JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 7 | August 2015

JONES DAY

Jones Day Attorney Spotlight: Guillermo Larrea

The growth of international business in Mexico and Central America; the rise of internet services, e-commerce, and social networks across all of Latin America; and regional concerns over data transfers, employee data processing, the use of web portals, and other data-driven developments are pushing data privacy and security to the forefront of Latin American policy agendas. Understanding the region's data privacy and security laws and attendant compliance obligations is a critical and necessary step toward minimizing risk for international and regional companies doing business there.

Resident in Jones Day's Mexico City Office, Guillermo Larrea develops compliance programs for Global 500 companies, is a prolific speaker and publisher on cybersecurity and privacy issues, and shares responsibility for coordinating the Firm's Cybersecurity, Privacy & Data Protection Practice in Latin America. His knowledge of regional data privacy and cybersecurity laws, and his experience with international data transfers, cloud-based and big data applications, and incident response and investigations, make him an invaluable resource for companies facing data privacy and security issues in the region.

EDITORIAL CONTACTS

Daniel J. McLoon
Los Angeles

Undine von Diemar
Munich

Mauricio Paez
New York

Jonathon Little
London

Kevin Lyles
Columbus

Paloma Bru
Madrid

Jay Johnson
Dallas

Olivier Haas
Paris

Adam Salter
Sydney

Anita Leung
Hong Kong

Editor-in-Chief: Anand Varadarajan

Practice Directory

HOT TOPICS IN THIS ISSUE

President Signs USA Freedom Act into Law

Brazil Completes Public Debate on Internet Civil Framework and Data Protection Bill

Article 29 Working Party Publishes Opinion Relating to Drone Use

China's National People's Congress Releases Draft Cybersecurity Law

Australian Privacy Regulator Releases Guide to Privacy Regulatory Action

United States

Policy, Best Practices, Standards, and Announcements

FBI Director Names New Associate Executive Assistant Director for FBI's Cyber-Response Branch
On May 1, the FBI Director named the former assistant director of the FBI Cyber Division, Joseph M. Demarest, Jr., to the newly established position of associate executive assistant director of the Criminal, Cyber, Response, and Services Branch. Demarest will act as the Chief Operations Officer for the division.

FTC Outlines Data Breach Investigation Steps
On May 20, the Federal Trade Commission ("FTC") outlined the steps of a typical data breach investigation on its Business Blog. Following a data breach, the FTC stated that it would seek information on the circumstances surrounding the breach and would more favorably treat a company that reported a breach and cooperated with law enforcement.

FTC Releases New Data Security Guidance Document
On June 30, the FTC released new data security guidance called Start with Security, a Guide for Business to help businesses identify and prioritize security issues.

National Security and Critical Infrastructure

ODNI Releases Second Annual Report Regarding Use of National Security Authorities
On April 22, the Office of the Director of National Intelligence ("ODNI") released its second annual statistical transparency report, which presents data on the frequency with which the government made use of critical national security authorities during the 2014 calendar year.

NIST Releases Draft Privacy Risk Management Framework for Federal Information Systems
In May, the National Institute of Standards and Technology ("NIST") released a draft report titled Privacy Risk Management for Federal Information Systems. The framework "provides the basis for the establishment of a common vocabulary to facilitate better understanding of and communication about privacy risks and the effective implementation of privacy principles in federal information systems." NIST requested public comments on the draft by July 31.

Assistant Attorney General for National Security Announces Charges against Government Employee for Cyberattack on Government Computers
On May 8, the Assistant Attorney General for National Security announced that a former U.S. Department of Energy and U.S. Nuclear Regulatory Commission employee was indicted after participating in an undercover email spear-phishing campaign aimed at destroying Department of Energy computers and obtaining sensitive nuclear information.

Congressional Think-Tank Report Warns of Increased Cyber Threats to U.S. Power Grid
On June 10, the Congressional Research Service published a report titled Cybersecurity Issues for the Bulk Power System. Authored by a specialist in energy policy, the report explains that "in recent years, new threats have materialized as new vulnerabilities have come to light, and a number of major concerns have emerged about the resilience and security of the nation's electric power system." The report also considers areas for congressional action to improve grid cybersecurity.

U.S. Navy Engineer Pleads Guilty to Attempted Espionage
On June 15, 2015, a civilian engineer in the U.S. Navy pled guilty to attempted espionage in relation to his attempt to circumvent a U.S. Navy computer system to provide schematics of a new nuclear aircraft carrier to the Egyptian government. The defendant began working for the Nuclear Engineering and Planning Department at the Norfolk Navy Shipyard in February 2014 and soon thereafter made efforts to contact Egyptian officials.

NIST Announces Increased Outreach Efforts for Cybersecurity Framework
On July 1, NIST announced plans to increase outreach efforts in certain industries, both domestically and abroad, and to use the Cybersecurity Framework to standardize cybersecurity efforts across nations. NIST also explained that it has "increased outreach on regulatory alignment in the past six months" and is seeking increased interactions with small and medium businesses.

DHS Secretary Discusses Airlines and Financial Outages
On July 8, following technical outages at United Airlines, the New York Stock Exchange, and *The Wall Street Journal*, the Department of Homeland Security ("DHS") Secretary stated in a speech at the Center for Strategic and International Studies that "[i]t appears from what we know at this stage that the malfunctions at United and the stock exchange were not the result of any nefarious actor," although "we know less about *The Wall Street Journal* at this point."

