Privacy & Cybersecurity Update
Issue 3 | October 2014

JONES DAY

Jones Day Attorney Spotlight—Undine von Diemar

Europe is at the forefront of privacy legislation. With the upcoming General Data Protection Regulation, Europe will soon adopt more comprehensive privacy protections that, among other things, authorize significant fines for violations. A thorough understanding of European privacy laws and the compliance obligations that they create is increasingly critical to minimizing the risk of privacy-related liability to multinational companies, companies that operate within the EU, and those with business operations (such as e-commerce or vendors) that implicate EU data protection. Undine von Diemar coordinates Jones Day's European Privacy & Cybersecurity practice, which consists of a team of dedicated privacy lawyers across Jones Day's European offices. Undine's knowledge of European privacy laws, combined with her experience in advising on international data transfers, cloud-based and big data applications, and data breaches and investigations, make her a valuable resource for Firm clients addressing privacy protections in Europe.

United States

Regulatory—Policy and Best Practices

EDITORIAL CONTACTS

Mauricio Paez
New York

Undine von Diemar
Munich

Kevin Lyles
Columbus

Jonathon Little
London

Katherine Ritchey
San Francisco

Paloma Bru
Madrid

Jay Johnson
Dallas

Olivier Haas
Paris

Adam Salter
Sydney

Anita Leung
Hong Kong

Practice Directory

HOT TOPICS IN THIS ISSUE

FTC Report Criticizes Mobile Shopping Applications' Data-Use Disclosure Practices
On August 1, the Federal Trade Commission ("FTC") issued a report on mobile shopping applications. In it, the FTC found that such apps often fail to provide clear explanations of the use of consumer data, consumer liability, or processes for handling payment-related disputes. The report includes recommendations to companies that provide mobile shopping applications to consumers.

FTC Submits Comments to CFPB on Mobile Financial Services
On September 10, FTC staff issued comments in response to a request from the Consumer Financial Protection Bureau ("CFPB") for information regarding the use of mobile financial services by consumers. The staff comments highlight the risks posed to consumers by mobile financial services and provide recommendations for industry participants.

Regulatory—International Trade

ITC Identifies Obstacles to Digital Trade
The International Trade Commission's ("ITC") August report, "Digital Trade in the U.S. and Global Economies, Part 2," described data localization requirements as obstacles to digital trade. The Commission found that 82 percent of large firms and 52 percent of small and medium-sized enterprises in the communications sector believed such requirements to be barriers to trade. Data localization and privacy requirements in China, the EU, and Brazil presented the greatest obstacles to large firms, while Canada topped the list for small and medium-sized enterprises.

Regulatory—Financial Services

The American Bankers Association Provides Resources for Communicating with Customers Regarding Data Breaches
On September 9, the American Bankers Association announced its release of a set of tools for bankers to use in communicating with customers and the general public about cybersecurity breaches. The resources include, among other things, sample news releases and social media posts.

The American Bankers Association Releases Results of Study on Costs Associated with Target Data Breach
On September 8, the American Bankers Association released the results of its survey of the impact on banks from the Target consumer data breach. The study found that the average loss per fraudulently used payment card was $331 for debit cards and $530 for credit cards.

The U.S. Department of Treasury Addresses Cybersecurity
On September 12, at the National Association of Federal Credit Union's 2014 Congressional Caucus, the Acting Assistant Secretary for Financial Institutions delivered remarks encouraging financial services providers to adopt the National Institute of Standards and Technology's Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework") to help reduce the risk of data breaches.

New York Department of Financial Services Proposes Regulatory Framework for Virtual Currency Businesses, Including Cybersecurity Requirements
On July 17, the New York Department of Financial Services released a proposed "BitLicense" regulatory framework for firms providing virtual currency services. The regulatory program will require each licensee to maintain a cybersecurity program. The New York Department of Financial Services subsequently extended the period for comments on the draft regulations until October 21.

Government Accountability Office Report Urges Better Information Security at FDIC
The Government Accountability Office ("GAO") issued a July 17 report assessing the effectiveness of the Federal Deposit Insurance Corporation's ("FDIC") controls designed to protect the confidentiality, integrity, and availability of the FDIC's financial systems and information. The report recognized the steps taken by the FDIC to ensure better information security since a 2013 GAO audit but concluded that weaknesses in the FDIC's controls still remain.

Regulatory—Health Care

HIPAA One-Year Transition Period for Business Associate Agreements Expires
On January 17, 2013, the Office for Civil Rights of the U.S. Department of Health and Human Services ("HHS") issued its final HIPAA regulations, which included a one-year transition rule relating to a new requirement that existing business associate agreements must reflect the breach notification rules in the HITECH Act. Under the transition rule, business associate agreements that were in effect on or before January 25, 2013, must be amended on the earlier of (i) the date that such business associate agreement is renewed or modified on or after September 23, 2013, or (ii) September 22, 2014.

HHS Inspector General Finds Security Flaws in Testing and Certification of Electronic Health Records
In August, the Office of Inspector General ("OIG") for HHS issued a report on the Department's Temporary Program to test and certify Electronic Health Records ("EHRs") for use, titled "The Office of the National Coordinator for Health Information Technology's Oversight of the Testing and Certification of Electronic Health Records." The OIG found that the Temporary Program did not ensure adequate security and protection of electronic patient information. Specifically, the Program did not ensure that testing and certification bodies developed procedures to evaluate whether certified EHRs continued to meet federal standards after certification, nor did it ensure that the testing and certification bodies developed training programs to ensure the competency of their own personnel.

NIST and HHS Host Conference on Safeguarding Health Information and Assurance
On September 23–24, the National Institute of Standards and Technology ("NIST") and HHS's Office for Civil Rights hosted a conference on "Safeguarding Health Information: Building Assurance through HIPAA Security." The conference presented a number of papers and best practices for HIPAA compliance and enforcement actions.

