Global Privacy & Cybersecurity Update
Issue 16 | November 2017
JONES DAY

GLOBAL PRIVACY & CYBERSECURITY UPDATE

Jones Day Cybersecurity, Privacy & Data Protection Attorney Spotlight: Todd McClelland

Emerging technologies like edge computing, blockchain, and artificial intelligence/cognitive computing, along with increasing connectivity of IoT and other devices, are key drivers of business growth, but they pose significant financial liability and risk to the enterprise. Navigating the legal issues associated with adoption and implementation of these technologies and their attendant risks and benefits, especially in light of an increasingly dynamic global regulatory landscape, is a critical component of business and governance strategy as companies look toward 2020 and beyond.

Todd McClelland is a partner based in Atlanta and a key member of Jones Day's Cybersecurity, Privacy & Data Protection Practice. Todd is one of the Firm's leading advisors on the data protection issues associated with these and other emerging technologies. Todd has particular knowledge of data breach response, cybersecurity compliance and assessment (e.g., PCI DSS, HIPAA Security Rule), cyber risk management, global data privacy compliance, and vendor agreements (e.g., cloud, outsourcing, data and technology licensing).

Todd maintains a *Best Lawyers in America* ranking in privacy and data security law. His cyber career began as a factory automation engineer designing and programming industrial computing networks and controllers.

United States

Regulatory—Policy, Best Practices, and Standards

United States and China Renew Promise Not to Hack

On October 4, U.S. and Chinese officials agreed to not engage in targeted hacking. Per a published summary of the dialogue, the United States and China agreed to

EDITORIAL CONTACTS

Daniel J. McLoon
Los Angeles

Mauricio F. Paez
New York

Jay Johnson
Dallas

Jonathon Little
London

Kevin D. Lyles
Columbus

Todd S. McClelland
Atlanta

Jeff Rabkin
San Francisco

Lisa M. Ropple
Boston

Adam Salter
Sydney

Michiru Takahashi
Tokyo

Undine von Diemar
Munich

Paloma Bru
Madrid

Olivier Haas
Paris

Jörg Hladjk
Brussels

Editor-in-Chief: Anand Varadarajan

HOT TOPICS IN THIS ISSUE

continue to work toward providing timely responses on information requests regarding cybercrime, not conduct or support cyberattacks and theft of intellectual property and trade secrets, make efforts to find "appropriate norms" for international cyberspace behavior, maintain "high-level joint dialogue" on cybercrime issues, and increase law enforcement cooperation on security issues.

Regulatory—Critical Infrastructure

NIST Releases Guidance on Application Container Security
On October 25, the National Institute of Standards and Technology ("NIST") issued a publication on application container technology and related security challenges. According to NIST, "[a]pplication container technology is increasingly being used to deploy, manage, and maintain applications." The guide seeks to provide "practical recommendations for addressing [security implications] when planning for, implementing, and maintaining containers."

Regulatory—Consumer and Retail

Senate Panel Reviews FTC Reform Proposals
On September 26, the Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security convened a hearing titled "FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare." In his opening statement, Senator Blumenthal stated that he would push for a measure that would provide the Federal Trade Commission ("FTC") with "the ability to prescribe rules requiring reasonable security practices."

FTC Plans Informational Injury Workshop
On September 29, the FTC announced that it will host a workshop on December 12 to examine consumer injury in the context of privacy and data security. The workshop will address how to characterize and measure injuries when information about consumers is misused.

FTC Provides Additional Guidance on COPPA
On October 23, the FTC provided additional guidance on how the Children's Online Privacy Protection Act ("COPPA") applies to the collection of audio voice recordings. The guidance requires that those companies covered by COPPA obtain verifiable parental consent before collecting an audio recording. However, the FTC stated that it would not seek an enforcement action against a company for not obtaining consent when a recording is collected solely as a replacement for written words.

Regulatory—Transportation

Data Privacy Chiefs Worldwide Issue Guidance on Connected Cars
On September 28, global data privacy chiefs issued a nonbinding connected cars data protection resolution offering guidance to companies on how to handle customer data. The resolution, adopted in a closed session at the 39th International Data Protection and Privacy Commissioners' Conference in Hong Kong, calls for users of autonomous vehicles or connected cars to be given full information on data collection and storage procedures. In addition, the resolution asks data controllers to abide by standard data protection principles and implement cybersecurity measures to ensure that drivers of connected vehicles cannot be unlawfully

Supreme Court Grants Certiorari to Resolve Dispute Over U.S. Warrants for Foreign-Stored Data

INAI Issues Guide for Personal Data Owners

EU Commission Publishes First Annual Review of EU-U.S. Privacy Shield

Article 29 Working Party Issues Guidelines on Data Breach Notifications

China Releases Additional Guidelines on Cybersecurity Law

RECENT AND PENDING SPEAKING ENGAGEMENTS

Data Protection, CISO Executive Network, Dallas, TX (Dec. 6). **Jones Day Speaker: Jay Johnson**

