JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 22 | May 2019 Jones Day

GLOBAL PRIVACY & CYBERSECURITY UPDATE

Jones Day Cybersecurity, Privacy & Data Protection Lawyer Spotlight:
Jennifer C. Everett

As data privacy and security regulations are on the rise in the United States, workplace compliance is at the forefront for employers. With a background in labor & employment law, Jennifer Everett is a senior associate based in Washington, D.C., with 10 years of experience advising institutional clients on employment, privacy, and cybersecurity compliance matters.

Jennifer's practice focuses on advising U.S. and international companies on developing and maintaining sustainable privacy and cybersecurity governance programs. Jennifer routinely counsels clients on strategic compliance with U.S. and global privacy and cybersecurity laws and enterprise-wide cyber risk management. She helps companies implement effective cross-border data management programs and negotiates data provisions in complex commercial agreements.

Jennifer also regularly counsels employers on privacy and cybersecurity matters in the workplace. This includes counseling employers on privacy and data protection related to employee monitoring, workplace investigations, personal device (BYOD) policies, employee background checks, and e-discovery.

United States

Regulatory—Policy, Best Practices, and Standards

NIST Director Discusses Future Development of

PRACTICE DIRECTORY

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

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

HOT TOPICS IN THIS ISSUE

Cybersecurity Framework
On March 4, the director of the National Institute of Standards and Technology ("NIST") discussed NIST's Cybersecurity Framework at the annual RSA conference. Acknowledging the Framework's increasing popularity over the last few years in both the private and public sector, the director announced that NIST will focus on expanding its use by federal agencies and small businesses. He also reemphasized NIST's continuing commitment to developing the Framework to keep up with technological advancements.

Regulatory—Consumer and Retail

IPEC Publishes Annual Intellectual Property Report
On February 4, the Office of the U.S. Intellectual Property Enforcement Coordinator ("IPEC") issued its Annual Intellectual Property Report to Congress. The report described efforts within the Executive Branch to promote the protection of intellectual property rights within and outside the United States, including the protection of trade secrets against cybercrime and cyber espionage. The report also discusses engagement with U.S. trading partners on intellectual property issues, legal authorities to protect against unfair trade practices, expanded law enforcement cooperation, and various intellectual property enforcement activities pursued by federal agencies.

FTC Launches Task Force to Monitor Competition in Technology Markets
On February 26, the Federal Trade Commission ("FTC") announced the creation of the Technology Task Force, which aims to monitor competition in U.S. technology markets, investigate any potential anticompetitive conduct, and take enforcement actions when warranted. The task force is intended to help enhance the agency's focus on competition in technology-related sectors of the economy, including markets in which online platforms compete.

Social Networking Provider Agrees to Record $5.7 Million COPPA Settlement
On February 27, the provider of a video social networking music application agreed to pay a record $5.7 million to settle FTC claims that the company illegally collected personal information from children. This is the largest civil penalty ever obtained by the Commission in a children's privacy case. The FTC's complaint alleged that the company violated the Children's Online Privacy Protection Act ("COPPA"), which requires that websites and online services directed to children obtain parental consent before collecting personal information from users under the age of 13. The operators allegedly knew children were using the app but nonetheless failed to seek parental consent before collecting names, email addresses, and other personal information from users under the age of 13.

Data Flows

Ecuador Announces Drafting of Data Protection Law

UK Government Plan to Recognize Existing EU Data Transfer Methods

Australia Announces Proposals to Amend Privacy Act

RECENT EVENTS

Jones Day Hosts Fourth Annual Latin America Privacy & Cybersecurity Symposium
On May 16-17, Jones Day hosted its Fourth Annual Latin America Privacy & Cybersecurity Symposium, bringing together privacy professionals, data protection agencies, and policymakers to discuss new legal obligations and trends in cybersecurity and data privacy in the region. The Symposium addressed Brazil's new General Data Protection Law, compliance obligations and best practices for companies in the region, and privacy and security issues related to data-driven initiatives, including fintech, artificial intelligence, and blockchain.

RECENT AND UPCOMING SPEAKING ENGAGEMENTS

Global Privacy & Cybersecurity Law Update, Dallas Bar Association Technology Summit, Dallas, Texas (September 2019). **Jones Day Speaker**: Jay Johnson

Industrial IoT, Privacy, Security, Risk 2019, Las Vegas, Nevada (September 2019). **Jones Day Speaker**: Mauricio Paez

Building a Cybercrime Prosecution: Law Enforcement and Corporate Perspectives (with DOJ and FBI), MIT Applied Cybersecurity Professional Education Program, Cambridge, Massachusetts (June 2019). **Jones Day Speaker**: Lisa Ropple

Privacy Developments After the GDPR: Use of Monitoring Software, Investigations and Data Access,

FTC Releases 2018 Privacy and Data Security Update

On March 15, the FTC released its annual report highlighting the agency's work in privacy and data security in 2018. The FTC highlighted several of its 2018 enforcement actions against technology companies, including a settlement against a mobile payments company regarding the privacy settings in the company's mobile application, an expanded settlement with a ride-sharing company to resolve data security and privacy allegations, and an enforcement action against a supplier of children's products under COPPA.

Regulatory—Financial

SEC Announces Changes to Form N-PORT Submissions

On February 27, the Securities and Exchange Commission ("SEC") announced that the submission deadlines for registered investment companies filing nonpublic monthly reports on Form N-PORT will be extended. Reports must now be filed on a quarterly basis instead of monthly. This change is part of the SEC's effort to reduce the agency's cyber risk profile by adopting alternative reporting options that reduce the frequency and sensitivity of the data it collects.

SEC Names Gabriel Benincasa as Chief Risk Officer

On February 28, the SEC announced that Gabriel Benincasa has been named the Commission's first chief risk officer. This position was created "to strengthen the agency's risk management and cybersecurity efforts." As chief risk officer, Mr. Benincasa will coordinate the SEC's "efforts to identify, monitor, and mitigate key risks facing the Commission."