FDA Finalizes Guidance on Medical Device Manufacturers' Practices for Managing Cybersecurity Risks
On October 1, the Food and Drug Administration ("FDA") finalized its guidance to medical device manufacturers to encourage manufacturers to consider possible cybersecurity risks when designing medical devices. The guidance, entitled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," also recommends manufacturers adopt a plan to manage system or software updates for such medical devices to reduce information security vulnerabilities.

FDA Announces Public Workshop and Requests Comments Regarding Medical Device Cybersecurity
The FDA announced a public workshop entitled "Collaborative Approaches for Medical Device and Healthcare Cybersecurity" to be held on October 21 and 22 in Arlington, Virginia. The purpose of the workshop is to bring together regulators and stakeholders from across the health care and public health sectors to discuss medical device cybersecurity risks and foster industrywide collaboration in the identification and management of such risks. The FDA is also soliciting electronic or written comments on all aspects of the public workshop topics, regardless of attendance at the public workshop. The deadline for submitting such comments is November 24.

Regulatory—Critical Infrastructure

NIST Calls for Cryptographic Transparency
On July 14, NIST's Visiting Committee on Advanced Technology issued a report that called for greater transparency in the development of NIST's cryptographic algorithms. The report follows public concern that NIST allowed its algorithms to be weakened to allow the National Security Agency backdoor access to information.

NIST Issues Updated Guide on Security and Privacy Controls
On July 31, the NIST issued a draft updated guide on Assessing Security and Privacy Controls in Federal Information Systems and Organizations under the Federal Information Security Management Act. The updated guide contains significant changes to the 2010 version and addresses four fundamental needs of federal agencies: (i) the need for new or updated assessment procedures; (ii) the need for a more granular breakdown of assessment objectives; (iii) the need for a more structured format and syntax for assessment procedures; and (iv) the need to support assessments of security and privacy capabilities and root-cause analysis of failure modes.

NIST Seeks Comments on the Cybersecurity Framework
On August 26, NIST requested comments on the private sector's initial experiences with the Cybersecurity Framework, released on February 12. NIST is seeking information about the use and awareness of the Cybersecurity Framework by critical infrastructure entities. NIST will use the comments to assist with adoption of the Cybersecurity Framework by private entities and incorporate the comments into future versions.

NIST Hosts Second Privacy Engineering Workshop
NIST furthered its Privacy Engineering initiative by holding its Second Privacy Engineering Workshop on September 15–16. The initiative was developed to provide guidance to information system users, owners, developers, and designers that handle personal information.

NIST Releases Revised Guidelines for Smart Grid Cybersecurity
In September, NIST announced the release of "NIST Interagency Report 7628 Revision 1, Guidelines for Smart Grid Cybersecurity." The guidelines promote the implementation by smart grid organizations of effective cybersecurity strategies that are tailored to each organization's smart grid-related characteristics, risks, and vulnerabilities.

DHS Office of Inspector General Recommends More Industry Involvement in Cybersecurity Efforts
On August 11, the Department of Homeland Security ("DHS") OIG released a report assessing DHS's progress in implementing the Enhanced Cybersecurity Services ("ECS") program. The voluntary ECS program was designed to encourage the sharing of classified and unclassified information related to cybersecurity threats between the private and public sectors. While the OIG report identified several ECS successes, the report also made several recommendations for program improvement, including encouraging DHS to improve program outreach to all critical infrastructure sectors.

Senator Asks Airline Carriers for Information on Consumer Data Retention
On August 18, Senator Jay Rockefeller (D-WV), Chairman of the Senate Committee on Commerce, Science, and Transportation, wrote a letter to executives of 10 airline carriers requesting information about the airlines' policies for retaining and protecting consumer data. In the letter, Senator Rockefeller noted that "[n]o comprehensive federal privacy law applies to the collection, use, and disclosure of consumer airline information," despite the fact that air travel requires carriers to collect an unusually large amount of personal information. In order to gauge airlines' responsiveness to consumer privacy concerns, the letter asked each airline to provide the Committee with a copy of its privacy policy and to inform the Committee about (i) what consumer data is retained and for how long, (ii) sources from which consumer data is obtained, (iii) measures taken to protect consumer

data, (iv) whether consumers have the right to view and correct their information, and (v) whether and how consumer data is sold to or shared with third parties.

Regulatory—Consumer Privacy

Retail Groups Back Tokenization to Curb Card Crime
Several retail industry groups—including the Merchant Advisory Group, the National Retail Federation, the National Restaurant Association, and the Retail Industry Leaders Association—released a statement on July 28 that called on stakeholders in the payments industry to embrace tokenization security standards as a means to protect consumers from cybercrime. Tokenization technology involves the generation of a unique, one-time-use token for every transaction.

FTC Solicits Comments on New Parental Verification Method
The FTC invited public comment on a new method for verifying parental consent under the Children's Online Privacy Protection Rule, 16 C.F.R. § 312, using a third-party common consent administrator.

DHS Issues Point-of-Sale Malware Warning
A July 31 DHS Advisory warned retailers and other companies of a new family of point-of-sale ("PoS") malware that recently was discovered and has been associated with several PoS data breach investigations. Using malware called Backoff, attackers have sought to gain access to company systems using brute force attacks through remote desktop applications. The attackers then deploy PoS malware to extract consumer payment data. The DHS Advisory includes mitigation and prevention strategies to address the threat from the Backoff malware.

Credit Union Industry Group Asks Congress to Enact National Data Security and Breach Notification Legislation for Retailers
On September 3, the National Association of Federal Credit Unions ("NAFCU") renewed its request to Congress to pass national data security and breach notification legislation in the wake of a recent data breach at a major retailer. The NAFCU's statement described the chilling effect data breaches can have on consumer activity and urged Congress to adopt a national data security standard for retailers, noting that credit unions and banks are already subject to such standards under the Gramm-Leach-Bliley Act.