Data Protection: A Primer on the General Data Protection Regulation, Women's Bar Association, Washington, D.C. (Dec. 5). **Jones Day Speaker: Jennifer C. Everett**

Competition Law and Data Protection, Association for the Study of Competition law, Brussels, Belgium (Nov. 23). **Jones Day Speaker: Laurent De Muyter**

Cybersecurity and Legal Compliance, Balabit, Mexico City, México (Nov. 16). **Jones Day Speaker: Guillermo E. Larrea**

Data Protection, CISO Executive Network, Washington, D.C. (Nov. 16). **Jones Day Speaker: Jennifer C. Everett**

Protecting Your Connected World: Managing Cybersecurity and Privacy Risks in the Health Care, Life Sciences, and Pharmaceutical Industry, Webinar (Nov. 14). **Jones Day Speakers: Samir Jain, Mauricio Paez**

The Next Generation of Cyber Laws and Regulations, SINET Showcase 2017, Washington, D.C. (Nov. 8). **Jones Day Speaker: Samir Jain**

HIPAA & Cybersecurity: Understanding the Privacy, Security and Data Breach Notification Rules, ERISA Basics National Institute—2017, Chicago, IL (Oct. 27). **Jones Day Speaker: Jennifer C. Everett**

Access Management, CISO Executive Network, Houston, TX (Oct. 26). **Jones Day Speaker: Nicole Perry**

Access Management, CISO Executive

tracked.

Regulatory—Defense and National Security

Cyber Command Exercises New Acquisition Powers
On September 29, the U.S. Cyber Command awarded its first contract under its new limited acquisition authority. The Fiscal Year 2016 National Defense Authorization Act granted the U.S. Cyber Command the authority to acquire, develop, and sustain equipment and capability related to cyberspace operations, and to execute contract actions up to $75 million a year through September 30, 2021. The U.S. Cyber Command will use such funds in the future to build partnerships, starting with an industry day announced for October 27 to meet with government and industry representatives.

Defense Department Hosts Media Roundtable in Observance of Cybersecurity Awareness Month
On October 17, the Defense Department's deputy chief information officer held a media roundtable at the Pentagon with her service counterparts to discuss key Department of Defense ("DOD") and military initiatives. The roundtable was part of the DOD's observance of Cybersecurity Awareness Month, which is organized by the Department of Homeland Security and has a different theme each week of October. Topics discussed included elevation of U.S. Cyber Command to a full combatant command and the cybersecurity initiatives of the various military branches.

Regulatory—Financial Services

SEC Discloses 2016 Cyber Intrusion to EDGAR System
On September 20, the Securities and Exchange Commission ("SEC") Commission Chairman explained that a 2016 cyber intrusion exploiting a software vulnerability may have been the basis for illicit gain through trading on nonpublic information. The Chairman later announced on October 2 that an ongoing staff investigation into the intrusion had determined that the names, dates of birth, and Social Security numbers of two individuals had been accessed by third parties. In these statements, the Chairman also addressed general collection and use of data by the Commission, incorporation of cybersecurity considerations in the SEC's disclosure-based and supervisory efforts, its coordination with other governmental entities, and general enforcement of the federal securities laws.

SEC Announces Two New Enforcement Initiatives
On September 25, the SEC issued a press release announcing two new enforcement initiatives to combat cyber-based threats and protect retail investors: the creation of a Cyber Unit and the establishment of a retail strategy task force. The Cyber Unit will focus on areas such as market manipulation schemes involving electronically transferred false information and data breaches intended to obtain nonpublic information. The retail strategy task force will focus on leveraging data analytics and technology to identify large-scale misconduct affecting retail investors.

SEC Inspector General Issues Report on Agency's Challenge to Ensure Effective Cybersecurity Program
On October 5, the SEC issued a report citing an effective cybersecurity program as a remaining management and

Network, Dallas, TX (Oct. 25). **Jones Day Speaker: Jay Johnson**

Next Generation of Cyber-threats Presentation to New England Legal Foundation Board of Directors, Boston, MA (Oct. 18). **Jones Day Speakers: Lisa M. Ropple, Samir Jain**

Handling a Cybersecurity Investigation: A Discussion with a Regulator, a Lawyer, and a Security Expert, The Society of Corporate Compliance & Ethics 16th Annual Compliance & Ethics Institute, Las Vegas, NV (Oct. 18). **Jones Day Speaker: Jay Johnson**

EU General Data Protection Regulation/Countdown to the GDPR—Top 10 Implementation Issues for Companies, Tokyo, Japan (Oct. 16). **Jones Day Speakers: Undine von Diemar, Jörg Hladjk, Michiru Takahashi, Jonathon Little**

Cyberdefense Around the World, The Cyber Frontier, The Atlantic, Washington, D.C. (Oct. 12). **Jones Day Speaker: Samir Jain**

