data breach experienced by the company in 2015 put at risk the personal information of 79 million consumers.

Company Faces Suit Over Cryptocurrency Theft
On August 15, a cryptocurrency investor filed suit against a mobile phone carrier alleging that inadequate data protection measures resulted in the theft of more than three million cryptocurrency coins worth more than $24 million from his mobile phone. The investor alleged that he experienced two separate hacks on his phone within seven months.

California's Attorney General Highlights Challenges in Implementing CCPA
On August 22, the California attorney general sent a letter to state legislative leaders explaining "several unworkable obligations and serious operational challenges" in the CCPA that would impede the Attorney General's Office in conducting oversight and enforcement of the new privacy law if not addressed.

Legislative—Federal

NIST Small Business Cybersecurity Act Becomes Law
On August 14, the NIST Small Business Cybersecurity Act was signed into law. The law requires NIST to disseminate resources to help small businesses identify and manage cybersecurity risks. The new law emphasizes promoting awareness of basic controls, implementing a workplace cybersecurity culture, and managing third-party stakeholder relationships.

Vice President Pence Calls on Congress to Create New Cyber Agency
On July 31, while speaking at the Department of Homeland Security Cybersecurity Summit, Vice President Mike Pence called on Congress to pass legislation before the end of the year that would create the Cybersecurity and Infrastructure Security Agency under the Department of Homeland Security. He emphasized the country's need for "a central hub for cybersecurity" and stated that the agency would "bring together the resources of our national government to focus on cybersecurity."

Legislative—States

California Enacts Consumer Privacy Act
On June 28, California's governor signed the California Consumer Privacy Act of 2018 into law. The law will require companies to follow restrictions on data monetization business models; accommodate rights to access, deletion, and porting of personal data; update their privacy policies; and be subject to additional penalties and liquidated damages. The law goes into effect on January 1, 2020. For more information, see our Jones Day *Commentary*.

Eight States Enact or Amend Data Breach Notification Laws
Since June 1, several states have enacted or amended their data breach notification laws:

- On June 1, Alabama's new data breach notification law became effective. 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.

- On June 2, amendments to Oregon's data breach notification law became effective. The amendment requires that an entity provide notification of a breach of security not later than 45 days after discovery. 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.

- On July 1, South Dakota's new data breach notification law became effective. 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.

- On July 20, amendments to Arizona's data breach notification law became effective. The law expands the definition of "personal information," requires individual and regulatory notification within 45 days of a breach, and broadens the risk-of-harm provision by allowing covered entities to forego individual or regulatory notification if it is determined the breach is unlikely to result in substantial economic loss to affected individuals.

- On August 1, amendments to Louisiana's data breach notification law became effective. Covered entities are now required to notify affected individuals of a data breach no later than 60 days from the discovery of the breach. If the notice is delayed for purposes of a law enforcement investigation or to determine the scope of the breach, prevent further disclosure, or restore data system integrity, the law requires that a covered entity notify the state attorney general of the reasons for the delay in writing within the 60-day notification period. The amendments expand the definition of "personally identifiable information" to include an individual's name along with a passport number or biometric data.

- On September 1, amendments to Colorado's data breach notification law became effective. Colorado has broadened the definition of "personally identifiable information," expanded the notification requirements to include notice to the state attorney general under certain circumstances, and imposed a 30-day deadline to notify affected individuals.

- On August 3, Ohio amended its data breach notification law to provide 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, which must "reasonably conform" to certain industry-recognized frameworks. Companies must also tailor their cybersecurity programs to the company's size and complexity, the nature of the company's activities, the nature of the personal information, the cost and availability of tools to improve information security controls, and the company's resources. Finally, the company's cybersecurity measures must "reasonably conform" to certain industry-recognized frameworks. The amendments will go into effect on November 2, 2018.