FTC Seeks Comment on Proposed Amendments to GLBA

On March 5, the FTC announced that it sought comments on proposed amendments to the FTC's Safeguards Rule and Privacy Rule under the Gramm-Leach-Bliley Act ("GLBA"). The proposal would add additional requirements for how financial institutions must protect customer information, such as requiring the encryption of customer data held or transmitted by the institution over external networks.

SEC Issues Privacy Risk Alert for Investment Advisers and Broker Dealers

On April 16, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert for investment advisers and broker-dealers. The Risk Alert identified the most frequent compliance issues related to customer privacy notices and safeguard policies for customer information under Regulation S-P, including the failure to provide initial, annual, and opt-out privacy notices and a lack of written privacy policies and procedures. The Risk Alert also discussed the lack of policies reasonably designed to safeguard customer

Eighth Annual European Labor & Employment Conference, Paris, France (May 2019). **Jones Day Speakers**: Olivier Haas, Jörg Hladjk

2019 Fourth Annual Latin America Privacy & Cybersecurity Symposium, Mexico City (May 2019). **Jones Day Speakers**: Various

Cybersecurity—Hot Topics in Due Diligence, Mergers and Acquisitions, Boston Bar Association (April 2019). **Jones Day Speaker**: Mauricio Paez

Jones Day and PKU Rule of Law Series, US and China Cybersecurity and Data Protection Regulations (April 2019). **Jones Day Speakers**: Mauricio Paez, Samir Jain, Jörg Hladjk

50 Points of Law—Civil Litigation: Major Developments & Traps for the Unwary, Massachusetts Continuing Legal Education, Boston, Massachusetts (April 2019). **Jones Day Speaker**: Lisa Ropple

50 Points of Law—What's New & Dangerous in Civil Litigation, MCLE 50th Anniversary Series, Boston, Massachusetts (April 2019). **Jones Day Speaker**: Lisa Ropple

Data Privacy, Retail Robotics & AI Conference, Northwestern University, Evanston, Illinois (April 2019). **Jones Day Speaker**: Mauricio Paez

Cybercrime, Cryptocurrency, and ICOs, Handling Your First (or Next) White Collar Crime Case, Texas State Bar, Austin, Texas (April 2019). **Jones Day Speakers**: Jay Johnson, Mark Rasmussen

Cybersecurity, Data Protection, and Blockchain Mechanisms—Techniques for Managing Arbitration Proceeding and Solving Problems, Gearing Up for Arbitration in the 21st Century, Paris, France (April, 2019). **Jones Day Speaker**: Olivier Haas

Privacy & Cybersecurity Summit: Global CCPA Implications with Booz

information, including a lack of secure login credentials, written incident response plan, or employee training, among others.

Regulatory—Energy/Utilities

DHS Expands Cyber-Training Program
On March 21, the Department of Homeland Security ("DHS") Science and Technology Directorate awarded $5.9 million to Norwich University to expand the DECIDE cyber-training platform to the energy sector. The investment will allow organizations to identify vulnerabilities and develop mitigation strategies prior to a real-life crisis to ensure that organizations receive proper training to recognize and respond to potential cyber threats.

DOE Seeks to Reduce Cybersecurity Threats in Manufacturing
On March 26, the Department of Energy ("DOE") announced up to $70 million in funding for a Clean Energy Manufacturing Innovation Institute to focus on early-stage research for advancing cybersecurity in energy-efficient manufacturing. DOE stated that the Institute "will focus on understanding the evolving cybersecurity threats to greater energy efficiency in manufacturing industries, developing new cybersecurity technologies and methods, and sharing information and knowledge" with U.S. manufacturers. The Institute also will address the education and training needed for cyber-secure automated sensors.

Regulatory—Transportation

USDOT Launches Council to Support Emerging Transportation Technologies
On March 12, the U.S. Secretary of Transportation announced the creation of the Non-Traditional and Emerging Transportation Technology ("NETT") Council within the U.S. Department of Transportation ("USDOT"). The NETT Council is charged with identifying and resolving jurisdictional and regulatory gaps that may impede the deployment of new technologies, such as autonomous vehicles. By streamlining discussion and review of these technologies, the secretary stated that the government can address "legitimate public concerns about safety, security and privacy without hampering innovation."

Congressional Committees Investigate Cyber Threat to Transportation
On February 26, the Committee on Homeland Security held a joint hearing titled "Securing U.S. Surface Transportation from Cyber Attacks" with the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation and the Subcommittee on Transportation and Maritime Security. The hearing focused on securing U.S. surface transportation, such as railroads and highways, from digital threats.

Allen at Hyundai Motor Group, Seoul, Korea (April 2019). **Jones Day Speaker**: Ed Chang

Current GDPR Topics from a DPA Perspective and GDPR Insurance as an Option to Protect Companies Against Non-Compliance Risks, IAPP KnowledgeNet, Munich, Germany (April 2019). **Jones Day Speaker**: Undine von Diemar

Technology Seminar on the Internet of Things: Legal Issues Relating to IoT Projects Roll-out, Cybersecurity, and Big Data Processing, Paris, France (April 2019). **Jones Day Speaker**: Olivier Haas

Data Localization and Privacy Regs, Cybersecurity Risk Management Council, Brussels, Belgium (April 2019). **Jones Day Speaker**: Jörg Hladjk

Cybersecurity: Three Goals for the Board of Directors, CISO Executive Network, Houston, Texas (March 2019). **Jones Day Speaker**: Nicole Perry

Cybersecurity Litigation, Massachusetts Bar Association, Boston, Massachusetts (March 2019). **Jones Day Speaker**: Lisa Ropple

"You've Been Breached, Now What?" Cyber Attack Simulation, Boston Conference on Cyber Security, Boston, Massachusetts (March 2019). **Jones Day Speaker**: Lisa Ropple

Big Data: Legal Framework and Practice, Law, Cognitive Technologies & Artificial Intelligence Study Program, Federation of Enterprises, Brussels, Belgium (March 2019). **Jones Day Speaker**: Laurent de Muyter

2019 IoT National Institute, American Bar Association, Washington, D.C. (March 2019). **Jones Day Speaker**: Jay Johnson

CIPP/E portion of the IAPP GDPR ready course, IAPP, Munich, Germany (March 2019). **Jones Day Speaker**: Undine von Diemar

Regulatory—Health Care/HIPAA

Health Records Company Settles False Claims Act Allegations

On February 6, the U.S. Attorney's Office for the District of Vermont announced that a health records company would pay $57.25 million to resolve False Claims Act allegations. The complaint alleged that the company caused its users to submit false claims to the government by misrepresenting the capabilities of its electronic health records software. The government had argued that the software did not fully incorporate the standardized clinical terminology necessary to ensure the reciprocal flow of information concerning patients and the accuracy of electronic prescriptions.