Access Management, CISO Executive Network, Washington, D.C. (Oct. 12). **Jones Day Speaker: Samir Jain**

FDA's Plan for Digital Health Innovation and Associated Cyber Risks, Washington, D.C. (Oct. 11). **Jones Day Speakers: Samir Jain, Marina Moreno**

Cybersecurity—A Key Data Governance Issue: From Personal Data to Critical Infrastructures, Paris, France (Oct. 10). **Jones Day Speaker: Olivier Haas**

Presentation on GDPR and related Brexit Impact, Association of Veterinary Consultants, Milan, Italy (Oct. 7). **Jones Day Speaker: Giuseppe Mezzapesa**

Industrial Security and Privacy—ICS/SCADA Threats, Laws, and Risk Mitigation, Privacy + Security, Washington, D.C. (Oct. 6). **Jones Day Speaker: Jay Johnson**

The GDPR and May 2018: Continuous Improvement over Delayed Perfection, Jones Day, London, England (Oct. 5). **Jones Day Speaker: Elizabeth Robertson**

Cybersecurity in the C-Suite, Tech Titans, Dallas, TX (Sept. 28). **Jones Day Speaker: Anand Varadarajan**

performance challenge for the 2018 fiscal year. The statement was issued per the Reports Consolidation Act of 2000 requiring the SEC to identify and report annually on the most serious management challenges facing the agency.

SEC Commissioner Discusses Risks of New Technologies
On October 12, an SEC Commissioner stated at the SEC's Investor Advisory Committee Meeting that the "rapidly expanding ICO market and the rising incidences of fraud within this market may signal a need for clearer oversight to better protect investors." The SEC's Commission Chairman also took the occasion to discuss the risks of blockchain, and SEC issued guidance on the technology.

Regulatory—Health Care/HIPAA

HHS Provides Guidance for Complying with HIPAA's Privacy Rule During Opioid Crisis
On October 27, the U.S. Department of Health and Human Services' ("HHS") Office for Civil Rights published a bulletin providing guidance to health care providers on how to comply with HIPAA's Privacy Rule when a patient is incapacitated or in crisis due to an opioid overdose. The guidelines detail exceptions to the Privacy Rule that can be triggered by an unconscious patient or one facing serious threats to his health and safety. In these cases, certain relevant health information can be shared with family and friends to gather information on the overdose or to mitigate the risk of continued opioid use after discharge.

Litigation, Judicial Rulings, and Agency Enforcement Actions

Computer Manufacturer Settles FTC Charges Relating to Compromised Preinstalled Software
On September 5, the FTC entered a consent agreement with a prominent computer manufacturer over allegations that the company sold consumer laptops with preinstalled software that interfered with how a user's browser interacted with websites and delivered pop-up advertisements. As part of the settlement, the manufacturer must retain consumers' affirmative consent before pre-installing sensitive software and is required to implement a comprehensive software security program for most consumer software preloaded on its laptops for the next 20 years.

Three Companies Reach Settlement Regarding False Participation in EU-U.S. Privacy Shield Framework
On September 8, the FTC reported that it reached consent agreements with a human resources software company, a printing services company, and a real estate lease management company. The FTC brought charges against these companies for their alleged misrepresentation of participation in the EU-U.S. Privacy Shield.

States Take Investigative and Enforcement Actions Following Data Breach

- On September 8, the Illinois Attorney General announced an investigation into the data breach of a consumer reporting agency. Since then, nearly 40 states have joined the probe.
- On September 19, the Massachusetts Attorney General filed the nation's first enforcement action against the consumer reporting agency, alleging that it failed to

Cybersecurity and FINTECH: effects on legal and compliance departments, International Chamber of Commerce (ICC), Mexico City, México (Sept. 28). **Jones Day Speaker: Guillermo E. Larrea**

Blockchain: Best Practices and Legal Issues, Paris, France (Sept. 28). **Jones Day Speakers: Philippe Goutay, Olivier Haas**

The Crypto Colloquium, New America, Washington, D.C. (Sept. 25). **Jones Day Speaker: Samir Jain**

Security Visibility & Incident Response, CISO Executive Network, Houston, TX (Sept. 21). **Jones Day Speaker: Nicole Perry**

Security Visibility & Incident Response, CISO Executive Network, Dallas, TX (Sept. 20). **Jones Day Speaker: Jay Johnson**

EU General Data Protection Regulation/Countdown to the GDPR—Top 10 Implementation Issues for Companies, Webinar (Sept. 14). **Jones Day Speakers: Undine von Diemar, Jörg Hladjk**

RECENT AND PENDING PUBLICATIONS

The Non-Inevitable Breadth of the Zeran Decision in Commemorating the 20th Anniversary of Internet Law's Most Important Judicial Decision, *The Recorder* (Nov. 2017). **Jones Day Author: Samir Jain**