- Effective January 1, 2019, Vermont has amended its data breach notification law to impose new data breach notification requirements on "data brokers," defined as a business or business unit that "knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." The law does not significantly modify Vermont's generally applicable data breach notification statute but will require data brokers to report any "data broker security breaches" to the Vermont Secretary of State as part of an annual registration process.

Canada

Canadian Federal Government Unveils New Cyber Security Strategy
In June, the Canadian federal government issued a new National Cyber Security Strategy. The strategy was based in part on the results of the government's Cyber Review, which took place from 2016–2018. The new strategy emphasizes detection, deterrence, and prosecution of cybercrime. Accordingly, the Royal Canadian Mounted Police plans to add new cyber investigators who will handle future reports of illegal activity online and liaise with foreign partners to identify potential threats.

Royal Bank of Canada Invests $2 Million in Cybersecurity Partnership with Ben-Gurion University
On June 26, the Royal Bank of Canada ("RBC") invested $2 million in Ben-Gurion University's Cyber-Security Research Center. RBC's investment will fund the development of adversarial artificial intelligence aimed at mitigating cybersecurity risks. The collaboration aims to further develop the resilience of AI and machine learning for use in facial and speech recognition as well as fraud, malware, and cyber issue detection.

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

[Return to Top]

Latin America

Argentina

Argentina's Agency of Access to Public Information Issues Data Protection Resolution
On July 23, the Agency of Access to Public Information *(Agencia de Acceso a la Información Pública)* issued Resolution 47/2018, which contained guidelines on security measures for data controllers and processors to preserve the integrity and security of data, implement access controls, prevent data destruction, and prevent personal data breaches (source document in Spanish). These security measures were issued to comply with international standards for protection of personal data.

Senators Demand that Social Media Representatives Attend Senate Sessions
On August 15, senators of the Argentinian Justice and Criminal Matters, Social Media, and Freedom of Speech Commissions (*Comisiones de Sistemas, Medios de Comunicación y Libertad de Expresión y de Justicia y Asuntos Penales*) demanded that representatives for social media companies attend Senate sessions to debate a draft bill addressing data protection on social media platforms and proposing penalties for identity theft or privacy violations on these platforms (source document in Spanish).

Brazil

Brazil Enacts General Data Protection Law
On August 14, Brazil's president enacted the Brazilian General Data Protection Law under which personal data will be protected regardless of how it is collected or stored (source document in Portuguese). The bill established that personal data may be processed under only 10 scenarios, which included: express consent, compliance with legal obligation, protection of life or physical integrity, performance of a lawful agreement, or in the legitimate interest of the entity responsible for the data processing or a third party. The president vetoed a proposed regulation that would have created a National Data Protection Authority (*Autoridade Nacional de Proteção de Dados*) to oversee data protection regulation. For information, please see our Jones Day *Commentary*.

Chile

Chile Holds First Meeting of Interministerial Committee on Cybersecurity
On June 12, Chile carried out the First Interministerial Cybersecurity Committee (*Comité Interministerial de Ciberseguridad*) (source document in Spanish). Following up on the "National Cybersecurity Policy" (*Política Nacional de Ciberseguridad*) issued by the previous administration, and as part of the "Administration 2018-22," the Vice Ministers of Defense, Foreign Affairs, Finance, and Telecommunications, among others, reunited to implement and reinforce the pending cybersecurity measures. The committee will issue proposed operative and legislative measures.

Chile Approves New Strategies on Cybersecurity
On August 13, the Chilean House of Representatives (*Cámara de Diputados de Chile*) approved three resolutions to develop Chile's data privacy regulations in connection with national security matters (source document in Spanish). The approved resolutions included the implementation of public policies on cybersecurity; the establishment of protocols, policies, programs, and laws to increase the cybersecurity of banks and financial institutions' online platforms; and the adoption of new measures to maximize cybersecurity requirements on national security matters.