Regulatory—Drones

Executive Order Expected on Drone Privacy Guidelines
Media outlets are reporting that President Obama plans to issue an executive order assigning responsibility to the National Telecommunications and Information Administration ("NTIA") for developing privacy guidelines related to the commercial use of unmanned aircraft, or commercial drones. The order is expected to direct the NTIA to facilitate a multistakeholder process for drafting a voluntary code of conduct that would establish best practices for the commercial use of drones, including addressing privacy concerns.

Judicial Rulings and Enforcement

Court Refuses to Sanction FTC in LabMD Case
On September 5, an administrative law judge denied LabMD's motion for sanctions against the FTC. LabMD's motion argued that the FTC deserved sanctions, including dismissal of the Commission's complaint, because it failed to verify the origin of a key file containing patients' sensitive health information that was allegedly discovered on a peer-to-peer sharing network.

District Court Refuses to Dismiss Breach Case on Standing Grounds
In a decision diverging from the national trend, the Northern District of California held

that users of software whose personal information was compromised in a data breach alleged an imminent threat of future harm sufficient to demonstrate standing. Many courts have interpreted the United States Supreme Court's recent decision in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013) as holding that an allegation of a possible future injury is insufficient for purposes of Article III standing, but the California court rejected that interpretation of the case. The court held instead that the consumers' allegations that hackers used the defendant's systems to decrypt credit card numbers and that some of the stolen data had been posted online constituted a sufficiently concrete and imminent threat of harm to satisfy *Clapper*. [A copy of the opinion can be provided upon request.]

Court Dismisses Neiman Marcus Class-Action Lack of Standing
A district court in Illinois granted Neiman Marcus's motion to dismiss a class-action lawsuit alleging the company was negligent in failing to protect consumer credit card information. The court held that the consumers did not have standing to bring the suit because they could not demonstrate concrete injury. The court explained that consumers would be reimbursed for any unauthorized credit card charges and could not show precise costs spent mitigating the risk of future fraudulent charges and identity theft, and that the loss of control over consumers' personal information was insufficiently concrete to confer standing.

Eleventh Circuit Will Hear Arguments in LabMD's FTC Challenge
On August 20, the Eleventh Circuit announced that it will hear oral arguments in LabMD's appeal of a district court's decision that the court could not interfere with the FTC's ongoing administrative enforcement actions against the company. A date for oral argument has not yet been set.

Senator Schumer Asks FTC To Investigate Mobile Fitness Devices
Senator Charles Schumer (D-NY) urged the FTC to investigate whether the makers of mobile fitness trackers are engaging in unfair and deceptive trade practices if they sell personal data to third parties without disclosing such transactions to consumers. His August 11 letter also asked the FTC to consider whether consumers should be given the chance to opt out of the sale of their personal data before they begin using the devices and applications.

FTC Approves Settlement with Companies Over Mobile Phone Applications
On August 13, the FTC approved final orders settling charges against two leading companies concerning mobile application security. The FTC alleged that by disabling SSL certificate verification and other things, the companies failed to adequately protect consumers' sensitive personal information, including credit card information and Social Security numbers, leaving them vulnerable to interception.

FTC Obtains Settlements in Two Suits Alleging Unlawful Collection of Children's Information
The FTC announced settlements in two cases in which it alleged that the companies' collection of children's personal information violated the Children's Online Privacy Protection Act. One company has agreed to pay $450,000 to settle charges that its mobile application failed to implement an effective age-screen, allowed customer registration by children under 13, and collected personal information including customer names and email addresses. The second company agreed to pay a $300,000 civil penalty to settle charges that its application targeted children, collected email addresses, and failed to follow the steps required under the Rule related to the collection of children's personal information.

FTC Announces Proposed Settlement in Children's In-App Purchase Case
The FTC announced a proposed settlement in a case in which it accused a company of violating Section 5 of the FTC Act, 15 U.S.C. § 45, by billing customers for in-app purchases without ensuring account-holder authorization for the charges. The proposed settlement requires the company to provide at least $19 million in refunds to consumers,

change its billing practices to obtain express consent before billing, provide consumers an opportunity to withdraw consent for future charges, and contact all consumers who made an in-app charge to inform them of the refund process.

Complaint Alleges Noncompliance with Safe Harbor Framework
The Center for Digital Democracy ("CDD") has filed complaints with the FTC for alleged noncompliance with the U.S.–EU Safe Harbor Framework by various U.S. companies. The CDD's actions may lead to increased enforcement by the FTC. In June, the FTC announced that it has approved final orders settling charges against 14 companies for falsely claiming to participate in the U.S.–EU Safe Harbor Framework. Generally, the Safe Harbor Framework is under review, and the European Union has made recommendations to improve it.

SEC Charges a Bank's Business Unit for Failing to Protect Confidential Trading Data of Subscribers
On July 25, the business unit of a large bank operating an alternative trading system ("ATS"), agreed to pay $5 million to settle the SEC's charges for violating sections of Rule 301 of Regulation ATS. The regulation establishes safeguards for protecting the confidential trading information of subscribers. The unit was alleged to have violated the regulation by allowing a technology affiliate to access and use the confidential trading information of subscribers without their consent and without disclosing the practice in its regulatory filings.

Verizon Settles with FCC Over Notice and Consent
On September 3, the FCC announced its settlement with Verizon following an investigation into potential violations of the FCC's privacy rules. The settlement represents the largest payment for an FCC case based solely on privacy.

State Attorneys General Respond to Home Depot Data Breach
In the wake of the data breach at Home Depot, attorneys general for Pennsylvania, Illinois, and others are investigating and advising victims on how to secure their personal information.