Looming Ruling on EU Data Transfer Rules Carries Potentially Serious Implications (Oct. 2017). **Jones Day Authors: Various**

China's New Cybersecurity Law Brings Enforcement Crackdown (Oct. 2017). **Jones Day Authors: Various**

New Ibero-American Standards to Provide Consistency in the Protection of Personal Data (Oct. 2017). **Jones Day Authors: Various**

Use of Standard Clauses Under Attack (source document in Italian) (Oct. 2017). **Jones Day Author: Giuseppe Mezzapesa**

Federal Court Applies Charitable Organization Exemption in Telephone Consumer Protection Act Case (Oct. 2017). **Jones Day Authors: Todd Kennard, William Dolan, Gregory Hanthorn**

Artificial Intelligence (subscription

protect sensitive and personal information of nearly three million Massachusetts residents. The complaint alleges that, between at least March 7 through July 30, the agency left sensitive and private consumer information exposed to intruders by relying on certain computer codes that it knew or should have known were vulnerable to exploitation.

Illinois District Court Refuses to Dismiss Claims Against Photo Service Under State's Biometric Data Law

On September 15, an Illinois federal court denied the motion to dismiss a putative class action against an online photo company under the Illinois Biometric Information Privacy Law Act ("BIPA"). BIPA prohibits private entities from collecting or obtaining an individual's "biometric identifier or biometric information" without first informing the individual in writing about the information that is being stored, the "specific purpose and length of time" of its use, and further obtaining the individual's express written release. The court rejected the company's claim that BIPA applies only to facial scans or prints derived from in-person scans.

District Court Dismisses Portion of Unfair Practices Claim

On September 19, a California federal court dismissed three of the six claims against a computer networking equipment manufacturer, including an allegation of unfair practices under the FTC Act. The court noted that "[t]he pleading problem the FTC faces concerns the first element of injury. The FTC does not allege any actual consumer injury in the form of a monetary loss or an actual incident where sensitive data was accessed or exposed."

required), *The Texas Lawbook* (Oct. 2017). **Jones Day Authors: Jay Johnson, Bob Kantner, Samir Kaushik**

California Issues New Autonomous Vehicle Regulations (Oct. 2017). **Jones Day Authors: Various**

Standards for Data Protection for the Ibero-American States (Oct. 2017). **Jones Day Authors: Various**

Artificial Intelligence—State of Play and Legal Challenges, Option Droit & Affaires (in French) (Sept. 2017). **Jones Day Authors: Olivier Haas, Hatziri Minaudier**

Protecting Your Identity After a Data Breach (Sept. 2017). **Jones Day Authors: Dan McLoon, Michelle Blum, Kerianne Tobitsch**

Blind Spots Remain as SELF DRIVE Act Passes House (Sept. 2017). **Jones Day Authors: Jeffrey Jones, Robert Kantner, Charles Moellenberg, Paul Rafferty**

Blockchain for Business (Sept. 2017). **Jones Day Authors: Various**

SEC Charges ICO Promoters with Defrauding Investors

On September 29, the SEC brought its first enforcement action in connection with an initial coin offering ("ICO"). According to the complaint, the particular digital tokens in question were allegedly backed by fictitious assets, and the defendants fraudulently raised $300,000 from hundreds of investors. The enforcement action followed guidance from the SEC over the past several months that "virtual coins or tokens may be securities and subject to the federal securities laws" and alerting investors to potential scams involving companies using ICOs in pump-and-dump schemes.

Court Grants Initial Approval for $7 Million Settlement in Restaurant TCPA Litigation

On October 6, a Michigan federal court granted preliminary approval of a settlement proposed by the lead plaintiff to end its class action accusing a restaurant of sending advertisements nearly 14,000 times to roughly 7,700 fax numbers. Class certification was granted in December 2015, and the class consisted of everyone who received at least one fax from the restaurant on three dates in 2006 offering "15% OFF Your Total Catering or Banquet Food Bill Up to $100." The settlement will provide class members who submit a valid claim either $500 per fax or a pro rata share of the settlement fund after other required payments are subtracted.

Supreme Court Grants Certiorari to Resolve Dispute over U.S. Warrants for Foreign-Stored Data

On October 16, the Supreme Court announced that it had granted the U.S. government's petition for certiorari in *United States v. Microsoft*, No. 17-2 (cert. granted Oct. 16, 2017) regarding the reach of a U.S. warrant over emails stored on a foreign server. At issue is a 2016 Second Circuit decision that held that warrants issued under the Stored Communications Act do not extend to emails and other user data that are stored overseas by a U.S. provider.

Legislative—Federal

House Bill Reauthorizes Foreign Surveillance with New Privacy Protections

On October 6, members of the House of Representatives introduced the USA Liberty Act to reauthorize a key program of the Foreign Intelligence Surveillance Act, which allows the National Security Agency to collect information on overseas targets. The new legislation includes added privacy protections, such as preventing the U.S. government from using information collected under this mechanism to criminally prosecute U.S. citizens without a warrant. The bill was referred to subcommittee.