Financial Services

SEC Division of Investment Management Issues Cybersecurity Guidance
On April 28, the Securities and Exchange Commission's ("SEC") Division of Investment Management released a guidance update to advise investment companies and registered investment advisers on a number of measures to address cybersecurity risks. Under the guidance, advising funds and advisers should conduct periodic cybersecurity assessments, create strategies to respond to threats, and account for obligations under federal securities laws.

American Bankers Association Provides Cybersecurity Tips for Consumers
On June 5, the American Bankers Association issued a press release outlining steps that consumers should take to protect themselves against data breaches and identity theft.

PayPal Narrows Robocalling Practices
On June 29, PayPal announced that it would narrow the robodialing provision in its user agreement following pressure from senators, the Federal Communications Commission ("FCC"), the New York Attorney General's Office, and consumer privacy groups to rethink the provisions related to robocalling. These groups took issue with the PayPal's new user agreement requiring users to receive robocalls in order to use the company's payment processing services.

FIFEC Releases Cybersecurity Assessment Tool
On June 30, the Federal Financial Institution Examination Council ("FIFEC") announced the release of an assessment tool intended to help financial institutions evaluate cybersecurity risks and preparedness.

Credit Union National Association and National Association of State Credit Union Supervisors to Co-Host Cybersecurity Symposium
On July 8, the Credit Union National Association and National Association of State Credit Union Supervisors announced that they will co-host a symposium on cybersecurity. The symposium will take place August 24–25 in Denver, Colorado, and will offer information on the state of cybersecurity in the financial industry and advice on how to bolster cybersecurity platforms.

American Bankers Association Testifies on Crime and Terrorism
On July 8, the American Bankers Association's Senior Vice President of payment and

cybersecurity policy testified before the Senate Subcommittee on Crime and Terrorism, urging Congress to enhance the banking industry's ability to share information on cybersecurity threats and to enact a national data security and notification law.

Transportation

Uber Releases New Rider Privacy Policy Disclosing Scope of Data Collection
On May 28, Uber Technologies Inc. released its new privacy policy, which took effect on July 15 and sets forth the scope of Uber's collection, use, and sharing of rider data, including location data and other information collected when a rider interacts with Uber's ride-sharing service.

EPIC Seeks FTC Investigation into Uber's Personal Data Collection Practices
On June 22, the Electronic Privacy Information Center ("EPIC") filed a complaint with the FTC requesting an investigation into Uber's data collection practices. In its complaint, EPIC asked the FTC to force Uber to end practices that are unnecessary to providing its ride-sharing service.

Health Care/HIPAA

21st Century Cures Act Regulates Medical Research under HIPAA
On July 10, the House of Representatives passed the 21st Century Cures Act to increase medical research funding and facilitate quicker access to new treatments. Among a variety of other medical research-related provisions affecting government agencies, the Act would require the Department of Health and Human Services to revise HIPAA to provide that the use and disclosure of protected health information would be treated as "health care operations" under the Privacy Rule.

Litigation, Judicial Rulings, and Agency Enforcements

Connecticut Supreme Court Denies Data Breach Coverage
On May 18, the Connecticut Supreme Court upheld a lower court's decision to deny insurance coverage to a multinational technology and consulting corporation stemming from a data breach that exposed sensitive employee data. The court found that the insurance companies did not need to cover losses tied to the data breach incident under a section of the relevant policy providing coverage for injuries caused through the publication of material that violates a person's right to privacy.

Vermont Attorney General Settles Untimely Data Breach Notification Cases
On May 19, the Vermont attorney general settled claims against a hotel chain for failing to notify Vermont residents of a security breach until six months after the breach occurred. On May 21, the Vermont attorney general announced that it settled claims against a university related to a security breach that took place in November 2013 where the university did not notify affected Vermont residents until approximately four months after the vulnerability was discovered.

Nevada Supreme Court Rules State Wiretap Law Applies to Cell Phones
On June 4, the Nevada Supreme Court ruled that the state's wiretap statute allows law enforcement to intercept cell phone calls and text messages because there are wires involved in the transmission of such communications.

Software Company Reaches Settlement over Data Breach
On June 9, 2015, plaintiffs in a class action lawsuit against a software company moved for approval of a settlement for injunctive relief. The suit arose after the company's 2013 data breach. Plaintiffs alleged that the defendant company failed to adequately disclose its security practices, and to follow its own privacy policy, in violation of California's Online Privacy Protection Act and Unfair Competition Law. Plaintiffs also stated a claim for damages under the California Data Breach Act, alleging negligence and unreasonable

delay in informing class members about the breach. In the settlement agreement, the defendant company agreed to enhance security measures and audit its security procedures.

U.S. Attorney Announces Sentence for Creator of Blackshades Remote Access Tool Malware
On June 23, the United Sates Attorney for the Southern District of New York announced that the first defendant to ever be extradited from Moldova was sentenced to 57 months in prison after pleading guilty to computer hacking. The defendant allegedly operated an organization called Blackshades, which sold and distributed a malware tool that enabled cybercriminals to take control of users' computers.

FTC Proposes Amendment to Gramm-Leach-Bliley Act Rules
On June 24, the FTC proposed an amendment to its rules under the Gramm-Leach-Bliley Act that would permit auto dealers in some cases to provide their privacy policies to consumers online rather than by mail.

FTC Settles Mobile Hijacking Charges with App Developer
On June 29, the FTC settled charges with an app developer for falsely representing to consumers that the app would not infect devices with malware. The app contained malware that utilized the devices to mine virtual currencies for the app developer without users' knowledge or consent. The order bans the developer from creating and distributing malware, requires it to destroy all consumer information collected through the marketing and distribution of the app, and includes a $50,000 judgment.