HHS Proposes New Rules for Electronic Health Information

On February 11, the U.S. Department of Health and Human Services ("HHS") proposed new rules to support seamless and secure access, exchange, and use of electronic health information. The rules seek to solve the issue of interoperability and patient access in the U.S. health care system while reducing administrative burdens on providers. The rules would allow patients to access their health information electronically through third-party software applications connected to their data.

Diagnostic Medical Imaging Company Settles PHI Breach

On May 6, HHS announced that a medical imaging services company agreed to pay $3 million to settle a breach that exposed the protected health information ("PHI") of more than 300,000 individuals. The HHS Office of Civil Rights ("OCR") determined that the company's servers had allowed uncontrolled access to its patient PHI, which permitted search engines to index and store patient data for offline viewing. OCR determined that the company did not thoroughly investigate the security incident until several months after notice of the breach and did not notify individuals in a timely manner.

Regulatory—Defense and National Security

DOD Releases Cloud Strategy

On February 4, the Department of Defense ("DOD") released its Cloud Strategy, reasserting DOD's commitment to the cloud from an enterprise perspective. The strategy focused implementation activities in two areas: (i) standing up cloud platforms that are "ready to receive data and applications"; and (ii) migrating existing applications and developing new applications in the cloud.

DOD Launches Technology-Focused Website

On April 24, DOD launched a new public website to inform members of the military industry and academia on DOD's research, development, engineering, and technological efforts. The website will highlight innovations related to

Data Breach Response—The First 72 Hours, Jones Day CLE (March 2019). **Jones Day Speaker**s: Lisa Ropple, Jay Johnson

RECENT AND UPCOMING PUBLICATIONS

Key Lessons From Australia's Notifiable Data Breach Scheme (April 2019). **Jones Day Authors**: Adam Salter, Prudence Smith

Navigating Public–Private Partnerships Around Connected Technology (March 2019). **Jones Day Authors**: Emily Tait, Aaron Charfoos, Chase Kaniecki, Jenny Whalen

Data Protection: Risk of Disruption if There Is a "No Deal" Brexit (March 2019). **Jones Day Authors**: Jonathon Little, Jörg Hladjk, Undine von Diemar, Olivier Haas

The FDA and Cybersecurity: How the Agency is Addressing Cybersecurity Risks to Medical Devices (March 2019). **Jones Day Authors**: Ian Pearson, Colleen Heisey, Todd Kennard, Samir Jain

FTC Issues Record Fine for COPPA Violation (March 2019). **Jones Day Authors**: Aaron Charfoos, Jennifer Everett, Mary Alexander Myers, Spencer Beall

Chapter, "Blockchain and the Internet of Things," American Bar Association book *The Internet of Things* (March 2019). **Jones Day Authors**: Jay Johnson, Mark Rasmussen, Kerianne Tobitsch

Chapter, "Privacy and the Internet of Things," American Bar Association book *The Internet of Things* (March 2019). **Jones Day Authors**: Mauricio Paez, Kerianne Tobitsch

Chapter, "Liability and Connected Products: Litigation and the IoT," American Bar Association book *The Internet of Things* (March 2019). **Jones Day Author**: Rick Martinez

artificial intelligence, big data analytics, autonomy, robotics, and advanced computing, among other topics.

Litigation, Judicial Rulings, and Agency Enforcement Actions

Court Gives Preliminary Approval to $50 Million Data Breach Settlement
On February 26, a federal court in Pennsylvania gave preliminary approval to a $50 million settlement related to a data breach at a restaurant chain that allegedly compromised customers' credit and debit information through malware. Plaintiffs alleged that the company failed to keep up with advancements in security measures, such as chips that would create unique codes for each customer transaction.

Home Security System Provider May Face Additional $8.4 Million in Attorneys' Fees for Alleged TCPA Violations
On March 18, attorneys for class plaintiffs requested $8.4 million dollars in attorneys' fees against a technology company that provides cloud-based home monitoring and remote control services after settling a Telephone Consumer Protection Act ("TCPA") class action for $28 million dollars. The class accused the company of using "autodialers" and "recorded messages" to call millions of cellphones, residential lines, and people on the national "do not call registry." The settlement class included more than 1.2 million consumers.

Legislative—Federal

GAO Calls for Federal Privacy Law
On February 13, the U.S. Government Accountability Office ("GAO") released a report calling for a federal privacy law based on interviews with former government officials, consumer advocates, academics, and industry professionals. The report calls for Congress to develop comprehensive internet data privacy legislation to enhance consumer protection. Specifically, GAO recommends: (i) enacting an overarching federal privacy statue; (ii) ensuring that the overseeing agency or agencies have notice-and-comment rulemaking authority; and (iii) providing authority to impose civil penalties for first-time violations.

Senators Introduce Bill Requiring Companies to Target Bias in Corporate Algorithms
On April 10, several U.S. senators introduced the Algorithmic Accountability Act, which would require companies to review artificial intelligence algorithms for bias or discrimination. The bill is aimed at companies that make more than $50 million per year, hold the data of at least one million people or devices, or primarily act as data brokers that buy and sell consumer data. The bill would also give the FTC authority to create regulations that require companies to conduct impact assessments of highly sensitive automated decision systems.