Congress Considers Small Business Cybersecurity Legislation

- On October 11, the House of Representatives passed a bill that aims to provide cybersecurity guidance

to small businesses in the United States. The NIST Small Business Cybersecurity Act (H.R. 2105) would require the Department of Commerce's National Institute of Standards and Technology ("NIST") to issue voluntary cybersecurity guidelines that fit the needs of small businesses.
- On September 28, the Senate passed a similar bill, the MAIN STREET Cybersecurity Act (S. 770). Unlike the House version, the Senate bill contains a provision stating that if another federal agency provides small business cybersecurity resources, the head of each agency must make sure "resources are consistent with the resources disseminated" through NIST.

Legislators Address Equifax Data Breach and Potential New Protections
On October 17, the Senate Banking Committee held a hearing to consider legislative responses in the wake of the hack to a consumer reporting agency that reportedly exposed more than 145 million Americans' unique personal identifying information. On September 15, the Senate introduced the Freedom from Equifax Exploitation Act to give consumers more control over their own credit data, while on October 12, the House of Representatives introduced the PROTECT Act to allow federal banking regulators to conduct regular examinations of credit bureaus' cybersecurity protocols.

Legislative—States

New Jersey Shopper Privacy Law Takes Effect
On October 1, New Jersey's Personal Information and Privacy Protection Act took effect. The law is designed to protect the privacy of retail shoppers' personal data embedded in the bar codes of identification cards scanned by businesses. The legislation limits the information collected to name, address, date of birth, state of issuance, and identification card number, and also prohibits sharing the information with third parties for marketing, advertising, or promotions.

Canada

Minister of Public Safety and Emergency Preparedness Issues Statement on Cyber Security Awareness
On October 2, the Minister of Public Safety and Emergency Preparedness made an announcement as part of Cyber Security Awareness Month. He observed that "cyber threats are getting more common and more widespread" and encouraged citizens to take appropriate precautionary measures.

Public Safety Canada Evaluates Canada's Cyber Security Strategy
On October 10, Public Safety Canada issued a final report after conducting an evaluation of the governance, implementation, and performance of Canada's Cyber Security Strategy. The report outlined a number of findings, including that the Strategy "contributed towards increasing the Government of Canada's capacity to prevent, detect, respond to, and recover from cyber attacks." The report likewise contained a number of recommendations, like strengthening information-sharing among partners and stakeholders, and collecting relevant performance information.

The following Jones Day lawyers contributed to this section: Jeremy Close, David Coogan, Jeff Connell, Jennifer Everett, Tyler Harris, Jay Johnson, Tyson Lies, Dan McLoon, Mary Alexander Myers, Kara O'Connell, Mauricio Paez, Nicole Perry, Alexa Sendukas, Anand Varadarajan, and Jenna Vilkin.

[Return to Top]

Latin America

Argentina

Supreme Court Holds Social Media Spying a Federal Crime
On September 19, the Argentinean Supreme Court ruled (source document in Spanish) that spying on Facebook or by email or cellphone contact lists of one's partner constitutes a federal crime. The Court ruled that such acts are "an illegitimate access to an electronic communication or computer data of restricted access, which can only be entered through means that according to its own characteristics is found within the telecommunications services."

President Amends Law on Access to Public Information
On September 25, through a decree of necessity and urgency (*Decreto de Necesidad y Urgencia*), the President amended the law (source document in Spanish) on access to public information. The modifications specifically affect the functions and powers of the Information Access Agency, which will be the entity responsible for controlling access to public information and the protection of personal data set up in archives, registers, and data banks.

Chile

Santiago Court of Appeals Rejects Appeal Filed Against Internet Search Engine
On October 2, the Santiago Court of Appeals rejected an appeal (source document in Spanish) filed against an internet search engine provider and two other digital media outlets for disseminating and maintaining unauthorized images of a young man who previously died. The ruling stated that the company

merely acted "as a search engine for public information" and that "[t]hose who have uploaded the pictures are responsible for the existence of such information available to the public on the internet."

Mexico

INAI Issues Guide for Personal Data Owners

On September 18, the National Institute for Transparency, Access to Information and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* or "INAI") issued a Guide for Personal Data Owners (source document in Spanish). The Guide covers distinct topic areas and is divided into four volumes: (i) general concepts of personal data protection; (ii) data protection guiding principles; (iii) ARCO (access, rectification, cancellation, and opposition) rights; and (iv) personal data procedures before INAI.

INAI Instructs National Security Research Center to Disclose Software Contracts

On October 29, INAI required (source document in Spanish) the Mexican National Security Research Centre (*Centro de Investigación y Seguridad Nacional*) to disclose contracts for software that allow the agency to view and monitor private communications. The instruction was issued in response to a civilian's request to the agency.