Colombia

Data Protection Authority Chairs 6th International Personal Data Protection Congress
On June 6, the Colombian Industry and Commerce Superintendence (*Superintendencia de Industria y Comercio*) carried out the 6th International Personal Data Protection Congress, which included experts from countries such as Canada, the United States, Uruguay, Argentina, Brazil, and Mexico (source document in Spanish). The Congress discussed the global impact of the European General Data Protection Regulation and how to achieve a joint regulation between nations.

Industry and Commerce Superintendence Provides Database Update
On July 12, the Superintendence of Industry and Commerce issued a notice that 80 percent of legal entities required to register their database with the Superintendence have done so (source document in Spanish). All nonpublic legal entities must register their database before November 30.

Mexico

Mexico Hosts Second Pacific Alliance Fintech Forum
On June 21, Mexico City hosted the second Pacific Alliance Fintech Forum, focused on development and regulation of the Fintech industry in the Latin American region (source document in Spanish). Topics included operational requirements, financial inclusion, financial innovation, and money-laundering prevention.

Federal Commission on Regulatory Improvement Issues Two Drafts of Rules and Provisions for Financial Technology Institutions
On August 6 and 7, the Federal Commission on Regulatory Improvement (*Comisión Federal para la Mejora Regulatoria*) issued two drafts of rules and provisions for Fintech institutions. The first draft, General Rules Regarding Article 58 of the Law to Regulate Financial Technology Institutions, establishes a legal framework for Fintech institutions addressing anti-money laundering and counter-financing of terrorism (source document in Spanish). The second draft, General Provisions for Financial Technology Institutions, regulates registration and operating requirements for Fintech institutions (source document in Spanish).

INAI Launches Public Sector Privacy Notice Generator
On August 18, the National Institute for Transparency, Access to Information and Personal Data Protection ("INAI") issued Resolution Number INAI/228/18, which launched the Public Sector Privacy Notice Generator, an online tool that allows data controllers to issue their own privacy notice without being a specialist in data protection matters (source document in Spanish).

Paraguay

National Minister of Information and Communication Technologies Releases Electronic Identity Service for Citizens
On July 23, the National Secretary of Information and Communication Technologies (*Secretaria Nacional de Tecnologías de la Información y Comunicación*) released the Electronic ID (*Identidad Electrónica*), a portal that allows citizens to perform online procedures with the government (source document in Spanish). Users can query or download information related to a citizen's profile, birth certificate, marriage certificate, academic level, and administrative judicial precedents.

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 Rules on Joint Controllership of Social Media Platforms
On June 5, the Court of Justice of the European Union ("CJEU") adopted a judgment in Case C-210/16 stating that an administrator of a fan page on a social media platform must comply with EU data protection rules because both the administrator and the social media platform act as joint controllers in processing the data of webpage visitors.

European Court of Justice Rules on Definition of "Controller" in Context of Religious Communities
On July 10, the CJEU adopted a judgment in Case C-25/17 where it considered whether a religious community, such as the Jehovah's Witnesses, is a controller, jointly with its members who engage in preaching, for the processing of personal data in the context of door-to-door preaching. First, the court determined that door-to-door preaching does not fall within exceptions under EU law to the rules governing protection of personal data. Second, the court found that personal data collected in the course of door-to-door preaching is governed by EU data protection rules.

European Parliament

European Parliament Asks for Suspension of EU-US Privacy Shield
On July 5, the European Parliament published a press release on a nonbinding resolution, asking the European Commission to suspend the Privacy Shield Framework. The EU-US Privacy Shield provides a mechanism to safeguard transfers of personal data from the European Union to the United States. In the wake of highly publicized data breaches, the European Parliament voted to suspend the EU-US Privacy Shield deal unless the United States complies with EU data protection rules by September 1. This was a nonbinding resolution, and the Privacy Shield Framework remains in effect.