Legislative—Federal

U.S. House of Representatives Passes Cybersecurity Bills
On July 28, the United States House of Representative passed four bills regarding cybersecurity. The National Cybersecurity and Critical Infrastructure Protection Act (H.R. 3696) would codify the responsibilities of DHS and foster collaboration between DHS and the private sector to improve critical infrastructure protection and incident response. The Critical Infrastructure Research and Development Advancement Act of 2014 (H.R. 2952) assigns responsibility to DHS for creating a new cybersecurity technology research and development plan. The House also passed bills that would improve DHS's ability to hire talented cybersecurity personnel (H.R. 3107) and require federal government websites to obtain certification before initiating a process that collects personal information (H.R. 3635). The bills must be approved by the Senate and President Obama before becoming law.

DHS Secretary Calls for Cybersecurity Legislation
On September 9, *The Hill* published an editorial by the Secretary of DHS that urged Congress to pass cybersecurity legislation, stating that "DHS has reached a point that requires the help of Congress" and noting that "some private companies can and do resist sharing information with DHS about cyber attacks on their systems, for fear of potential liability."

Legislative—States

California Enacts Amendments to Breach Notification Law
California bill A.B. 1710 was approved by lawmakers in August and signed into law by Governor Brown on September 30. Set to take effect on January 1, 2015, the bill extends data security requirements to businesses that "maintain" personal information and prohibits entities from selling, offering for sale, or advertising an individual's Social Security number. Please refer to the *Jones Day Commentary*, "California Adds More Teeth to Its Data Breach Notification Law," for more information.

[Return to Top]

Canada

Canada Claims China Responsible for National Research Council Cyberattack
On July 29, Canada announced that it believed the National Research Council ("NRC"), Canada's research and technology organization, was the victim of a Chinese state-sponsored cyber intrusion. The Canadian government confirmed that the NRC's networks do not operate within the broader network of the federal government and there was no evidence of a broader data compromise.

GPEN Publishes Results of Online Sweep on Compliance of Mobile Applications with Data Protection Framework
The Global Privacy Enforcement Network ("GPEN"), a gathering of 27 data protection authorities worldwide, recently examined more than 1,200 mobile apps, both paid and free of charge, and public and commercial, in categories such as leisure, health, physical exercise, and bank transactions. The analysis determined that (i) only 15 percent of the apps examined provided clear information to users as to how their personal data was to be collected, used, and disclosed, (ii) nearly a third of the apps analyzed requested excessive permission regarding their functions, and (iii) in 59 percent of the apps, it was not easy for the participants to find information relating to privacy before installation.

The following Jones Day attorneys contributed to the United States and Canada sections: Chris Cogburn, Bart Green, Jay Johnson, Colin Leary, Gabe Ledeen, Nicole Perry, Scott Poteet, Katherine Ritchey, Jessica Sawyer, Anand Varadarajan, and Zach Werner.

[Return to Top]

Latin America

Brazil

Brazilian House of Representatives Considers Bill of Law Criminalizing Fake User Profiles on Internet
On July 2, a bill of law (source document in Portuguese) proposing the criminalization of fake user profiles on the internet was introduced to the Brazilian House of Representatives. The Bill proposes to amend article 307 of the Criminal Code (source document in Portuguese), criminalizing the use of a fake profile on the world wide web. If approved, the law will be applied to those who attribute to themselves or to a third party a fake identity, including through the internet or any other electronic platform, with the intent of harming, intimidating, threatening, obtaining an advantage over, or damaging a third party to the agent's benefit or the benefit of a third party.

Brazilian Court Rules Anonymous Apps Unconstitutional
On August 18, a Brazilian civil court in Vitória, Espirito Santo, granted a preliminary injunction (source document in Portuguese) to a public prosecutor, prohibiting certain companies from distributing an anonymous sharing app and Microsoft from distributing the Windows Phone client, Cryptic. Chapter Five, Article 1 of the Brazilian Constitution specifies that "the expression of thought is free, anonymity being forbidden"

and provided the legal justification upon which the Brazilian judge rested his decision.

Brazilian Arbitration Chamber Specializing in Information Technology and e-Commerce Initiates Activities
Created in 2013, the Brazilian Chamber of Mediation and Arbitration of Internet Technology, E-Commerce, and Communication recently started its activities, acting as an arbitrage court composed of specialists in laws applicable to information technology. The Chamber mediates conflicts and legal discussions. It is independent and is focused on the solution of conflicts involving electronic frauds, violations of privacy, and virtual bids, among other matters.

Chile

Chilean Senate Approves Constitutional Amendment Project
On September 9, the Senate of the Republic of Chile approved in general (source document in Spanish) a proposed constitutional amendment that seeks to constitutionally protect personal data. During the parliamentary debate, senators discussed the use of databases, the need to clearly differentiate between public and private records, the relevance of having a public institution to safeguard this new right, and the repercussions of including owner consent as a requirement for the processing of personal data. The project was returned to the Committee on Constitution, Legislation, Justice, and Regulation for further review and discussion. Congressmen will have until October 13 to file recommendations.

Mexico

Mexican Data Protection Authority Votes Against Privacy Challenge of Telecom Law
On August 13, the Mexican Data Protection Authority ("IFAI") voted not to challenge (source document in Spanish) the Federal Telecommunications and Broadcasting Act 2014 (source document in Spanish) in the Mexican Supreme Court. Four out of seven IFAI commissioners voted against a proposal to use the IFAI's powers to challenge several articles of the Act on the grounds that they violated the constitutional rights to privacy and the protection of personal data. The Act came into effect on August 13 and is controversial for reducing freedom to access information, extending data retention periods, and increasing the surveillance powers of the Mexican authorities.