FTC Testifies Before Congress for Creation of National Privacy Law
On May 8, the FTC called for the enactment of a comprehensive federal data security law during testimony before the Senate Homeland Security and Government Affairs Subcommittee. The testimony was delivered by the Director of the Bureau of Consumer Protection and backed by a 5–0 vote approving its inclusion in the formal record. The testimony also requested that Congress permit the agency to enforce civil penalties to deter unlawful conduct, grant it jurisdiction over nonprofits and common carriers, and give it the authority to issue implementing rules under the Administrative Procedure Act.

Legislative—States

California Attorney General Plans to Publish CCPA Rulemaking Notices in Fall 2019
On February 8, the California Office of the Attorney General announced it anticipates publishing a Notice of Proposed Regulatory Action regarding the California Consumer Privacy Act ("CCPA") in fall 2019. The CCPA delays enforcement until six months after the attorney general implements regulations, or July 1, 2020, whichever comes first. The regulations will establish procedures for protecting consumers' rights and provide guidance to businesses on compliance, including on issues such as the categories of personal information, exceptions necessary to comply with state or federal law, and rules and procedures regarding consumer opt-outs and notices.

State Attorneys General Urge FTC to Update Identity Theft Rules
On February 14, attorneys general from 31 states submitted a letter to the FTC to update its identity theft rules. The FTC originally adopted identity theft rules in November 2007, prior to substantial technological

developments and growth in identity theft. The letter suggested adding a requirement that cardholders are notified by phone or email if a phone or email address associated with their account is changed, as well as changing "suspicious account activity" to include account access by new devices and repeated unsuccessful access attempts.

California Attorney General and Senator Introduce Legislation to Clarify CCPA
On February 25, California Attorney General Xavier Becerra and Senator Hannah-Beth Jackson announced legislation to strengthen and clarify the CCPA. The bill, SB 561, would remove companies' rights to cure CCPA violations within 30 days before enforcement can occur and would add a private right of action for consumers. In addition, the bill would remove requirements that the attorney general provide businesses and third parties with individual legal counsel on CCPA compliance, instead specifying that the attorney general may publish general guidance on compliance.

Mississippi Attorney General Requires Education Company to Strengthen Post-Breach Security Measures
On March 8, the Mississippi attorney general announced an Assurance of Voluntary Compliance with an education testing service provider that requires the company to strengthen its cybersecurity measures. Following a data breach involving student information, the company will be subject to various requirements, including prompt notification of a breach, encryption of students' personal information, and the appointment of a supervisor who will be responsible for security updates and patch management. Most significantly, the assurance requires the company to implement a comprehensive information security program involving annual risk assessments, privacy and cybersecurity training for employees, and designation of a chief information security officer.

Utah Passes New Internet Privacy Law
On March 28, the governor of Utah signed into law H.B.0057, Utah's Electronic Information or Data Privacy Law. The law protects data stored with third parties, including email and cloud storage providers, from unlimited government access and requires law enforcement to obtain a warrant before accessing such data.

North Dakota Passes Law Authorizing Legislative Study on Consumer Personal Data
On March 28, the governor of North Dakota signed into law HB 1485, which requires a study of issues related to personal data for one year during the 2019–2020 legislative term. The study will examine protections for consumers related to the disclosure of personal data, as well as enforcement and remedies. The study also will examine privacy laws of other states and applicable federal law. The bill originally began as a proposal with provisions similar to the CCPA, but the legislature ultimately decided to conduct a study for one year before implementing data privacy legislation. The law takes effect on August 1.

States Propose CCPA-Type Bills
In 2019, several states introduced proposed legislation similar to the CCPA, which California passed in 2018. These proposed bills are still under consideration in several states. Recent developments include:

- On February 5, Mississippi House Bill 1253 died in committee.
- On March 8, the Maryland Senate Finance Committee held a hearing on Senate Bill 613.
- On April 1, North Dakota passed House Bill 1485; however, the bill's text was replaced with an act providing for a legislative study of consumer personal data disclosures.
- On April 2, Texas left House Bill 4518 pending in the House Business and Industry Committee.
- On April 17, Connecticut amended Senate Bill 1108; the bill now establishes a task force to study possible methods for protecting consumer privacy. On April 25, the Senate passed the amended bill, and it is now under consideration by the House.
- On April 28, Washington did not pass Senate Bill 5376 as the bill did not make its way through the legislative process.
- On April 30, the Rhode Island Senate Judiciary Committee recommended Senate Bill 234 be held for

further study.

- On May 2, Texas placed its amended House Bill 4390 on its General State Calendar. The amended version of House Bill 4390 removed provisions requiring covered businesses to implement certain risk assessments and to inform individuals and the public about their data collection and processing practices.

Canada

OPC Publishes Advice on Privacy Settings
On March 5, the Office of the Privacy Commissioner of Canada ("OPC") published advice for users when choosing privacy settings for social media sites or other online services, mobile devices and mobile applications, home digital assistants, wearables, and online games. The OPC cautioned that privacy settings do not ensure privacy protection but instead help users increase control over how their personal information is handled online.

OPC Revises Policy Position on Transborder Data Flows
On April 23, the OPC revised its policy position on transborder data flows under the Personal Information Protection and Electronic Documents Act. The OPC stated that organizations must obtain individual consent when disclosing personal information across a border, and the disclosing organization remains accountable for that information after its transfer. When determining the form of consent, the organization should consider the sensitivity of the information and individuals' reasonable expectations.

The following Jones Day lawyers contributed to this section: Tony Black, Shirley Chan, Meredith Collier, David Coogan, Jennifer Everett, Levent Hergüner, Jay Johnson, Christopher Markham, Mallory McKenzie, Mary Alexander Myers, Clinton Oxford, Mauricio Paez, Nicole Perry, Lauren Timmons, Kerianne Tobitsch, and Jenny Whalen-Ball.
[Return to Top]

Latin America

Argentina

Argentina Subscribes to Convention 108
On February 28, the Agency of the Access of Public Information (*Agencia de Acceso a la Información Pública*) announced its subscription to the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (*Convención 108*) and its Additional Protocol (source documents in Spanish). The Convention 108 is the only multilateral binding instrument on data protection, which aims to protect the privacy of data owners against any misuse on data processing matters.