European Commission

EU Negotiators Reach Political Agreement on Free Flow of Non-Personal Data in Digital Single Market
On June 19, the European Parliament, Council, and European Commission reached a political agreement on new rules to allow non-personal data to be stored and processed anywhere in the European Union without unjustified restrictions, supporting the creation of a competitive data economy within the Digital Single Market. The rules will allow for the free flow of non-personal data across borders, availability of data for regulatory control, and creation of codes of conduct for cloud service providers.

European Union and Japan Agree to Create World's Largest Area of Safe Data Flows

On July 17, the European Union and Japan agreed to recognize each other's data protection systems as "equivalent," which would allow personal data to flow safely between the European Union and Japan. The next step is for each side to adopt the adequacy finding. For the European Union, this involves obtaining an opinion from the European Data Protection Board and approval from a committee composed of representatives of the EU Member States. If approved, this mutual adequacy arrangement would create the world's largest area of safe transfers of data based on a high level of protection for personal data.

European Data Protection Supervisor

EDPS Publishes Opinion on EU Proposal Regarding Reuse of Public-Sector Information
On July 10, the European Data Protection Supervisor ("EDPS") released its opinion on the proposal of the European Parliament and the Council on the reuse of public-sector information ("PSI"). The PSI Directive aims at facilitating the reuse of PSI throughout the European Union by harmonizing the basic conditions that make PSI available to reusers and enhancing the development of community products and services based on PSI. The opinion makes recommendations to clarify the relationship and coherence of the PSI Directive with the GDPR.

EDPS Issues Opinion on EU Proposal Amending Directive 2017/1132 Regarding Use of Digital Tools and Processes
On July 26, the EDPS issued an opinion, in response to a consultation by the European Commission, regarding its proposal on the use of digital tools and processes in company law. The EDPS welcomed the Proposal and shared the Commission's views that the use of digital tools may provide for more equal opportunities for companies while recognizing that increased access to personal data must be accompanied with effective measures to prevent unlawful or unfair processing of data.

EDPS Publishes Opinion on EU Proposal for Regulation Strengthening Security of EU Citizens' Identity Cards
On August 10, the EDPS issued an opinion outlining its position on the Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of: (i) identity cards of EU citizens; and (ii) residence documents issued to EU citizens and their family members exercising their right of free movement. According to the EDPS, the proposal does not sufficiently justify the need to process two types of biometric data (facial images and fingerprints) in this context because the goal pursued could be achieved using a less-intrusive approach.

European Union Agency for Network and Information Security

ENISA Publishes Annual Incident Report
On July 9, the European Network and Information Security Agency ("ENISA") published its annual report detailing significant security incidents in 2017 affecting the European electronic communications sector. The incidents are reported to ENISA and the European Commission, pursuant to Article 13a of the 2009/140/EC Framework Directive, by the National Regulatory Authorities of the EU Member States.

Belgium

Belgium Adopts New Privacy Law Implementing GDPR
On July 19, the Belgian Federal Parliament adopted a law on the protection of physical persons with regard to the processing of personal data (source document in French and Dutch). The law implements Belgian-specific rules and exceptions allowed under the GDPR. It complements the institutional law adopted on December 3, 2017, establishing the Belgian Data Protection Authority. It enters into force on the day of its publication in the official journal.

Belgium Allows Class Actions for GDPR Infringements
On July 19, the Belgian Federal Parliament adopted a law allowing class actions in Belgium for GDPR infringements (source document in French and Dutch). Class actions in Belgium are open not only to consumers but also to small and medium-size undertakings. The law still needs to be published in the official journal, but the provision about class action for GDPR infringements will apply retroactively as of May 25.

France

France Adapts its Legislative and Regulatory Framework to GDPR
On June 20, France adopted a law revising the French data protection framework (resulting from law 78-17 of January 6, 1978) to incorporate requirements under the GDPR (source document in French). France also adopted a complementary decree on August 1 to adjust regulatory implementation measures originally set forth on June 2, 2005. The new French regulatory framework on data protection contains rules for specific types of data processing activities.