IFAI, IMSS, and Profedet Initiate Working Group to Improve Method by Which Citizens Can Access Personal Data
On August 28, the IFAI, the Mexican Social Security Institute, and the Mexican Federal Office for the Protection of Labor installed an interagency working group (source document in Spanish) to expedite the attention to requests by rightholders for access to their personal information.

The following Jones Day attorneys contributed to the Latin America section: Guillermo Larrea and Virginia Uelze.

[Return to Top]

Europe, Middle East, and Africa

European Union

European Commission Designates Three New Members
The European Commission designated three new members of particular relevance to privacy and data security.
- Read More

European Commission Promulgates Technical Standards to Make RFID Use Data

Protection Compliant
The European Commission made available three new EU technical standards to help users of radio frequency identification ("RFID") tags comply with the requirements under the Data Protection Directive (95/46/EC). RFID tags are used to automatically identify and track objects by wirelessly exchanging electronically stored information with so-called readers. The illicit tracking of RFID tags poses a risk to personal location privacy as exact movement profiles can be generated. The first of the new standards provides procedures to develop risk assessment templates for retailers and other entities that supply goods with RFID tags, detailing how they should manage their use (EN 16571:2014). The second new standard is aimed at informing consumers that a product includes an RFID tag by attaching an EU-wide logo to the product (EN 16656:2014). The third new standard is aimed at informing consumers that an RFID system is in use (EN 16570:2014). The new standards are to be implemented by the EU member states at the national level by December 31, 2014, and January 31, 2015, respectively, by publication of an identical national standard or by endorsement.

Article 29 Working Party

Article 29 Working Party Publishes Questions for Search Engines on Right to be Forgotten
The Article 29 Working Party (an independent advisory body composed of European data privacy authorities) met on July 24 with representatives of leading U.S.-based search engines to discuss the practical implementation of the ruling of the European Court of Justice regarding the right to be forgotten (case C-131/12, *Costeja*). The Article 29 Working Party also published a list of questions addressed to the search engines. The aim of the Article 29 Working Party's initiative is to publish guidelines, which are expected to be finalized in November.

Article 29 Working Party Releases Statement on Invalidation of Data Retention Directive
The Article 29 Working Party adopted a statement on the April 8 ruling of the European Court of Justice that invalidated the Data Retention Directive 2006/24/EC. The Working Party welcomed the ECJ decision, which was based on the fact that the data retention principles set forth by the Directive (i) entailed substantial interference with the fundamental rights to privacy and data protection, (ii) failed to limit such interference with what is necessary for the purpose of fighting "serious crime," and (iii) failed to define the guarantees applicable in connection with the data retention principles of the Directive. The Working Party pointed out that even though the national measures implementing the Directive are not directly affected by the invalidation of the Directive, member states should ensure that their national framework relating to data retention is in line with the grounds of the ECJ decision. In particular: (i) the national legal data retention obligations should be differentiated depending on the types of data, (ii) access by national authorities should be limited to what is necessary and subject to substantive and procedural conditions, and (iii) the data storage conditions imposed by law should ensure effective protection against unlawful access. Failure of national data retention regulations to comply with such principles may result in such regulations being challenged before national courts.

Article 29 Data Protection Working Party on Big Data
The Article 29 Working Party commented in a letter to the White House on the U.S. report titled "Big Data: Seizing Opportunities, Preserving Values." The Working Party welcomed the approach outlined in the report to extend the existing privacy protection in the United States to non-U.S. persons and to support greater interoperability of privacy standards at the international level. The Working Party stated in particular that "it has no reason to believe that the EU data protection principles, as they are enshrined in Directive 95/46/EC, are fundamentally challenged by the development of big data." In this context the Working Party emphasized the importance of observing its various policy documents on the issue, setting out standards that might prove to be challenging for big data applications (e.g., Opinion 05/2014 on Anonymisation Techniques, Opinion 01/2014 on

the Application of necessity and proportionality concepts and data protection within the law enforcement sector, Opinion 03/2013 on purpose limitation, Opinion 06/2013 on open data and public sector information re-use, and Opinion 06/2014 on legitimate interest).

European Data Protection Supervisor

European Data Protection Supervisor Publishes Position Paper on Transfer of Personal Data to Third Countries
The European Data Protection Supervisor ("EDPS") published a July 14 paper titled "The Transfer of Personal Data to Third Countries and International Organisations by EU Institutions and Bodies." The paper provided guidance to EU institutions and bodies on interpreting and applying the rules set out in Regulation 45/2001 in the context of international transfers of personal data.

European Data Protection Supervisor Workshop on Privacy, Consumers, Competition, and Big Data
On June 2, the EDPS held a workshop on the policy implications of the rapidly expanding digital market for the fields of data protection, competition, and consumer protection. Its report highlights the challenges that big data poses to competition reviews and concludes, among other things, that privacy will need to be a consideration in competition matters in the future.

European Conference of Data Protection Authorities

European Conference of Data Protection Authorities Adopts Resolution Supporting Revision of Convention 108 of Council of Europe
On June 5, the European Conference of Data Protection Authorities adopted a resolution supporting the Council of Europe's efforts to modernize the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). The resolution asked to preserve and, where possible, increase the current level of protection afforded by the Convention (e.g., by introducing an obligation to give notice of data security breaches).

France

French DPA Sanctions Telecoms Operator for Data Security Breach
In April, a major French telecoms operator notified CNIL, the French data protection authority ("DPA"), of a major personal data breach in connection with an email campaign and noted that the breach resulted from a technical failure of one of the operator's service providers. The CNIL investigated the case and, in an August 7 decision (source document in French), concluded that, even though the technical issue had been resolved, the telecoms operator had not complied with its obligation to implement all useful means to ensure the security of the personal data that is processed. The CNIL particularly pointed out that the operator (i) should have carried out a prior security audit of its service provider before entrusting the service provider with the email campaign; and (ii) had breached its security obligations by communicating personal data files to its service providers without securing the communications and by failing to include in its agreements with the data processors the necessary data security and confidentiality clauses required by law.