Federal Union Files Complaint against OPM for Breach
On June 29, the American Federation of Government Employees filed a putative class action complaint against the U.S. Office of Personnel Management ("OPM") for claims arising from an April data breach that allegedly compromised the security of more than 18 million federal employees' personnel and security files. The complaint alleged violations of the U.S. Privacy Act, the Administrative Procedure Act, and common law negligence against OPM's contractor.

FBI Director Testifies About "Going Dark" Problem
On July 8, the Director of the FBI testified before the Senate Judiciary Committee about law enforcement's growing inability to access information stored on suspects' electronic devices because of encryption—the so-called "Going Dark" problem. The FBI had not yet decided whether to pursue legislation aimed at ensuring that law enforcement can access this information where appropriate.

Operation Shrouded Horizon Takes Down Darkode Forum
On July 15, the FBI announced the results of a multi-agency investigation, called Operation Shrouded Horizon. The investigation led to the takedown of the Darkode forum, an underground, password-protected, online forum where malware, botnets, stolen personal identifying information, credit card information, and hacked server credentials were sold. The FBI seized Darkode's domain and servers and indicted 12 individuals associated with the forum.

Legislative—Federal

President Signs USA Freedom Act into Law
On June 2, President Obama signed the USA Freedom Act into law. The Act reforms NSA surveillance measures, overhauls the bulk collection program for domestic telephone metadata, and places new limits on Patriot Act authorities.

House Votes to Bar NSA from Weakening Encryption Standards
On June 4, the House of Representatives voted in favor of an amendment to a spending bill (H.R. 2578) that would prohibit NIST from cooperating with the National Security Agency ("NSA") or the Central Intelligence Agency ("CIA") to weaken encryption

standards. The amendment prohibits NIST from consulting with NSA or CIA "to alter cryptographic or computer standards, except to improve information security."

Lawmakers Urge Updated TCPA Rules to Account for Wireless Changes
On June 15, members of the House Committee on Energy and Commerce sent a letter to the FCC Chairman and FTC Chairwoman urging updates to the Telephone Consumer Protection Act ("TCPA") rules that protect Americans from unwanted sales calls. According to the letter, when the TCPA was enacted in 1991, the overall wireless penetration rate was 2.9 percent, whereas now 44 percent of American homes have only wireless phones.

Rise in "Internet of Things" Spurs Lawmaker Interest
On June 23, a bipartisan group of senators from the Senate Commerce, Science and Transportation Committee sent a letter to the Government Accountability Office asking for a study of the current and future state of connected devices and the Internet of Things and its impact on the economy and consumers.

Internet Companies Seek Limited Surveillance of Email, Status Updates, and Texts
On June 25, a coalition of internet companies and interest groups sent a letter to Senate leaders seeking support for the Judicial Redress Act, which was introduced on June 17 to permit foreigners to sue the U.S. government for privacy violations when internet and other communications are improperly used by law enforcement.

Homeland Security Bill Includes Increase in Cyber Funds
On July 14, the House Appropriations Committee approved the fiscal year 2016 DHS Appropriations Bill. Although the legislation provides for less overall funding for DHS, the bill would boost the Department's cybersecurity funding. The bill awaits passage in the Senate.

Legislative—States

Washington State Passes Bill Requiring Warrant for Stingray Use
On May 11, the Washington governor signed a bill that requires law enforcement to obtain warrants before deploying international mobile subscriber identity catchers, also known as Stingray cell phone interceptors. The law became immediately effective.

Florida Enacts Drone Privacy Law
On May 14, the Florida governor signed legislation banning drone surveillance of private individuals without their consent. The law allows individuals whose photos are captured by a drone when they had a reasonable expectation of privacy to sue for injunctive relief and compensatory and punitive damages. The bill became effective on July 1.

Connecticut Enacts Employee Social Media Privacy Measure
On May 19, the Connecticut governor signed a law that bars employers from requiring employees or job applicants to provide the employers with access to employee personal online account information. The law will become effective on October 1.

Oregon Prohibits Employers from Requiring Employees or Applicants to Establish and Maintain Social Media Accounts
On June 2, the Oregon governor signed a statute that prohibits employers from forcing their employees or job applicants to have social media accounts as a condition of employment. The law also prevents employers from requiring employees to allow advertising on their personal social media accounts. The law becomes effective on January 1, 2016.

New York Releases Digital Currency Framework
On June 3, the New York Department of Financial Services issued New York's final BitLicense regulatory framework for virtual currencies such as Bitcoin. The framework rules relate to consumer protection, anti-money laundering compliance, cybersecurity,

and financial intermediaries that hold customer funds. Under the framework, licensees are required to "establish and maintain an effective cyber security program to ensure the availability and functionality of the Licensee's electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering."

New Hampshire and Oregon Enact Bills Protecting Students' Online Personal Data

On June 11, the New Hampshire governor signed legislation that provides privacy protections for students' online personal information. The measure requires certain operators of websites, online services, and other online and mobile applications targeted at students and their families to create and maintain reasonable security practices to protect covered data. On June 22, the Oregon governor also enacted legislation that restricts the sale of student information, the creation of student profiles, and the sending of targeted advertisements to students. Both measures take effect in July 2016.