CNIL Issues 2018 Inspection Policies
On July 2, the French Data Protection Authority ("CNIL") set out its priorities for its 2018 inspections to monitor compliance with data protection laws (source document in French). Key themes will include the treatment of job applicant data and documentation requested by real estate companies. The CNIL

announced it would use the European inter-agency cooperation mechanisms introduced by the GDPR.

French Members of Parliament Call for Cyber Defense Act
On July 4, two French Members of Parliament issued a parliamentary report on cyber defense (source document in French). The members stated the resources dedicated to cyber defense were insufficient and that French legal tools to protect IT systems and data sovereignty were defective. The members called for new legislation to address these concerns.

ANSSI and DSAC Strengthen Cooperation in Digital Security
On July 13, the French Network and Information Security Agency ("ANSSI") and the French Directorate for Civil Aviation Safety ("DSAC") signed a letter of intent to cooperate in protecting the civil aviation sector from cyberattacks (source document in French). The agreement requires the organizations to exchange information regarding security incidents and identify safety requirements for aviation software and communications equipment.

CNIL Adopts Five New Methods of Reference in Health Care Sector
On July 16, the CNIL adopted five new Methods of Reference (MR-001 to MR-005) for the health care sector to simplify compliance procedures when processing personal data for health research purposes (source document in French). Data controllers that process personal data in compliance with a Method of Reference will not be required to obtain prior authorization from the CNIL.

CNIL Fines Video Streaming Company Up to €50,000
On July 24, the CNIL fined a company operating in the video streaming sector up to €50,000 for inadequate security (source document in French). The company experienced a data incident in 2016 affecting approximately 82.5 million email addresses. The CNIL determined that the company lacked security measures, such as the use of encryption when storing the credentials of administrative accounts or the use of VPN for remote connections.

CNIL Explains Conditions Under Which Consent is Validly Obtained
On August 3, the CNIL issued a press release to explain the conditions under which data controllers may obtain valid consent from data subjects when relying on consent as a legal basis for processing personal data (source document in French). This announcement does not change the notion of "consent" but does provide additional guarantees, notably in the context of consent by minors.

CNIL Issues Guidance for Responding to Right-of-Access Request
On August 8, the CNIL provided guidelines for responding to a right-of-access request (source document in French). The CNIL requires a data controller to respond to a right-of-access request free of charge within one month or, where the request is complex, within two additional months. The data controller must inform the data subject of a decision not to answer his or her request.

CNIL Provides Guidance on Formalities in Relation to Health Data Processing in Health Research Sector
On August 20, the CNIL provided guidance on the measures to be taken by health researchers who modify the initial purposes for data processing (source document in French). A significant change in the purposes for data processing may require prior authorization from the CNIL in certain circumstances (such as research involving the human body). Health research is one of the few exceptions where the CNIL still requires authorization prior to implementation of data processing.

Germany

Administrative Court Bayreuth Confirms that Use of Custom Audience on Social Media Requires Consent of Data Subjects
On June 15, the Bavarian Data Protection Authority ("DPA") published a press release stating that the Administrative Court of Bayreuth confirmed in a preliminary injunction the opinion of the Bavarian DPA on the use of a custom audience on social media (source document in German). The court confirmed that the processing of personal data in connection with a custom audience requires the individual's consent.

German DPAs Publish "Must-List" for DPIAs; Bavarian DPA Publishes Comprehensive Guidance on DPIAs
On June 27, the *Datenschutzkonferenz*, which is the consensus of all German DPAs, published a "must-list" for data protection impact assessments ("DPIA") (source document in German). The document contains a comprehensive list of processing activities, their fields of application, and examples of activities that require a DPIA. The Bavarian DPA also published comprehensive guidance, case studies, and links to additional information for carrying out a DPIA and the necessary risk analysis (source document in German).