Germany

Germany Heads Toward Legislative Approach to IT Security
Despite the EU Cybersecurity Directive currently under discussion, the German Ministry of the Interior presented a draft bill (source document in German) that focuses on IT security standards for companies operating critical infrastructure—namely, those in telecommunications, energy, transport, nutrition, banking, insurance, etc.

Bavarian DPA Rules Dashcams Illegal
The Bavarian DPA enjoined the use of a dashcam. Its decision recently was affirmed by a judgment of the court of Ansbach (source document in German). According to the decision, a dashcam user processes personal data and is therefore subject to the Federal German Data Protection Act. Furthermore, the law prohibits such processing, because fundamental rights and the right of informational self-determination prevail over the need for evidence in the event of a car accident. Following the judgment of the Ansbach court, a Munich court held (source document in German) in a civil proceeding that dashcam material cannot be used as evidence because it was unlawfully obtained.

Ireland

Ireland DPC Wins Fines Against Company Directors Under Data Protection Acts
Ireland's Data Protection Commissioner ("DPC") announced that it had secured fines against the directors of a private investigation company for violating the Data Protection Acts, 1988 and 2003. The prosecutions marked several "firsts" for the office: its first prosecution against private investigators, its first prosecution of a company's directors for their role in data protection offenses, and its first prosecution for knowingly or recklessly obtaining or disclosing personal data or information without the consent of the data controller.

Italy

Italian DPA Issues Data Processing Measures for Adoption by Google
In a July 10 decision, the DPA provided specific measures that Google must take to make the processing of personal data under its new privacy policy fully compliant with Italian privacy law. In particular, Google must, among other things, obtain the prior consent of its users in Italy in order to properly use their personal data for profiling and behavioral advertising activities and must define the retention period of the processed data.

The Netherlands

Dutch National Centre Investigates Reported Theft of 1.2 Billion Email Address and Password Combinations
Following media reports concerning the theft of 1.2 billion email address and password combinations by a Russian criminal organization, the Dutch National Centre for Cyber Security ("NCSC") investigated and shared available information with the central government as well as other relevant organizations. The NCSC confirmed that it closely monitors new developments (source document in Dutch) and contacted Holden Security, the American company that purports to have information concerning the stolen information, as well as various international partners, in order to learn more about the stolen data. The NCSC has pointed to guidance such as "10 Tips for Safe Internet Use" (source document in Dutch) and "Help! My Data Leaked On The Internet" (source document in Dutch) in order to prevent theft and misuse of personal data on the Internet.

Dutch Secretary of Security and Justice Addresses Social Media Use Experiments
Media reported in June that Facebook experimented in 2012 with certain users by manipulating the information posted on its site, finding that it could make people feel more positive or negative through a process of "emotional contagion." In light of those reports, the Ministry of Security and Justice was asked (source document in Dutch) to respond to several questions on the privacy of social media users. In response, the secretary stated that whether social media services should request explicit consent of the user for such experimentation depends on the arrangement between the user and the social media provider. According to the secretary, under Articles 33 and 34 of the Personal Data Protection Act, search engine and social media service providers are obligated to inform users regarding the purpose of the processing of personal data, and if the conditions of use are sufficiently clear, specific user approval is not required.

Dutch DPA Intends to Declare Notification of the Employers' Association "ZorgZijn Werkt" Warnings Register Lawful
The Employers' Association provided notice of its intent to establish a warning database to register unjust and criminal acts by caretakers against clients. The Association, having no license based on the Private Security Organizations and Detective Agencies Act, will necessarily process criminal information and/or information about unlawful or objectionable behavior for the benefit of third parties. The DPA concluded (source document in Dutch) that it intends to declare the notification lawful.

Russia

Russia May Rush Deadline for Data Localization: Parliament Proposes Deadline of January 1, 2015
In July, President Putin signed into law a number of restrictive amendments (source document in Russian) to Russia's existing data security laws, now known as the Federal Law "On Amendments to Certain Legislative Acts of the Russian Federation for Clarification of the Procedure of Personal Data Processing in Information and Telecommunication Networks." The law requires that any databases used for gathering, storage, and processing of data relating to Russian citizens be located in Russia. Although these amendments are scheduled to become effective in September 2016, the lower chamber of the Russian Parliament is now considering a bill (original source document in Russian) amending this new law to bring the effective date forward to January 1, 2015. It is not yet clear if the new deadline will be put forward or postponed.

United Kingdom

New UK Offense to Apply to Serious Cyberattacks
The UK government has proposed new measures in the Serious Crime Bill to punish serious cyberattacks. The new law would introduce a new offense committed if a person carries out an unauthorized act in relation to a computer that causes or creates a significant risk of serious damage to human welfare, the economy, the environment, or national security in any country. The offense would be punishable by up to 14 years' imprisonment and/or a fine, or life imprisonment where the act caused death, illness, injury, or serious damage to national security.

The following Jones Day attorneys contributed to this section: Paloma Bru, Undine von Diemar, Laurent de Muyter, Olivier Haas, Olaf Hohlefelder, Ted Kroke, Jonathon Little, Afra Mantoni, Serena Nasuti, Selma Olthof, and Sergei Volfson.

[Return to Top]

Asia

China

Standard Terms of Internet-Trading-Platform Contracts Address Seller's Liability with Consumer's Personal Information
On July 30, the State Administration of Industry and Commerce promulgated guidelines (source document in Chinese) on the Standard Terms of Internet-Trading-Platform Contracts (Article 10) to provide that, under the standard terms, the seller cannot preclude its liability with respect to the security of the consumer's personal information.