Delaware Attorney General-Proposed Internet Privacy and Safety Bills Pass General Assembly

On June 25, the State of Delaware announced that its General Assembly passed the remaining parts of a four-part package of bills directed toward internet privacy and safety. The bills were proposed by the Delaware attorney general and a bipartisan group of legislators. The legislation, which includes the Delaware Online Privacy and Protection Act and Student Data Privacy Protection Act, will be enforced by the Delaware Department of Justice.

Attorneys General Ask Congress Not to Preempt State Laws When Enacting National Data Security Legislation

On July 7, the National Association of Attorneys General sent a letter to Congressional leaders, signed by 47 state attorneys general, expressing the importance of respecting states' authority to protect against data breaches and identity theft. The letter cautioned against federal preemption, stating that "it is important that any federal legislation ensure that states can continue to enforce breach notification requirements under their own state laws."

States Amend Data Breach Notification Obligations

With varying effective dates, eight states recently passed amendments to their data breach notification laws.

Nevada passed an amendment (A.B. No. 179) expanding the definition of "personal information" to include a name in combination with a driver authorization card number, a medical identification number, a health insurance number, or a user name, unique identifier, or email address, along with a password, access code, or security question and answer.

Wyoming passed two amendments (S.F. No. 35 and S.F. No. 36) requiring notice to affected persons to be "clear and conspicuous" with certain content requirements, allowing for a compliance exemption for covered entities or business associates that comply with HIPAA, and expanding the definition of "personal information" to include, for example, an account number, credit card number, or debit card number in combination with any security code, access code, or password.

Washington passed an amendment (H.B. No. 1078) broadening the notification obligations to include breaches involving noncomputerized personal information and requiring data breach notification to affected consumers not later than 45 days after the breach was discovered.

North Dakota passed an amendment (S.B. No. 2214) expanding the definition of "personal information" to include a name in combination with an identification number assigned to the individual by the individual's employer in combination with any required

security code, access code, or password and requiring notification to the attorney general of data breaches involving more than 250 individuals.

Connecticut passed an amendment (S.B. No. 949) requiring data breach notification to individuals within 90 days after discovery of a breach and if applicable, providing identity theft mitigation services at no cost to the consumer for a period of not less than 12 months.

Montana passed an amendment (H.B. No. 74) expanding the definition of "personal information" to include a name in combination with medical record information or a taxpayer identification number and requiring notification to the attorney general's consumer protection office.

Oregon passed an amendment (S.B. No. 601) expanding the definition of "personal information" to include biometric and health insurance information and requiring notification to the attorney general of data breaches involving more than 250 Oregon residents.

Rhode Island passed an amendment (S.B. No. 134) expanding the definition of "personal information," requiring data breach notification to individuals not later than 45 days after confirmation of a breach, and mandating notification to the attorney general and major credit reporting agencies for breaches involving more than 500 Rhode Island residents.

Illinois's Congress approved an amendment (S.B. No. 1833) to its data breach notification bill by adding "biometric data" to the definition of personal information. The proposed amendment awaits signature from the state governor before it becomes effective.

[Return to Top]

Canada

Canada Institutes Data Breach Notification Requirements and Various Amendments to Privacy Statute
On June 18, Canada passed the Digital Privacy Act, which issued a number of amendments to existing privacy legislation. These amendments include mandatory data breach notification to individuals and the Privacy Commissioner, record maintenance of every breach of security safeguards involving personal information under the organizations' control, and heightened consent requirements for the collection, use, or disclosure of personal information.

Industry Canada Publishes New Transparency Reporting Guidelines
On June 30, Industry Canada, the federal government's economic development and corporate affairs department, issued Transparency Reporting Guidelines. These voluntary guidelines provide categories of disclosures and limitations that private organizations should consider when reporting statistics to consumers regarding the organizations' sharing of personal information to government agencies.

Canada's Standing Senate Committee on Banking, Trade and Commerce Issues Digital Currencies Report
In June, the Standing Senate Committee on Banking, Trade and Commerce issued a report on cryptocurrencies. As part of the report, the Committee studied the security risks and benefits of cryptocurrencies and issued various recommendations to the federal government concerning the government's future legislative and regulatory approach to cryptocurrencies.

The following Jones Day attorneys contributed to the United States and Canada sections: Steven Gersten, Jay Johnson, Sam Lam, Colin Leary, Tyson Lies, Dan McLoon, Chiji Offor, Mauricio Paez, Nicole Perry, Scott Poteet, Jessica Sawyer, Alexa Sendukas, and Anand Varadarajan.

[Return to Top]

Latin America

Argentina

Personal Data Protection Agency Proposes New Regulation for Personal Data Retrieved from Drones
On May 27, the Argentinean Personal Data Protection Agency published a National Directorate (source document in Spanish) regulating personal data retrieved from the deployment of drones. The proposed regulation covers video recordings as well as other data retrieved through sensors attached to drones, such as sounds or images. The National Directorate is not applicable when drones are used for recreational or scientific purposes.

Brazil

Brazil Completes Public Debate on Internet Civil Framework and Data Protection Bill
On May 31, the Brazilian Ministry of Justice concluded public debate on the upcoming administrative decree designed to regulate the Internet Civil Framework (source document in Portuguese). On July 5, the Brazilian Ministry of Justice closed the public debate on the Draft Bill of Data Protection (source document in Portuguese). The Internet Civil Framework covers network neutrality, freedom of speech, and users' data privacy, while the Data Protection legislation focuses on standards for securing and restricting access to data.