Italy

GPS Systems and Privacy by Design
On June 28, the Italian DPA prohibited an employer from any further processing of data collected through geolocation devices installed in company vehicles. The DPA also required the geolocation service provider

to render its services fully compliant with the GDPR. The GDPR violations included not informing data subjects about the continuous monitoring of their working activity and monitoring non-work activities.

Italian DPA Approves Inspection Plan for Second Semester of 2018
On July 26, the Italian DPA approved the inspection plan for the second semester of 2018. The plan is the first approved after the GDPR went into effect. The Italian DPA will focus mainly on processing of personal data carried out by large-scale databases, security measures implemented by banks, and telemarketing activity. The DPA will assess compliance with the GDPR's requirements for privacy notices, prior consent, data retention period, and the designation of a data protection officer.

The Netherlands

Dutch Tax Authority Unlawfully Processes National Identity Numbers
On July 6, the Dutch DPA showed in a study that the Dutch Tax Authority has no legal basis to use the national identity number ("BSN") in the VAT identification number of self-employed persons with a sole proprietorship (source document in Dutch). The Dutch tax authority has to end the infringement as soon as possible or be subject to potential enforcement measures.

Dutch DPA Fines Bank for Failure to Comply with Right of Access
On August 9, the Dutch DPA fined a Dutch bank €48,000 for its failure to comply with a data access request from one of its customers (source document in Dutch). The customer made the initial request in 2016 and filed an enforcement request with the DPA when the bank failed to comply. The DPA granted the bank two months to comply, warning that the bank would receive an administrative penalty of €12,000 for each week that it failed to comply. The bank provided the requested information at the end of the two-month period, resulting in €48,000 in penalties, which the bank appealed.

Spain

Spanish DPA Issues Guidance on Managing and Notifying Security Breaches Under GDPR
On June 19, the Spanish DPA published the guidelines for managing security breaches and providing notification in compliance with the GDPR (source document in Spanish). The document addresses detection and identification of security breaches, steps to respond to the breach, and notifications to supervisory authorities. This guide applies to small, medium, and large Spanish businesses, as well as to data controllers of public administrations involved in the tasks of managing security breaches.

Spanish Parliament Approves Emergency Royal Decree Law to Enforce GDPR
On July 27, the Spanish parliament approved an emergency Royal Decree Law to regulate enforcement procedures for violations of the GDPR in Spain (source document in Spanish). Although the GDPR is already applicable in Spain, the Royal Decree Law regulates procedures for conducting investigations of potential infringements and imposing sanctions. The Royal Decree Law went into effect on July 31, 2018, and will be in force until the new Spanish Organic Law is passed in Spain.

Spanish DPA Publishes Guide on Processing Data Captured by Video Cameras
On June 29, the Spanish DPA published a guide on the processing of data captured though cameras in accordance with the GDPR (source document in Spanish). The guide addresses the GDPR principles affected by the processing of images captured by video cameras for security or other purposes.

United Kingdom

ICO Fines Social Media Company £500,000
On July 10, the Information Commissioners' Office ("ICO") issued a Notice of Intent to issue a monetary penalty of £500,000 on a social media company. The ICO determined that the company failed to safeguard its users' personal data when providing the data to a third party and failed to be transparent with users about the use of their data by third parties. The ICO issued this notice on public interest grounds and will hear representations from Facebook before issuing a final decision.

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 Expresses Concerns over Potential Data Breach of Online Survey Company
On July 7, the Office of the Privacy Commissioner for Personal Data ("Privacy Commissioner") issued a press release regarding a potential breach of personal data by an online survey company (source document in Chinese). The Privacy Commissioner is currently investigating the incident. The Privacy

Commissioner recommends that individuals or organizations potentially affected by this data breach report it to the Privacy Commissioner and inform the Privacy Commissioner about the mitigation measures they are implementing in response to the incident.