Brazil

Brazilian Consumer Protection Department Investigates Communications Provider's Data Privacy Breach
On February 28, the National Consumer Protection Department of the Brazilian Ministry of Justice and Public Security set up an investigation procedure against a provider of internet and mobile phone communications for allegedly using a digital tool capable of mapping users' internet browsing (source document in Portuguese). According to the Department, the provider, in conjunction with another company, allegedly violated consumer privacy by misdirecting users to an electronic address, which allegedly enabled the company to collect user navigation data.

Brazilian Government Investigates Integration of Social Media Platforms
On March 11, the Special Data Protection and Artificial Intelligence Unit of the Prosecutors' Office of the Brazilian Federal District initiated an investigation to monitor the integration of communication across social media platforms (source document in Portuguese). The investigation will determine whether the integration complies with Brazilian legislation, such as the Brazilian Federal Constitution and the Brazilian Civil Internet Framework.

Ministry of Justice Files Two Lawsuits Against Social Media Company
On March 12, the Brazilian National Consumer Protection Department of the Ministry of Justice and Public

Security filed two lawsuits against a social media company and its local affiliate (source document in Portuguese). The first lawsuit involved the sharing of data from users extracted from the Facebook Login platform through an application. The second lawsuit involved the actions of hackers, who allegedly invaded accounts of Brazilian users registered in the Facebook Platform and collected personal data.

Chile

President Announces New Law to Perform Preventive Identity Control

On March 14, the Chilean pesident announced the implementation of a program that aims to modernize Chile's security services by employing security cameras and drones for crime prevention actions and their investigations (source document in Spanish). The program authorizes the police to investigate individuals older than 14 years of age.

Colombia

Superintendence Demands Social Media Company to Strengthen Security Measures

On January 28, the Colombian Superintendence of Industry and Commerce (*Superintendencia de Industria y Comercio*) requested that, pursuant to Resolution 1321, a social media company adopt measures that guarantee the security of Colombian users (source documents in Spanish). The communication specified that the measures must ensure compliance with Colombian regulations concerning the compromise of personal data by unauthorized or fraudulent access. At the end of this period, the company must deliver an official certificate that it implemented such improvements.

Ecuador

Public Data Authority Announces Drafting of Data Protection Law

On February 3, the National Director of the Personal Data Registry (*Dirección Nacional de Registro de Datos Públicos*) expressed the need for a Personal Data Protection Law for Ecuador (source document in Spanish). The current draft provides legal tools for private institutions that manage and work with databases to ensure that their personal data processing services are responsible and ethical, and it creates an information exchange between Ecuador and other countries.

Mexico

INAI Approves Annual Program for Compliance Verification

On February 7, the National Institute for Transparency, Access to Information, and Personal Data Protection ("INAI") issued the Approval of the Annual Program for Compliance Verification with Transparency Obligations by the Government Agencies in Federal Scope (*Programa Anual para la Verificación del Cumplimiento de las Obligaciones en Materia de Transparencia por parte de los Sujetos Obligados del Ámbito Federal*) (source document in Spanish). Among other initiatives, the program seeks to provide clarity for those involved; set the type, scope, and number of verifications that will be carried out during 2019; and publicize the schedule of actions to be developed during the verification process of 2019.

INAI Issues Tool to Document Security Measures

On February 8, the INAI issued the Breaches Evaluator (*Evaluador de Vulneraciones*), which can be used as a tool to register existing and missing security measures inside an organization (source documents in Spanish). The document allows users to create several evaluations or assessments of their security measures, using 142 questions based on function of the security measure and risks of infringement at each stage of the processing of personal data.

INAI Determines Attorney General's Office Breached Data Protection Law

On February 20, the INAI announced that the Attorney General's Office failed to comply with the security obligations and the principle of liability provided in the General Law on the Protection of Personal Data held by Government Agencies (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*) (source document in Spanish). The announcement found that the office lacked a log of data processing activities or a system to ensure the safe erasure of personal data, among other violations.

INAI Requires Sanctions for Individual Responsible for Personal Data Exposure at Financial

Services Company
On February 25, the INAI stated that the Internal Control Division of the National Bank for Savings and Financial Services (*Banco del Ahorro Nacional y Servicios Financieros-Bansefi*) must sanction the individual responsible for the exposure of users' personal data on the internet during an update of its portal (source document in Spanish). The personal data was shared by certain users without the data owner's consent.

INAI and Mexican Institute of Teleservices Agree on Actions to Ensure Data Protection in Call Centers
On March 5, the INAI and the Mexican Institute of Teleservices announced the execution of a General Collaboration Agreement (source document in Spanish). The agreement covers processing of personal data in the teleservices sector and is designed to generate best practices, implement higher standards in the protection of data privacy, promote public policies, and strengthen the fulfilment of principles and duties in the private sector.

INAI and GPEN Present Results of Evaluation of Global Organizations
On March 5, the INAI and the Global Network for Law Enforcement in Terms of Privacy (*Red Global para la Aplicación de la Ley en Materia de Privacidad-GPEN*) announced the results of the Privacy Sweep 2018 (*Barrido de Privacidad 2018*) (source document in Spanish). The study analyzed the compliance of 365 organization from 18 countries with data protection laws and regulations. Results indicate that several organizations do not have pre-established processes to address complaints and queries posed by data owners and are not equipped to handle personal data security incidents and breaches properly.

The following Jones Day lawyers contributed to this section: Guillermo Larrea and Daniel D'Agostini.
[Return to Top]

Europe

European Council

Bulgarian Presidency Releases Revised Draft of Proposed ePrivacy Regulation
On February 15, the Bulgarian presidency published a revised draft of the proposed ePrivacy Regulation. The revisions cover issues such as the investigative and corrective powers for supervisory authorities, the role of the European Data Protection Board, and cooperation between relevant authorities.

European Court of Justice

Advocate General Releases Opinion on Consent to Cookies
On March 21, the Advocate General released an Opinion providing views on how to obtain valid consent to the use of cookies. The case, involving an online lottery service, is examining whether data subjects provided valid consent to online cookies when invited to unselect a pre-checked checkbox (i.e., opt-out) if they do not wish to consent to cookies. According to the Advocate General, consent is not considered valid under the GDPR and the ePrivacy Directive in this circumstance. Instead, the Advocate General stated that consent for participating in a lottery and consent for the use of cookies should be separately presented to data subjects, and the Advocate General addressed what information must be provided to users regarding cookies.