Colombia

Supreme Court Rules on Right to be Forgotten
On May 12, the Colombian Supreme Court delivered a ruling (source document in Spanish) on the "Right to be Forgotten." The plaintiff filed a lawsuit against a newspaper that published an online article discussing her name in connection with a crime for which she was not convicted. Finding that her civil rights were violated, the court ordered the newspaper to prevent access to the online article when internet users searched for news related to the crime.

Mexico

Mexico's Data Protection Authority Changes Name
On May 5, the new General Law on Transparency and Access to Public Information (source document in Spanish) took effect after publication in the Federal Official Gazette. As a result, the Federal Institute for Information Access and Data Protection (*Instituto Federal de Acceso a la Información y Protección de Datos* or IFAI) acquired new authority and changed its name to National Institute of Transparency, Access to Information, and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* or INAI) (source document in Spanish).

Peru

Lima Hosts Ibero-American Data Protection Summit
On May 6, the Lima hosted the XIII Ibero-American Data Protection Network Summit. Members of the Data Protection Network, data protection authorities, and experts

discussed the development of data protection regulations in Latin America and the relevance of the role played by experts in enforcing data protection laws. The Summit's authority members issued a statement (source document in Spanish) undertaking commitments to ensure the development of personal data protection laws and regulations.

The following Jones Day attorneys contributed to the Latin America section: Daniel D'Agostini, Guillermo Larrea, and Elie Sherique.

[Return to Top]

Europe

European Union

EU Commission Adopts a Digital Single Market Initiative
On May 6, the European Commission released a communication and a strategy for a digital single market aimed at expanding digital opportunities in Europe. The Commission highlighted three goals: (i) providing better access for consumers and businesses to digital goods and services across Europe; (ii) creating the right conditions and a level playing field for digital networks and innovative services to flourish; and (iii) maximizing the growth potential of the digital economy. The initiative includes a list of concrete actions having a direct impact on privacy and cybersecurity matters in the EU.

EU Commission President Says Passenger Name Record Data Sharing Agreements on Hold
On June 12, the European Commission President stated that the EU would not conclude any agreements on passenger name record data transfer to non-EU countries until the European Court of Justice issues its opinion regarding these agreements and their impact on privacy rights.

Article 29 Working Party

Article 29 Working Party Provides Guidance on Binding Corporate Rules for Processors
On May 22, the Article 29 Working Party published a revised Binding Corporate Rules document pursuant to article 26 (2) of Directive 95/46/EC to regulate processors both internally and vis-à-vis third parties. The duties of processors and controllers remain the same, but the Working Party adjusted the requirements for transfers within the same group of organizations and specifics relating to training programs and data protection officers.

Article 29 Working Party Publishes Opinion Relating to Drone Use
On June 16, the Article 29 Working Party released an opinion on the challenges posed by large-scale deployment of drones for individuals' privacy and civil and political liberties. The Working Party identified key risks and provided relevant guidelines for drone manufacturers, including concepts of privacy by design and privacy by default, providing disclosures within the packaging about the potential intrusiveness of these technologies, and creating maps identifying where the use of drones is allowed. The Working Party also included recommendations for European and national policymakers to strengthen the governing legal framework.

Article 29 Working Party Discusses Finalization of General Data Protection Regulation
On June 17, the Working Party released a position on the core topics to be discussed when finalizing the General Data Protection Regulation.

European Data Protection Supervisor

EDPS Publishes Opinion on Mobile Health
On May 19, the European Data Protection Supervisor ("EDPS") published an opinion addressing the privacy challenges of mHealth technologies and the delivery of health-related information to consumers through smart devices. The EDPS provided recommendations to legislators and stakeholders in the mHealth market aimed at enabling mHealth technologies to deliver innovative services while complying with the applicable data protection principles.

Belgium

Privacy Commission Adopts Recommendations on Social Networking Site's Plug-Ins
On May 13, the Privacy Commission adopted a recommendation on tracking through social plug-ins directed at a social media site and its users. The Commission noted concerns under Belgian privacy law and announced that it will adopt further recommendations on other aspects of the social media site's privacy policy covered in the academic report.

Constitutional Court Annuls the Belgian Data Retention Law
On June 11, the Belgian Constitutional Court annulled the Belgian law (source document in French) that required electronic communication operators to retain data for one year. Drawing from an ECJ decision from 2014, the Constitutional Court held the law disproportionate and contrary to the Belgian Constitution and the European Charter of Human Rights.

Privacy Commission Releases Opinion on Proposal for European Data Protection Regulation
On June 17, the Commission published an opinion (source document in French) on the draft European Data Protection Regulation adopted by the Council. The opinion follows previous opinions on the draft proposal (source document in French) from the European Commission and the amendments proposed by the European Parliament (source document in French).

Privacy Commission Releases Data Mining Opinion
On June 17, the Commission released an opinion on draft legislation (source document in French) recognizing the legitimacy of data collection for handling social and tax fraud.

Privacy Commission Favors Modifying Criminal Code and Procedure
On June 17, the Commission issued an opinion favoring modifications (source document in French) to the criminal procedure codes, including (i) the extended scope of the summary investigation, (ii) measures concerning localization of communications and wire-tapping within the competence of the investigating judge, and (iii) exchanges of information between various law enforcement authorities.

Privacy Commission Discusses Information Exchange between Police and Customs Duties Administration
On July 1, the Commission released an opinion on draft legislation (source document in French) expanding the number of individuals within the customs/excise duties administration allowed to receive personal data from the police.