The following Jones Day lawyers contributed to this section: Guillermo E. Larrea, Daniel C. D'Agostini, and Mónica Peña Islas.

[Return to Top]

Europe

European Union

EU and U.S. Seek to Finalize Arbitration Panel under EU-U.S. Privacy Shield

On September 22, the European Commission and the U.S. Department of Commerce issued a press release calling for arbitrators to serve on the Arbitration Panel under the EU-U.S. Privacy Shield. The request follows the recently adopted "arbitration mechanism which Europeans whose personal data are transferred to certified U.S. companies may invoke when they consider that their data protection rights under the framework have been infringed."

EU Commission Publishes First Annual Review of EU-U.S. Privacy Shield

On October 18, the European Commission published its report on the first annual review of the EU-U.S. Privacy Shield. The report reflects the Commission's findings on the implementation and enforcement of the EU-U.S. Privacy Shield framework in its first year of operation. Although the report notes that the Privacy Shield ensures an adequate level of data protection, it also includes recommendations for improved functioning and operation.

Article 29 Working Party

Article 29 Working Party Issues Guidelines on Data Breach Notifications

On October 3, the Article 29 Working Party released draft guidelines providing clarification and guidance on the notification requirements following data breaches involving personal data under the General Data Protection Regulation ("GDPR"). The Article 29 Working Party will accept comments from stakeholders until November 28.

Article 29 Working Party Releases Guidelines on Administrative Fines

On October 3, the Article 29 Working Party adopted draft guidelines regarding the application and setting of administrative fines under the GDPR. The guidelines outline the criteria applied by data protection authorities when considering whether to impose fines and emphasize the need for consistency with the amount of fines and enforcement methods.

Article 29 Working Party Issues Opinion on Processing Personal Data for Cooperative Intelligent Transport Systems

On October 4, the Article 29 Working Party adopted an opinion on processing personal data in the context of Cooperative Intelligent Transport Systems ("C-ITS"), which is a "peer-to-peer solution for the exchange of data between vehicles and other road infrastructural facilities." The document provides background information on how personal data is processed in the context of C-ITS and provides general guidance on data protection implementation.

Article 29 Working Party Releases Guidelines on Automated Individual Decision-Making and Profiling

On October 17, the Article 29 Working Party issued draft guidelines to further clarify the GDPR provisions addressing risks arising from profiling and automated decision-making. The Article 29 Working Party will accept comments from stakeholders until November 28.

European Data Protection Supervisor

EDPS Issues Press Release on 2018 International Conference of Data Protection
On October 3, the European Data Protection Supervisor ("EDPS") released a statement on the 2018 International Conference of Data Protection ("Conference"). Among other topics, the EDPS emphasized that the Conference and privacy commissioners would focus on digital ethics and how to respond to the changing data protection and privacy landscape.

European Network and Information Security Agency (ENISA)

ENISA Publishes Survey Report on ICT Security Certification
On September 19, ENISA published a survey report regarding considerations for information and communication technologies ("ICT") security certification in the EU. The report follows ENISA's continuing efforts to establish certification standards for ICT security products and services, and the survey provides a framework to consult stakeholders and seek structured feedback regarding policy options.

Belgium

Privacy Commission Issues Opinion on Bill Establishing the Belgian Data Protection Authority
On September 20, the Privacy Commission released an opinion (source document in Dutch and in French) on draft legislation introduced by the Belgian Parliament establishing the DPA. The opinion reviews key articles in the bill and highlights ambiguities and shortcomings.

France

French Government Publishes Order on Electronic Identification and Trust Services for Electronic Transactions
On October 4, the French Prime Minister issued an order (source document in French) on Electronic Identification and Trust Services for Electronic Transactions to reinforce the existing regulations on electronic transactions. Among other changes, the order introduces a legal definition of "electronic identification" and sets an optional certification system for electronic identification service providers. ANSSI will act as the certification authority and the terms of such certification will be set by the French *Conseil d'Etat*.

CNIL and French Commission on Access to Administrative Documents Discuss Compliance and Privacy Rights
On October 5, the French Data Protection Authority ("CNIL") met the French Commission on Access to Administrative Documents ("CADA") to launch the Open Data Pack (source document in French), in an effort to encourage compliance with data regulations and privacy rights. The Pack provides guidance for understanding and implementing the legal framework and how to answer questions from the public at large.

CNIL Publishes Compliance Guidelines on Use of Personal Data by Autonomous Vehicles
On October 17, CNIL issued its personal data protection compliance pack (source document in French) to provide guidance to automotive companies when processing personal data through autonomous vehicles. In its guidance, CNIL identified three scenarios of personal data collection and processing by vehicles: (i) personal data used by the vehicle without further transfer or exchange; (ii) personal data sent to companies for purposes of providing a service to the vehicle owner; and (iii) personal data sent to companies to trigger a vehicle-related action.