Local People's Governments Must Report to Superior Department if Disclosing Personal Privacy Information
On August 7, the State Council promulgated interim regulations (source document in Chinese) on the Disclosure of Enterprise Information (Article 3) to provide that relevant departments of local people's governments at or above the county level shall report to their respective superior competent departments for approval if the enterprise information

to be disclosed by the former implicates personal privacy.

Personal Information to be Deleted when Publishing Administrative Penalty Information
On August 19, the State Administration for Industry and Commerce promulgated interim provisions (source document in Chinese) on the Publication of Administrative Penalty Information. Article 6 provides that when publishing administrative penalty information, the administrations shall delete relevant personal information.

Chinese Convict British-American Investigators for Selling Illegally Obtained Personal Information
A Chinese court in Shanghai convicted a British-American couple of illegally purchasing the personal information of more than 250 Chinese citizens and selling the information to clients. The couple's company had been hired by GlaxoSmithKline to conduct an internal investigation at the time of their arrest. The arrest took place days after the Chinese government publicly alleged that Glaxo employees had participated in bribery.

Hong Kong

Hong Kong Recruitment Media Pledges to Fight Blind Recruitment Advertisements
On August 4, six major recruitment media companies pledged to fight blind recruitment advertisements. Such advertisements solicit job applicants' personal data without disclosing the advertisers' identities, in violation of the Personal Data (Privacy) Ordinance for failing to collect personal data by lawful and fair means.

Hong Kong Privacy Commissioner Urges Expansion of Do-Not-Call Registers to Include Person-to-Person Calls
On August 5, the Privacy Commissioner for Personal Data urged the Administration to expand the do-not-call registers to include person-to-person calls. The do-not-call registers allow telephone subscribers to register their telephone numbers to prevent unsolicited commercial electronic messages.

Japan

Japanese Government Submits Bill for Basic Act of Cybersecurity
On June 11, a bill (source document in Japanese)—Basic Act of Cybersecurity—was submitted to the House of Representatives. The bill, aimed at improving cybersecurity, was passed by the House of Representatives on June 13 and sent to the House of Councillors.

Ministry of Economy, Trade, and Industry Reviews Ministerial Guidelines on Personal Information Protection Act
On August 15, the minister of the Ministry of Economy, Trade, and Industry ("METI") announced that the ministry would review and revise its ministerial guidelines on the Personal Information Protection Act. In the wake of a recent massive customer data breach incident, METI found that the guidelines needed to be revised in order to reinforce certain security measures to be taken by companies, including improved control and supervision over data processing vendors.

Singapore

Singapore Penalizes First Offenders Under New Personal Data Protection Act
In August, Star Zest Home Tuition and its sole director became the first offenders penalized under the do-not-call rules of Singapore's Personal Data Protection Act of 2012 for sending advertising messages to Singapore phone numbers registered with the Do Not Call Registry. The agency and director were fined S$39,000.

Personal Data Protection Commission Publishes Advisory Guidelines for Education, Health Care, and Social Service Sectors
On September 11, the Personal Data Protection Commission of Singapore published three sector-specific advisory guidelines for the education, health care, and social services sectors respectively, bringing the total number of advisory guidelines published to date to five (the other two sectors covered were telecommunications and real estate agency).

Do Not Call Registry Results Valid for 30 Days
Effective July 2, organizations that compare internal marketing lists with the Do Not Call Registry can rely on the results of that registry for up to 30 days (down from the previous 60 days).

Taiwan

Ministry of Justice Submits Draft Bill to Relax Requirements Under Communication and Surveillance Act
The Ministry of Justice submitted a draft bill for the Executive Yuan (source document in Chinese) to relax the limitations imposed on prosecutors' requests for communication records and to allow prosecutors to obtain such records in an emergency.

Executive Yuan to Submit Bill Authorizing Establishment of National Communication Safety Technology Center
The Executive Yuan seeks to submit a bill (source document in Chinese) authorizing the establishment of a National Communication Safety Technology Center. If such a bill is passed, the Executive Yuan can relocate a technical center (source document in Chinese) employing approximately 100 people to the jurisdiction of the Ministry of Science and Technology. The current proposal is that the National Communication Safety Technology Center will focus on certain aspects of information safety in the public and private sectors.

National Communication Commission Aims to Address Issues Derived from Cross-Strait Serving Trade Agreement
Due to the "China issue," the National Communication Commission ("NCC") prohibits the use of telecom systems built by PRC manufacturers and has imposed restrictions on PRC nationals entering certain telecom equipment rooms. The NCC also has imposed strict rules on capital investments from the PRC in "Type II Telecommunication" in Taiwan, requiring PRC companies to first obtain ISO/IEC certification before making any such investment in Taiwan, preventing them from removing customer data, sales department and system/equipment to the PRC, and precluding them from providing computer maintenance to Taiwanese telecom companies. The NCC aims to provide unified definitions for all services relating to telecommunication so that the types of investments allowed under the Cross-Strait Serving Trade Agreement are clearly defined.

The following Jones Day attorneys contributed to this section: Po-Chien Chen, Elaine Ho, Alice Hu, Anita Leung, and Michiru Takahashi.

[Return to Top]

Australia and New Zealand

Australian Law Reform Commission Proposes Changes to Australian Privacy Laws Regarding Serious Invasions of Privacy
The Australian Law Reform Commission recently released a report that was commissioned by the Attorney General of Australia on "Serious Invasions of Privacy in the Digital Era." The report recommends that a statutory civil cause of action for serious invasions of privacy be introduced in a Commonwealth Act. The proposed cause of action would be actionable only where (i) the invasion of privacy is serious; (ii) the invasion is committed intentionally or recklessly (with mere negligence being insufficient); (iii) the invasion is either by intrusion into an individual's private space or by misuse of private information;

(iv) an objective person in the position of the plaintiff would have a reasonable expectation of privacy in the circumstances; and (v) the public interest in upholding privacy outweighs other public interests.