France

***Conseil d'Etat* Clarifies Individual Consent for Receiving Marketing Emails**
On March 11, the *Conseil d'Etat* (France's highest administrative jurisdiction) clarified the characteristics (source document in French) of the individual consent for receiving unsolicited electronic marketing materials. The *Conseil d'Etat* decided that mere acceptance of the terms of use of software cannot satisfy the specific consent requirement

provided by article L. 34-5 of the Posts and Electronic Communications Code.

Conseil d'Etat Upholds Sanction for Sending Text Message Spam
On March 23, the *Conseil d'Etat* confirmed the 20,000 Euros fine (source document in French) imposed by the French data protection authority ("CNIL") against a company for sending marketing text messages without prior individual consent. The *Conseil d'Etat* upheld the proportionality of the penalty because the company did not respect the right of the individual to be informed and to oppose data processing.

Conseil d'Etat Rules on Automatic Personal Data Processing Relating to Child Pornography Offenses
On May 20, the *Conseil d'Etat* upheld a CNIL decision (source document in French) denying authorization to a private company to implement automatic personal data processing to monitor child pornography offenses. According to the *Conseil d'Etat*, private companies are not authorized persons or organizations that can process data on criminal offenses, pursuant to article 9 of the French data protection act.

CNIL Requests Search Engine to Remove Links from Several Lists
On May 21, CNIL gave formal notice to an internet search engine to delist certain search results on every domain name extension in order for the delisting to be effective. CNIL made a similar request in 2014, but the search engine only honored some of the requests with domains corresponding to European countries.

CNIL Releases 2015 Control Priorities
On May 25, CNIL announced priorities (source document in French) in the following areas: contactless payment, the national driving license registrar implemented by the Ministry of Interior, "well-being and health" related connected objects, tools measuring the use of public space, and Binding Corporate Rules. Furthermore, CNIL stated its continued international cooperation efforts with other data protection authorities.

CNIL Sanctions Sending of Electronic Newsletter Containing Marketing Materials without Prior Consent
On June 1, CNIL imposed a 15,000 Euros fine (source document in French) on a company for not systematically and sufficiently informing data subjects about the processing of their data. Despite formal warnings from CNIL, the company did not systematically inform the data subject about other newsletters he would be receiving.

CNIL Formally Notifies Sites that Did Not Collect Internet Users' Consent before Implementing Cookies
On June 30, CNIL published the results (source document in French) of its 2014 investigations relating to compliance with the rules for implementing cookies. CNIL concluded that websites did not sufficiently inform internet users and did not collect their consent before implementing cookies. CNIL's president gave formal notice to 20 websites to comply with the applicable laws.

CNIL Releases PIA Manual
On July 2, CNIL published its manual on the privacy impact assessment ("PIA") procedure to help data controllers implement privacy by design. The manual discusses the methodological approach, tools, and measures for risk treatment.

Germany

Germany Adopts New IT Security Act
On June 12, the German Parliament (*Bundestag*) adopted the new Information Technology Security Act (source document in German). On July 10, The German Federal Council (*Bundesrat*) approved the Act without referring it to the Reconciliation Committee (*Vermittlungsschuss*). It now awaits the signature of the Federal President (*Bundespräsident*) and official publication before taking effect.

Federal Data Protection Commissioner Presents Activities Report
On June 17, the Federal Data Protection Commissioner issued the 25th Activities Report (source document in German) for 2013–14. A key theme in the report is controlling intelligence service activities. The structure of the report changed from previous releases, as individual reports are no longer allocated to the relevant topic but to the competent committee of the Parliament.

Federal Data Protection Commissioner Warns About Fitness Apps
On July 17, the Federal Data Protection Commissioner issued a press release (source document in German) about the risks of using fitness apps offered by private health insurance companies in exchange for access to better insurance tariffs. The Commissioner pointed out that members of statutory health insurance policies are protected by law against the disclosure of sensitive data and suggested legislation adopting similar protections for persons with private health insurance.

Italy

Data Protection Authority Adopts Measures Relating to Cookies
On May 8, the Italian Data Protection Authority adopted simplified measures for informing data subjects about cookies. Starting on June 3, companies managing websites must comply with the measures in the event they use cookies by displaying a banner on the home page with specific information for the user to consider.

The Netherlands

DDPA Requires Notification and Increases Penalties for Data Breaches
On June 4, the Netherlands adopted a new amendment to the Data Protection Act (source document in Dutch) substantially increasing Dutch Data Protection Authority ("DDPA") penalties and requiring notification of data breaches. Under the new law, companies must notify the DDPA and affected individuals of a security breach if the breach results in a substantial risk of harm to personal data.

Dutch Family Businesses Express Privacy Concerns Regarding UBO Register
On June 9, two major Dutch business lobby organizations expressed privacy concerns in a letter to the Minister of Economic Affairs and the Minister of Security and Justice (source document in Dutch) regarding the implementation of the Fourth Anti-Money Laundering Directive. The Directive requires EU member states to establish a register of ultimate beneficiary owners ("UBOs"), which would contain information about persons holding at least 25 percent of the voting rights or capital interest in a company. The organizations urged the Ministers to counter these measures in the Directive.

DDPA Comments on Public-Private Online Identification Standard
On June 11, the DDPA commented on eID (source document in Dutch), a proposed new standard for online identification for access to both corporate and government services. The authority expressed concerns about the shared responsibility and accountability for the platform and noted that the Data Protection Act requires the appointment of a single responsible party. The DDPA also stated that the proposed use of a Citizen Service Number for corporate services requires a statutory basis currently missing from the eID platform.