French Government Launches Online Assistance System for Cyber Victims
On October 17, the French government launched a victim assistance website (source document in French), accessible at "Cybermalveillance.gouv.fr," to be a nationwide forum that connects victims of malicious cyber activity with local service providers. The service website is tasked with listing solution service providers throughout the nation, launching national information and awareness campaigns on digital security, and creating a digital risk observatory.

Data Protection Authorities Audit 455 Websites and Mobile Applications
On October 24, 24 data protection authorities, led by CNIL, published the results of an audit (source document in French) of various travel and online sales websites and mobile applications regarding their use and processing of individuals' personal data. The audit revealed that sites' privacy policies are unclear, use generic clauses, and lack information on the safeguards taken to ensure the security of users' data. Furthermore, only half of the sites and applications inform users about their right to access their data and how to exercise such rights.

CNIL Issues Guidelines on Free Wi-Fi Networks
On October 25, CNIL issued guidelines (source document in French) on best practices when using a third-party Wi-Fi in a public area. CNIL recommended that individuals confirm the name of the network with the network owner, provide minimal information when registering, and turn off the wireless tracking functionality when not using Wi-Fi.

Germany

Bavarian DPA Comments on Online Marketing Tool
On October 4, the Bavarian Data Protection Authority ("DPA") issued a press release (source document in German) on its survey of 40 companies that use the marketing tool "Facebook Custom Audience" for targeted advertisements. The survey revealed that the two tested variants of "Facebook Custom Audience" (pixel-method and customer-list method) often violated data protection law. The press release also provides guidance on how to implement "Facebook Custom Audience" in compliance with data protection laws.

Bavarian DPA Starts Cyber Security Initiative
On October 10, the Bavarian DPA issued a press release (source document in German) on its "Cyber Security Initiative" aimed at educating companies on cyber risks and the hefty fines for data breaches under the GDPR. The initiative includes an https encryption test, under which Bavarian companies may have their websites tested (source document in German) and receive feedback from the DPA.

Italy

Italian DPA Executes Letter of Intent with Intelligence Services
On October 6, the Italian DPA and the General Department of Information for Security ("DIS") executed an agreement (source document in Italian) extending the requirement for the DIS to preliminarily inform the DPA about IT archives that will be used for security information collection. In his statement, the DPA Chairman noted that "the agreement has proven to be an efficient instrument for strengthening data protection of citizens within the context of intelligence services."

The Netherlands

Software Company Unlawfully Processes Data of Windows 10 Users
On October 6, the Dutch Data Protection Authority ("DDPA") determined (source document in Dutch) that a software company unlawfully processed personal data of Windows 10 users. According to the DDPA, the company did not clearly inform its users about the purposes for which the personal data was being collected, and users could not provide valid consent for the processing of their personal data.

DDPA Finds Unrestricted Publication of WHOIS Data Unlawful
On October 26, the DDPA found (source document in Dutch) that the public disclosure of WHOIS data of domain name holders that are natural persons by Dutch registries violates the Dutch Personal Data Protection Act (*Wet bescherming persoonsgegevens*). WHOIS data includes the domain name holder's name, address, email address, and telephone number. Under the ICANN 2017 Global Amendment to Registry Agreements, registries are required to publish personal data of WHOIS domain name holders without redactions. However, the DDPA stated that this constitutes a violation of the privacy law because there is no "legitimate interest" or "necessary legal grounds" for publishing the data.

Spain

AEPD Issues GDPR Compliance Tool
On September 6, the Spanish Data Protection Agency ("AEPD") issued "Facilita GDPR," a GDPR compliance tool (source document in Spanish) intended for companies and professionals who process low-risk personal data. The tool consists of a 20-minute online questionnaire through which companies and professionals can assess whether the data they process can be considered "low risk." The tool also provides required documents for GDPR compliance.

AEPD Finds Social Media Company in Violation of Spanish Data Protection Law
On September 11, AEPD issued (source document in Spanish) a final decision against a social media company in connection with its data processing activities and issued a fine of €1.2 million. According to the AEPD, the company collected user-processed special categories of data for advertising purposes without obtaining the data subjects' express consent.

United Kingdom

UK Introduces Data Protection Bill to Parliament
On September 14, the UK government introduced a data protection bill to the House of Lords. Among other changes, the legislation will update definitions required for implementation of the GDPR, extend the provisions of the GDPR to processing that would not otherwise be covered by EU law, implement the Law Enforcement Directive in the UK, and repeal the Data Protection Act of 1998.

ICO Publishes Guidance on Fees and Registration Changes for Post-GDPR Implementation
On October 5, the Information Commissioner's Office ("ICO") published a proposal that would require data controllers to pay a data protection fee under the Digital Economy Act after the repeal of the Data Protection Act of 1998. There will be three levels of payment reflecting the size of the organization, and the new fees would commence in April 2018.

UK Data Class Action Reaches High Court
On October 9, the nation's first data breach class action trial began. The case involves in the personal data of 5,500 individuals, whose information was allegedly leaked by a disgruntled employee of a major supermarket chain. Upon a determination of liability, the proceedings would move to assess damages.