The following Jones Day attorneys contributed to this section: Adam Salter and Nicola Walker.

[Return to Top]

Jones Day Privacy and Cybersecurity Lawyers

Emmanuel G. Baud
Paris

Jean-Paul Boulee
Atlanta

Wolfgang G. Büchner
Munich

Shawn Cleveland
Dallas/Houston

James A. Cox
Dallas

Walter W. Davis
Atlanta

Timothy P. Fraelich
Cleveland

Joshua L. Fuchs
Houston

Karen P. Hewitt
San Diego

Robert W. Kantner
Dallas

Elena Kaplan
Atlanta

Jeffrey L. Kapp
Cleveland

J. Todd Kennard
Columbus

Ted-Philip Kroke
Frankfurt

Anita Leung
Hong Kong

Jonathon Little
London

Kevin D. Lyles
Columbus

John M. Majoras
Columbus/Washington

Todd McClelland
Atlanta

Jason McDonell
San Francisco

Carmen G. McLean
Washington

Daniel J. McLoon
Los Angeles

Janine Cone Metcalf
Atlanta

Caroline N. Mitchell
San Francisco

Matthew D. Orwig
Dallas/Houston

Mauricio F. Paez
New York

Chaka M. Patterson
Chicago

Katherine S. Ritchey
San Francisco

Elizabeth A. Robertson
London

Adam Salter
Sydney

Gregory P. Silberman
Silicon Valley

Michiru Takahashi
Tokyo

Rhys Thomas
London

Michael W. Vella
Shanghai

Amy E. Vieta
New York

Undine von Diemar
Munich

Toru Yamada
Tokyo

Sidney R. Brown
Atlanta

Paloma Bru
Madrid

Amanda B. Childs
Dallas

Michele L. Gibbons
Houston/New York

Jay Johnson
Dallas

Guillermo E. Larrea
Mexico City

Christopher J. Lopata
New York

Margaret I. Lyle
Dallas

Stefano Macchi di Cellere
Milan/London

Georg Mikes
Frankfurt

Michael G. Morgan
Los Angeles

Sergei Volfson
Moscow

Olivier Haas
Paris

David L. Odom
Dallas

Po-Chien Chen
Taipei

Nigel Chin
Singapore

Christopher S. Cogburn
Atlanta

Laurent De Muyter
Brussels

Adrian Garcia
Dallas

Steven G. Gersten
Dallas

Bart Green
Irvine

Joshua Grossman
New York

Javier Gutiérrez Ponce
Madrid

Aaron M. Healey
Columbus

Elaine Ho
Singapore

Nancy L. Hoffman
New York

Nandini Iyer
Silicon Valley

Bastiaan K. Kout
Amsterdam

Colin Leary
San Francisco

Gabriel Ledeen
San Francisco

Afra Mantoni
Milan

Susan M. O'Connor
New York

Nicole M. Perry
Houston

Scott B. Poteet
Dallas

Brandy Hutton Ranjan
Columbus

Jessica M. Sawyer
Los Angeles

Raquel Travesí
Madrid

Virginia Uelze
São Paulo

Anand Varadarajan
Dallas

Nicola Walker
Sydney

Zachary M. Werner
New York

Natalie A. Williams

Marc L. Swartzbaugh
Cleveland

Atlanta

Follow us on:

Jones Day is a legal institution with 2,400 lawyers on five continents. We are One Firm Worldwide[SM].

JONES DAY | **Privacy & Cybersecurity Update**
Issue 3 | October 2014

JONES DAY

United States | Canada | Latin America | EU, Middle East & Africa
Asia | Australia & New Zealand

Europe

European Union

European Commission Designates Three New Members

The European Commission designated three new members of particular relevance to privacy and data security:

Vera Jourova, former Czech minister, will head the Directorate-General Justice, which remains responsible for data protection rules (including the reform currently discussed before the European Council and Parliament). Her mission statement includes "ensuring the swift adoption of the EU data protection reform" and "concluding negotiations on a comprehensive EU-U.S. data protection agreement which provides justiciable rights for all EU citizens, regardless of where they reside, as well as reviewing the Safe Harbour arrangement."

Guenther Oettinger, outgoing EU energy commissioner from Germany, will be in charge of digital economy and society. As part of his mission statement, Commissioner Oettinger will prepare "ambitious legislative steps towards a connected Digital Single Market" and assess the necessity of proposing new measures, as "more ambition should be added to the ongoing reform of our telecoms rules." He also will work on "a plan to make the EU a leader in cyber security preparedness and trustworthy ICT, and to increase the confidentiality of communications." Finally, he will support finalizing

EDITORIAL CONTACTS

Mauricio Paez
New York

Undine von Diemar
Munich

Kevin Lyles
Columbus

Jonathon Little
London

Katherine Ritchey
San Francisco

Paloma Bru
Madrid

Jay Johnson
Dallas

Olivier Haas
Paris

Adam Salter
Sydney

Anita Leung
Hong Kong

Practice Directory

the negotiations on "an ambitious Data Protection Regulation in 2015" and reform the E-Privacy Directive.

Andrus Ansip, former Estonian Prime Minister, has been designated Commission Vice President in charge of the digital single market. In that role, he will review and coordinate the actions of Vera Jourova and Guenther Oettinger. His mission statement includes "break[ing] down national silos in telecoms regulation [and] in copyright and data protection," as "companies will need to be subject to the same data protection and consumer rules, regardless of where their servers are based." He will aim to conclude both the negotiations on the reform of data protection rules and the review of the Safe Harbor arrangement with the U.S.

[Return to Homepage]

Follow us on:

Jones Day is a legal institution with 2,400 lawyers on five continents. We are One Firm Worldwide[SM].