European Parliament

European Parliament Adopts the EU Cybersecurity Act
On March 12, the European Parliament adopted the EU Cybersecurity Act. The Cybersecurity Act strengthened the role of the European Union Agency for Cybersecurity ("ENISA") and established an EU-wide cybersecurity certification scheme to ensure that certified products, processes, and services sold in EU countries meet cybersecurity standards. The Council of the European Union must formally approve the Act.

European Commission

European Commission Adopts Recommendation on European Electronic Health Record Exchange Format

On February 6, the European Commission published a recommendation on the development of an exchange of electronic health records between health practitioners and hospitals across EU borders. The recommendation provides common technical specifications for the transfer of health data and states that a joint coordination process between the Commission, Member States, and stakeholders will facilitate further discussions on the format of the exchange.

European Commission Adopts Regulation on Ecodesign Requirements for Servers and Data Storage Products

On March 15, the EU Commission adopted a Regulation on Ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC and amending Commission Regulation (EU) No. 617/2013. The Regulation establishes ecodesign requirements for placing online data storage products and servers on the market.

European Data Protection Board

EDPB Adopts Guidelines on Codes of Conduct and Monitoring Bodies

On February 12, the European Data Protection Board ("EDPB") published for public consultation Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies. The guidelines aim to provide guidance and interpretative assistance in relation to the application of Articles 40 and 41 of the GDPR.

EDPB Issues Information Note on GDPR Data Transfers if No-Deal Brexit

On February 12, the EDPB issued an Information Note on data transfers under the GDPR in the event of a no-deal Brexit. The Information Note lists the data transfer instruments available to parties in the absence of an adequacy decision and states that, according to the UK government, "the current practice, which permits personal data to flow freely from the UK to the EEA, will continue in the event of a no-deal Brexit."

EDPB Provides Information Note Regarding Binding Corporate Rules

On February 12, the EDPB issued an Information Note on Binding Corporate Rules ("BCRs") for companies that use the United Kingdom's ICO as a BCR Lead Supervisory Authority. The Information Note invites companies to consider different recommendations regarding the identification of a new BCR Lead Supervisory Authority in another EU Member State. The EDPB also refers to the Working Document on the approval procedure for Binding Corporate Rules under the GDPR, which sets forth the criteria to identify a new BCR Lead Supervisory Authority.

EDPB Issues Statement on U.S. FATCA

On February 25, the EDPB issued Statement 01/2019 on the U.S. Foreign Account Tax Compliance Act ("FATCA") regarding the adverse effects of FATCA on EU citizens. The EDPB stated that it will scrutinize the existing data protection safeguards under the legislation authorizing the transfer of personal data to the U.S. Internal Revenue Service.

EDPB Issues Findings on GDPR Implementation, Cooperation, and Consistency

On February 26, the EDPB issued an overview of the implementation of the GDPR and the roles and means of the national supervisory authorities. The overview provides key statistics relating to GDPR cooperation and consistency mechanisms. Furthermore, the overview describes GDPR enforcement at a national level and finds that "the number of one-stop-shop procedures are increasing steadily" due to greater cooperation among supervisory authorities.

EDPB Releases Opinion on ePrivacy Directive and GDPR Interplay

On March 12, the EDPB adopted an opinion on the interplay between the ePrivacy Directive and the GDPR, which provides guidance on the processing activities within the material scope of the GDPR and the ePrivacy Directive, the responsibilities and powers of data protection authorities ("DPAs") under the GDPR, and the applicability of GDPR cooperation and consistency mechanisms. According to the EDPB's opinion, DPAs are competent to enforce the GDPR, even if a subset of the processing falls within the scope of the ePrivacy Directive.

EDPB Calls on EU Legislators to Accelerate Process for Adoption of ePrivacy Regulation

On March 13, the EDPB issued a statement inviting EU legislators to "intensify efforts towards the adoption of an ePrivacy Regulation." The EDPB recommends that the ePrivacy Regulation should set the same level of protection offered by the current ePrivacy Directive 2002/58/EC. In addition, the EDPB underlined that the ePrivacy Regulation must "complement the GDPR by providing additional strong guarantees for all

types of electronic communications."

EDPB Issues Statement on Use of Personal Data in Political Campaigns
On March 13, the EDPB issued a statement concerning the use of personal data in the course of political campaigns. The EDPB cited key points that political parties should respect when processing personal data in the course of electoral activities. The EDPB also declared that, to this end, data protection authorities "will make full use of their powers," as provided by the GDPR.

European Data Protection Supervisor

EDPS Announces Potential Guidelines for Assessing Proportionality
On February 25, the European Data Protection Supervisor ("EDPS") announced its intention to issue guidelines for assessing the proportionality of measures that limit the fundamental rights to privacy and the protection of personal data. The guidelines complement the EDPS Necessity Toolkit and seek to assist EU institutions with ensuring that any limitation of the fundamental right to the protection of personal data is compliant with the requirements of EU primary law.

EDPS Releases 2018 Annual Report
On February 26, the EDPS released the 2018 Annual Report, which provides insights into 2018 EDPS activities. Of note, the Annual Report highlights EDPS's efforts to prepare for the GDPR, which became fully applicable across the European Union on May 25, 2018.

European Union Agency for Network and Information Security

ENISA Publishes Study on Cybersecurity Policy Development
On March 14, ENISA published a study regarding cybersecurity policy developments with respect to autonomous agents. The study highlights a number of relevant security and privacy considerations, such as unauthorized autonomous systems, hijacking and misuse, transparency and accountability, pervasiveness, and retention and opacity of processing.

ENISA Issues Guidance and Gaps Analysis for European Standardization
On March 15, ENISA published its guidance and gaps analysis for European standardization, which explores how the standards-developing ecosystem is responding to the privacy changes. The guidance also provides insights into "state-of-the-art" privacy standards in the information security context through a relevant gap analysis.