Proposed New Law Gives Intelligence Services Broader Powers
On July 2, the Minister of the Internal Affairs proposed and published (source document in Dutch) a new Intelligence and Security Services Act as part of an internet consultation process. The law provides the Dutch intelligence and security agencies with more powers for intercepting communications and searching automated systems. The Commission for Oversight for the Intelligence and Security Services would become an autonomous independent complaints authority with the power to issue binding opinions on complaints. Interested parties are invited to submit comments to the proposal before September 1.

Spain

Data Protection Agency Publishes 2014 Annual Report
In June, the Spanish Data Protection Agency ("DPA") published its 2014 Annual Report (source document in Spanish). The Spanish DPA received more than 12,000 claims, 15 percent more than in 2013. Common complaints included video surveillance, inclusion in debtor files, and fraudulent procurement. The telecom sector reported the highest number of data-related fines, followed by financial institutions and companies supplying energy and water.

Government Appoints Nine Members to Advisory Council of DPA
On July 4, the Spanish government appointed nine members (source document in Spanish) to the Advisory Council of the Spanish DPA. The term of appointment is four years, and one of the members will serve as chairman of the Spanish Agency.

High Court of Justice of Madrid Allows Video Surveillance Evidence without Notice to Employees
In a recent decision, the High Court of Justice of Madrid stated that the temporary installation (source document in Spanish) of video recording cameras at the workplace without notice to the workers is allowed. The court found no privacy violation where the cameras were installed on suspicion that a worker was stealing from the company.

DPA Grants Right to Process Data of Worker's Family Members without Consent
In a recent decision, the Spanish DPA recognized the legitimacy of employers (source document in Spanish) to process, without consent, the personal data of worker family members for purposes of clearing conflicts of interest.

DPA Allows Video Surveillance Privacy Masking
In a recent decision, the Spanish DPA allowed the application (source document in Spanish) of the Organic Law 15/1999 of Personal Data Protection to the video surveillance systems that use privacy masking, which would prevent the clear observation of captured images beyond the monitored security perimeter.

United Kingdom

National Cyber Security Programme Publishes Annual Survey of Information Security Breaches
On June 2, the UK National Cyber Security Programme published its annual survey of information security breaches, conducted by PwC. The Programme noted a substantial yearly increase in the number of security breaches experienced by large and small organizations, as well as an increase in associated costs. Average costs for a large organization range from £1.46m to £3.14m.

Information Commissioner Raids Cold-Calling Company
On June 24, the Information Commissioner's Office released a statement indicating that it had raided a company suspected of using automated dialing facilities to make more than 100,000 cold calls per day. The Office stated that organizations may make automated marketing calls only to people who have specifically consented to receiving such calls from that organization.

Information Commissioner's Office Publishes 2014–2015 Annual Report
On July 1, the UK Information Commissioner's Office published its annual report for 2014–2015, which includes statistics on trends in complaints and enforcement. The report indicated a record number of complaints under the Privacy and Electronic Communications Regulations governing electronic marketing communications.

The following Jones Day attorneys contributed to the Europe sections: Paloma Bru, Undine von Diemar, Olivier Haas, Bastiaan Kout, Jonathon Little, Laurent De Muyter, Selma Olthof, Sara Rizzon, and Rhys Thomas.

[Return to Top]

Asia

People's Republic of China

Court Holds Personalized Baidu Advertisement Does Not Infringe Privacy Right
In May, the Nanjing Municipal Intermediate People's Court ruled that the personalized Baidu advertisement (source document in Chinese) using cookie technology is not an infringement of privacy rights.

NPC Passes the National Security Law
In July 1, the National People's Congress ("NPC") passed the National Security Law (source document in Chinese). In addition to strengthening the protection of national security and ensuring national unification and territorial integrity, the law emphasizes the importance of cybersecurity and the need to prevent cyberattacks and illegal content dissemination.

NPC Releases Draft Cybersecurity Law
On July 6, the NPC released a draft Cybersecurity Law (source document in Chinese) to: (i) ensure network security; (ii) preserve cyberspace sovereignty, national security, and societal public interest; (iii) protect the lawful rights and interests of citizens, legal persons, and other organizations; and (iv) promote the healthy development of economic and social informatization. The law would require network operators to establish and complete user information protection systems and strengthen protection of users' personal information, privacy, and commercial secrets. Network operators using citizens' personal information would also have to provide notice and obtain consent where appropriate.

Hong Kong

PCPD Assesses Privacy Issues Relating to Youngsters
On May 11, the Privacy Commissioner for Personal Data ("PCPD") joined the Global Privacy Enforcement Network to examine websites and mobile applications that primarily target youngsters for various issues related to youth privacy. The results of this privacy sweep will be published in the fall.

PCPD Study Reveals Gap in Child Privacy Knowledge
On May 19, the PCPD released the results of an exploratory study on child privacy carried out by the Centre of the Advancement of Social Sciences Research of Hong Kong Baptist University. The study shows the lack of awareness about children's privacy among children, their parents, and teachers. The PCPD developed a website called "Youth Privacy Portal" that provides information on personal data privacy for children and parents.

PCPD Releases Results of Hong Kong Accountability Benchmarking Micro-Study
On June 10, global risk assessment enterprise Nymity announced the results of a collaborative study with PCPD called the Hong Kong Accountability Benchmarking Micro-Study. The Study reveals the privacy management status of participating organizations and shows that compared to other large global institutions, a higher percentage of organizations in Hong Kong implement personal data inventory and data classification.