Privacy Commissioner Issues Best Practice Guide on Privacy Management Program
In August, the Privacy Commissioner issued a revised guide of best practices for implementing a privacy management program ("PMP"). The Guide is a revised version of the version published in 2014 and contains more concrete examples, charts, questionnaire templates, and checklists. The Privacy Commissioner encourages organizations to develop their own PMP to incorporate personal data protection into corporate governance responsibilities throughout the organization, including the boardroom.

Privacy Commissioner Completes Compliance Check on Social Media Data Incident
On August 22, the Privacy Commissioner issued a press release announcing the completion of its compliance check into suspected misuse of users' personal data on a social media platform. The compliance check found no evidence that any account holders in Hong Kong were affected by the incident but recommends that social media operators adopt a culture of data protection.

Privacy Commissioner Issues Charges Against Telecommunications Company for Direct Marketing Violations
On August 22, the Privacy Commissioner issued a Media Statement announcing two charges against a telecommunications company under the Personal Data (Privacy) Ordinance ("PDPO") for failing to comply with an individual's request to opt out of direct marketing, contrary to section 35G(3) of the PDPO. The company pleaded guilty to both charges and was fined HK$20,000 in total, or HK$10,000 for each charge.

Japan

Final Agreement to Establish Framework to Easily Transfer Personal Data between Japan and EU
On July 17, the Personal Information Protection Commission of Japan and the European Commission issued a Joint Statement announcing that they reached a final agreement to establish a framework to transfer personal data between Japan and the European Union.

Singapore

PDPC Issues Discussion Paper on Artificial Intelligence and Personal Data
On June 4, Singapore's Personal Data Protection Commission ("PDPC") issued a discussion paper presenting a preliminary analysis of the issues related to personal data in the commercial development and use of artificial intelligence solutions. The paper addressed ethical, governance, and consumer protection issues and proposed an accountability-based framework for businesses to implement when using artificial intelligence for commercial purposes.

PDPC Announces Restrictions on Use of National Identification Numbers
On August 31, Singapore's PDPC announced that organizations are expected to stop collecting, using, or disclosing customers' national identification numbers when not required under law or necessary to verify an individual's identity to a high degree of fidelity. The PDPC issued guidelines to assist organizations on the appropriate use of national identification numbers and alternative forms of identification.

People's Republic of China

Committee Publishes 24 New Draft Technical Standards for Public Comment
On June 11, the National Information Security Standardization Technical Committee published 24 new draft technical standards for public comment (source document in Chinese). These draft standards would govern critical information infrastructure operators, digital systems for automobiles, industrial control systems, evaluation of personal data security, Bluetooth security, and application of passwords for digital documents.

MPS Publishes Draft Regulations on Cybersecurity Multi-Level Protection Scheme for Public Comment
On June 27, China's Ministry of Public Security ("MPS") published draft Regulations on a Cybersecurity Multi-Level Protection Scheme for public comment (source document in Chinese). The draft Regulation updates the details of implementing a multi-level protection scheme for cybersecurity, including classifying the internet levels and setting out the duties for network operators and governments.

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 Second Quarterly Report

On July 31, the Office of the Australian Information Commissioner published its second quarterly report on data breach notifications received pursuant to the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth). The report analyzes 242 notifications that the Information Commissioner received. Top causes of data breaches reported include malicious or criminal attacks (59%), human error (36%), and system faults (5%).

Australia Extends Deadline to Opt Out of My Health Records

On August 10, the Minister for Health announced an extension until November 15 for Australians to opt out of having a My Health Record automatically created for them. My Health Records is an online summary of an individual's health information, such as medicines they are taking and treatment they are undergoing, which health care providers will be able to view in accordance with an individual's access controls. The Office of the Australian Information Commissioner will regulate the handling of personal information in My Health Records in accordance with the My Health Records Act 2012, including investigating any complaints about the mishandling of health information.

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

[Return to Top]