ICO Advises Small Businesses Preparing for GDPR Implementation
On November 1, ICO began offering a dedicated advice line to provide assistance to small organizations preparing for implementation under the GDPR. This phone line complements ICO's online resources and follows ICO's "12 steps to take now" and "simple-to-use-SME toolkit" resources.

The following Jones Day lawyers contributed to this section: Paloma Bru, Laurent De Muyter, Undine von Diemar, Marina Foncuberta, Olivier Haas, Jörg Hladjk, Bastiaan Kout, Matthijs Lagas, Jonathon R. Little, Martin Lotz, Hatziri Minaudier, Giuseppe Mezzapesa, Selma Olthof, Audrey Paquet, Elizabeth Robertson, and Rhys Thomas.

[Return to Top]

Asia

Hong Kong

PCPD Completes Compliance Check of University After Screenshots of CCTV Footage Were Leaked to the Press
On September 20, the Privacy Commissioner for Personal Data ("PCPD") released a statement regarding the PCPD compliance check of a university. Pursuant to an investigation, security officers from the university released photos from CCTV of two students suspected of posting a controversial banner on campus. The PCPD issued guidance for protecting the rights of individuals and society at large for future investigations.

PCPD Hosts International Conference of Data Protection and Privacy Commissioners
On September 28, the PCPD issued a statement regarding the 39th International Conference of Data Protection and Privacy Commissioners ("ICDPPC"). PCPD Hong Kong hosted the annual five-day conference that included closed sessions and an awards dinner for ICDPPC Global Privacy and Data Protection Awards.

Singapore

Deputy Commissioner of PDPC Gives Keynote Speech at International Conference of Data Protection and Privacy Commissioners
On September 28, the Deputy Commissioner of the Personal Data Protection Commission ("PDPC") gave the keynote speech at the 39th International Conference of Data Protection and Privacy Commissioners in Hong Kong. The speech was titled "Singapore's Personal Data Protection Philosophies—Pivoting from Compliance to Accountability to Support Innovation."

PDPC Fines Insurance Company for Failing to Protect Personal Data of Insurance Policyholder
On October 11, the PDPC issued an opinion that fined an insurance provider for failing to make reasonable security arrangements to protect against the unauthorized disclosure of the personal data of its insurance policyholder and his dependent. The opinion found that the provider had mistakenly mailed personal data to one policyholder that was meant for another.

PDPC Announces Public Consultation on Proposed Revision of National Registration Identity Cards Advisory Guidelines
On November 7, the PDPC announced that the public consultation period for the proposed revisions to the National Registration Identity Cards ("NRIC") had opened. The proposed advisory guidelines address whether organizations can collect, use, or disclose an individual's NRIC number.

People's Republic of China

China Releases Additional Guidelines on Cybersecurity Law
On August 30, the National Information Security Standardization Technical Committee released three draft voluntary guidelines relating to the implementation of Cybersecurity Law: (i) Information Security Technology—General Security Requirements for Network Products and Services; (ii) Information Security Technology—Guide to Security Inspection and Evaluation of Critical Information Infrastructure; and (iii) Information Security Technology—Systems of Indicators for the Assurance of the Security of Critical Information Infrastructure (source documents in Chinese).

The following Jones Day lawyers contributed to this section: Michiru Takahashi, Li-Jung Huang, David Coogan, and Richard Zeng.

[Return to Top]

Australia

Privacy and Information Commissioner Releases Guide to Data De-Identification
On September 18, the Office of the Australian Information Commissioner ("Commissioner") and the Commonwealth Scientific and Industrial Research Organization's Data61 released The De-Identification Decision-Making Framework ("Framework"). The Framework is a practical guide to the de-identification of personal information held by Australian organizations. When discussing the Framework, the Australian Information and Privacy Commissioner noted that "[i]ntegrating the different perspectives on the topic of de-identification into a single, comprehensible framework is what this guide is all about."

Privacy and Information Commissioner Releases 2016–2017 Annual Report
On October 18, the Commissioner released its Annual Report for July 2016 to June 2017. According to the report, the Commissioner received 2,494 privacy complaints, an increase of 17 percent from 2015–16. The majority of these complaints related to the use, disclosure, and security of personal information. The Commissioner also closed 2,485 complaints during the period, an increase of 22 percent on the previous year. In addition, the Commissioner received 114 voluntary data breach notifications and 632 review requests under the Freedom of Information Act 1982.

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

[Return to Top]

Follow us on:

Jones Day is a legal institution with more than 2,500 lawyers on five continents. We are One Firm Worldwide℠.

Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. The electronic mailing/distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the author and do not necessarily reflect those of the Firm.

© 2017 Jones Day. All rights reserved. 51 Louisiana Avenue, N.W., Washington, D.C. 20001-2113.
www.jonesday.com