Belgium

Private Entities Launch Action Against Exemption of Fines for Public Authorities
On March 12, the Federation of Enterprises in Belgium launched an action before the Constitutional Court to annul a provision of the Belgian privacy law of July 30, 2018, implementing the GDPR. The challenged provision provides for an exemption of fines for public authorities.

Belgian Data Protection Authority Publishes Categories of Processing Subject to Impact Assessment
On March 22, the Belgian Data Protection Authority published in the official Journal the decision of its general secretariat, which lists the categories of processing that must be subject to a data protection impact assessment under Article 35 of the GDPR (source document in French and Dutch). The list went into effect on April 1.

France

French National Cybersecurity Agency Participates in New EU Cybersecurity Competence Network called "SPARTA"
On February 18, the SPARTA consortium was launched with the support of the European Research and Innovation Framework Program. The French National Cybersecurity Agency will collaborate with SPARTA for three years. SPARTA's objective will be to "develop and implement top-tier cybersecurity research" in order to strengthen the strategic autonomy of the European Union.

CNIL Closes Proceedings Initiated Against Five Insurance Companies

On February 19, the French Data Protection Authority ("CNIL") issued decisions closing proceedings initiated last October against five insurance companies for alleged misused personal data (source document in French). After the implementation of several changes to the information systems by the challenged entities, CNIL stated that the companies had complied with formal notices and closed the proceedings.

CNIL and CADA Clarify Guidelines for Open Data
On February 21, the CNIL and the French Commission for Access to Administrative Documents ("CADA") launched a public consultation on the first part of their "practical guide" on the online publication and reuse of open data. The guide, intended for both administrations and citizens, seeks to clarify the legal framework of open data, and the observations collected will be used to amend the guide.

CNIL Closes Proceedings Against Digital Advertiser
On February 25, the CNIL closed proceedings initiated against a company in the digital advertising sector for processing personal data without legal basis (source document in French). The CNIL stated that the company complied with the formal notice issued last November by implementing a new pop-up window to obtain the consent of users and allowing the user to express his/her consent through an on/off widget for each data processing purpose, among other changes.

CNIL Releases Report on Data Processor Accountability
On March 5, the CNIL published its report on data processor accountability (source document in French). According to CNIL, surveys revealed that although data processors have become aware of the changes in light of the GDPR, there is needed improvement regarding the preparation of incident management processes and impact assessments.

Germany

Regional Labor Court Publishes Decision on Access to Investigation Data
In March, the regional labor court of Baden-Württemberg published a decision holding that a data subject's rights to access and receive a copy of personal data pursuant to the GDPR may include personal data relating to internal employee investigations. The court held that the defendant's invocation of the whistleblower protection was insufficient due its inability to offer specific facts supporting the protection.

DSK Issues Guidance on Data Transfers in Event of Brexit
On March 8, the *Datenschutzkonferenz* ("DSK"), which is the consensus body of the German Data Protection Authorities, published a resolution regarding the necessary steps for transferring data from Germany to the United Kingdom and Northern Ireland in the event of Brexit (source document in German). The resolution explained that in the event of a "Deal-Brexit," the current "deal-draft" would foresee the continued applicability of the GDPR, at least until the end of 2020, and set forth next steps in the event of a "No-Deal Brexit."

Administrative Court Rules on GPS Tracking in Employment Context
On March 19, the administrative court in Lueneburg ruled that, in the employment context, GPS tracking of company vehicles must be "necessary" and that employers must properly obtain valid and informed consent (source document in German). The court relied on GDPR Article 88 and Germany's Federal Data Protection Act in reaching its decision.

Italy

DPA Issues Decision on Wearable Devices in Workplace
On February 28, the Italian Data Protection Authority ("DPA") issued a decision clarifying a company's obligations with respect to using wearable GPS devices to monitor its employees (source document in Italian). The DPA required the company to identify specific measures aimed at ensuring the protection of its employees' dignity, retain employee data only for periods of time strictly necessary for its stated purpose, and detail the cases in which it would be necessary to access personal data.

DPA Issues Clarifications on Processing of Health Data
On March 7, the Italian DPA released clarifications on health data processing in light of GDPR principles (source document in Italian). Among other clarifications, the Italian DPA maintained that doctors are allowed to process the personal data of their patients for medical purposes without consent, provided

patients have information about processing activities, and that all health-related business operators are required to maintain detailed data processing records for all processing activities carried out in connection with patients' data.

The Netherlands

DDPA Investigates Use of Personal Data in Election Campaigns
On February 15, the Dutch Data Protection Agency ("DDPA") announced its request to political parties for information on how they process personal data during election campaigns, with a focus on third-party service providers that use micro-targeting marketing methods. The DDPA also asked administrators in charge of managing tools that help voters test their political preferences to pay close attention to requirements for processing personal data.

DDPA Disallows "Cookie Walls"
On March 7, the DDPA published its opinion on the use of "cookie walls," which is the practice by which websites condition access upon a visitor's agreement to allow tracking cookies. According to the DDPA, the use of cookie walls does not comply with the GDPR's requirement that visitors freely provide their consent.

DDPA Amends Policy on Administrative Fines
On March 14, the DDPA published guidelines amending its policy for calculating administrative fines for GDPR and other privacy-related violations (source document in Dutch). The policy sets outs the DDPA's approach to GDPR infringements, which involves assigning each provision to a specific penalty category. Of note, the DDPA retains its ability to impose fines outside the set bandwidth, and the new fine policy will be used until European guidelines for calculating fines have been accepted.

Alcohol and Drug Testing During Work Hours Allowed Only with Statutory Basis
On March 15, the DDPA announced that employers are allowed to test their employees for alcohol or drug use only if there is a specific statutory basis, such as those provided in the Dutch Aviation Act (source document in Dutch). The DDPA stated that the results of these tests qualify as sensitive personal data, which, under the GDPR, organizations do not have the right to process unless there is a statutory exception. The DDPA also stated that the relevant statutory basis for the alcohol and drug testing should contain sufficient safeguards to minimize the privacy impact.