Singapore

PDPC Publishes Advisory Guidelines on Requiring Consent for Marketing
On May 15, the PDPC of Singapore issued the Advisory Guidelines on Requiring Consent for Marketing purposes together with Sample Clauses for Obtaining and Withdrawing Consent. The guidelines focus on situations in which organizations may wish to obtain an individual's consent for marketing activities, and it addresses how best to comply with the

Personal Data Protection Act 2012.

PDPC Issues Guides for Protecting Electronic Personal Data and Managing Data Breaches
On May 15, the PDPC issued three guides: (i) a brochure entitled "Is Personal Data Safe with Your Organisation? Electronic Personal Data Protection for Organisations"; (ii) a guide to Securing Personal Data in Electronic Medium; and (iii) a guide to Managing Data Breaches.

PDPC Releases DPO Connect e-Newsletter
On June 11, the PDPC launched a monthly e-newsletter (DPO Connect) to keep data protection officers apprised of the PDPC's view on personal data protection matters, personal data protection practices of others, and best practices relating to compliance with the Personal Data Protection Act 2012.

Taiwan

Ministry of Justice Clarifies Definition of "Government Agency"
On April 14, the Ministry of Justice explained the definition of "government agency" (source document in Chinese) described under the Personal Information Protection Act. The definition classifies public hospitals as government agencies under the Act, subjecting them to national compensation for violations of the Act.

The following Jones Day attorneys contributed to the Asia sections: Emmanuel Amos, Li-Jung Huang, Anita Leung, Michiru Takahashi, and Richard Zeng.

[Return to Top]

Australia

Government Announces Bill for Mandatory Data Breach Notification Scheme
Earlier this year, the Upper House of the Australian Parliament began considering a bill that requires entities to notify the Information Commissioner of serious data breaches involving personal, credit reporting, credit eligibility, or tax file number information.

Privacy Regulator Releases Guide to Privacy Regulatory Action
On June 30, the Office of the Australian Information Commissioner ("OAIC") released the Guide to Privacy Regulatory Action , which provides guidance on the OAIC's exercise of its new regulatory powers. Under its new powers, the OAIC may conduct an assessment of how an entity handles personal information, apply to the court for a civil penalty order, and investigate acts or practices that may interfere with the privacy of an individual. The guide describes how particular interference with privacy may be serious and details the OAIC's policy in seeking civil penalty orders.

The following Jones Day attorneys contributed to the Australia section: Peter Brabant, Adam Salter, and Nicola Walker.

[Return to Top]

Jones Day Cybersecurity, Privacy, and Data Protection Lawyers

Emmanuel G. Baud Paris	Wolfgang G. Büchner Munich	Shawn Cleveland Dallas	James A. Cox Dallas
Walter W. Davis	Scott A. Edelstein	Timothy P. Fraelich	Joshua L. Fuchs

Atlanta

Karen P. Hewitt
San Diego

Jeffrey L. Kapp
Cleveland

Jonathon Little
London

Kristen Pollock McDonald
Atlanta

Janine Cone Metcalf
Atlanta

Chaka M. Patterson
Chicago

Gregory P. Silberman
Silicon Valley

Michael W. Vella
Shanghai

Sidney R. Brown
Atlanta

Guillermo E. Larrea
Mexico City

Michael G. Morgan
Los Angeles

Po-Chien Chen
Taipei

Adrian Garcia
Dallas

Javier Gutiérrez Ponce
Madrid

Nandini Iyer
Silicon Valley

Nicole M. Perry
Houston

Raquel Travesí
Madrid

Washington/Los Angeles

John E. Iole
Pittsburgh

J. Todd Kennard
Columbus

Kevin D. Lyles
Columbus

Jason McDonell
San Francisco

Caroline N. Mitchell
San Francisco

Jeff Rabkin
San Francisco

Cristiana Spontoni
Brussels

Undine von Diemar
Munich

Paloma Bru
Madrid

Christopher J. Lopata
New York

Sergei Volfson
Moscow

Nigel Chin
Singapore

Steven G. Gersten
Dallas

Aaron M. Healey
Columbus

Bastiaan K. Kout
Amsterdam

Scott B. Poteet
Dallas

Anand Varadarajan
Dallas

Cleveland

Robert W. Kantner
Dallas

Ted-Philip Kroke
Frankfurt

John M. Majoras
Columbus/Washington

Carmen G. McLean
Washington

Matthew D. Orwig
Dallas/Houston

Elizabeth A. Robertson
London

Michiru Takahashi
Tokyo

Toru Yamada
Tokyo

Amanda B. Childs
Dallas

Margaret I. Lyle
Dallas

Olivier Haas
Paris

Christopher S. Cogburn
Atlanta

Bart Green
Irvine

Elaine Ho
Singapore

Colin Leary
San Francisco

Brandy Hutton Ranjan
Columbus

Natalie A. Williams
Atlanta

Houston

Elena Kaplan
Atlanta

Anita Leung
Hong Kong

Todd McClelland
Atlanta

Daniel J. McLoon
Los Angeles

Mauricio F. Paez
New York

Adam Salter
Sydney

Rhys Thomas
London

Jay Johnson
Dallas

Georg Mikes
Frankfurt

David L. Odom
Dallas

Laurent De Muyter
Brussels

Joshua Grossman
New York

Nancy L. Hoffman
New York

Susan M. O'Connor
New York

Jessica M. Sawyer
Los Angeles

Marc L. Swartzbaugh
Cleveland