Spain

SDPA Publishes Study on Effect of Fingerprinting on Citizen Privacy
On February 7, the Spanish Data Protection Agency ("SDPA") published its Survey on Device Fingerprinting, which examines the use of fingerprint identification and its impact on user privacy. The survey offers recommendations to users for minimizing potential privacy impacts and provides advice to manufacturers and developers of the technology.

SDPA Allows Communications with Customers Through WhatsApp
In March 2019, the SDPA published a resolution in a proceeding involving a data subject's claim that a mobile phone provider violated the GDPR (source document in Spanish). The data subject claimed that the company used WhatsApp to contact him about a home installation in violation of the GDPR. The SDPA dismissed the proceedings, finding that the company's actions were lawful under the GDPR as they were necessary for the execution of a contract with the data subject.

SDPA Publishes Circular on Processing of Personal Data by Political Parties
On March 11, the SDPA published its Circular examining the use of political opinion data and electronic messaging systems by political parties, federations, and coalitions (source document in Spanish). The Circular maintains that only personal data that has been "freely expressed" may be used in election campaigns and that political parties can obtain data from public sources, such as the web, but not from private messaging groups. The Circular also prohibits political parties from inferring political ideology through the use of AI techniques or big data.

United Kingdom

UK Government Plans to Recognize Existing EU Data Transfer Methods

On April 11, the UK government indicated that it will use its authority under the EU (Withdrawal) Act 2018 to implement measures to allow transfers of personal data from the United Kingdom to the European Union to continue. To that end, the government stated its intent to pass regulations to transitionally recognize: (i) all European Economic Area countries as "adequate" for the purpose of transfers of personal data from the United Kingdom, to preserve the effect of existing EU adequacy decisions; (ii) the EU standard contractual clauses; and (iii) existing binding corporate rules.

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, Sara Rizzon, Irene Robledo, Elizabeth Robertson, Lucia Stoican, and Rhys Thomas.
[Return to Top]

Asia

Hong Kong

Privacy Commissioner Publishes Investigation Report on Intrusion into Broadband Network's Customer Database
On February 21, the Privacy Commissioner published an Investigation Report in connection with a data breach of Hong Kong Broadband Network Limited's ("HKBN") network exposing the data of approximately 380,000 customers and service applicants. The Report found that HKBN failed to adequately review its system migration efforts, update security patches and encryption for the breached database, and implement a reasonable retention period for former customers' personal data.

Privacy Commissioner Releases Study Report on Implementation of Privacy Management Program by Data Users
On March 5, the Privacy Commissioner released the "2018 Study Report on Implementation of Privacy Management Programme by Data Users," which examines the Privacy Management Programmes of 26 organizations from various sectors. The study reviews the organizations' commitment to data privacy protection and recommends actions organizations should take to comply with the Personal Data Privacy Ordinance.

People's Republic of China

Committee Proposes Amendments to Personal Information Security Specification
On February 1, the National Information Security Standardization Technical Committee issued draft amendments to GB/T 5273-2017, the "Information Security Technology—Personal Information Security Specification" (source documents in Chinese). The Specification, which went into effect on May 1, 2018, governs the protection of personal information and provides guidance on the interpretation of China's Cybersecurity Law. The amendments introduced additional requirements on data controllers regarding third-party access and user consent to data collection and targeted advertising.

Committee Solicits Opinions on Proposed Social Networking Specification
On February 1, the National Information Security Standardization Technical Committee published a notice soliciting opinions on the draft "Information Security Technology–Specification for the Management of Information Identification on Social Networking Platform" (source document in Chinese). Among other obligations, the Draft Specification seeks to impose a requirement on social network platforms to formulate strategies on the management of user identity and provides guidance on managing processes for the generation, usage, transmission, storage, and destruction of identifying information.

Regulators Publish Joint Announcement on Application Security Certification
On March 15, the State Administration for Market Regulation and the Cyberspace Administration of China jointly published an Announcement on the Implementation of App Security Certification (source document in Chinese). The announcement creates a security certification scheme for mobile applications, which will assist operators of mobile applications in demonstrating their compliance with the personal data collection and use provisions of GB/T 5273-2017 (source document in Chinese). The China Cybersecurity Review Technology and Certification Center is designated as the certification body and is responsible for appointing technical testing agencies to conduct testing and inspection in the certification process.

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

Zhang.
[Return to Top]

Australia

Federal Government Announces Proposals to Amend Privacy Act

On March 24, the federal government announced that it will introduce legislation amending the Privacy Act in the second half of 2019. The amendment proposes increased penalties for Privacy Act breaches to the greater of AUD $10 million, three times the value of any benefit obtained through the misuse of information, or 10 percent of a company's annual domestic turnover, whichever penalty is greater. The legislation also would allow the Office of the Australian Information Commissioner to issue infringement notices and impose monetary penalties, and it would require social media companies to stop using or disclosing personal information if requested.

Senate Economics Legislation Committee Releases Report on New Consumer Data Right Bill

On March 21, the Senate Economics Legislation Committee released its report on the draft bill that would establish the Consumer Data Right ("CDR"), which recommends that the CDR draft bill be passed into law. The Committee noted that the CDR draft bill has general support from interested parties. However, parties providing submissions maintained concerns about the privacy arrangements in the draft bill, including the potential need to comply with both the Privacy Safeguards in the draft bill and the Australian Privacy Principles already in place. The draft bill will next be considered by the House of Representatives, although this consideration has not yet been scheduled. Introduction of the CDR to the banking sector in Australia is still scheduled for July 1, 2019.

Joint Parliamentary Committee Considers Law Providing Access to Communications

The Joint Parliamentary Committee on Intelligence and Security continues its inquiry into the Telecommunications and Other Legislation (Assistance and Access) Act 2018. The Act requires designated communications providers to grant access to communications on their platforms when requested by law enforcement agencies. The Act has come under criticism for weakening the privacy of all encrypted communications. The Committee's review will consider all aspects of the Act and its implementation, including a review of the amendments introduced immediately before the Act's passage on December 6, 2018.

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