JONES DAY | **Privacy & Cybersecurity Update**
Issue 2 | July 2014

JONES DAY

Jones Day Attorney Spotlight—Chaka Patterson

Increasingly, U.S. State Attorneys General are devoting significant resources to privacy and data breach matters, both pursuant to specific state laws and to their general consumer protection duties. Chaka Patterson is an important part of Jones Day's Privacy & Cybersecurity practice due to the significant risks and unique issues presented by State Attorneys General. Chaka served as Chief of the Special Litigation Bureau in the Office of the Illinois Attorney General, where he led a team of attorneys who focused on high-profile cases and targets. Chaka's knowledge of the inner workings of State Attorneys General Offices—combined with his experience with key laws, including false claims, consumer fraud, and unfair business practices statutes—make him a valuable asset to clients facing State Attorney General inquiries into privacy and data breach matters.

United States

Regulatory—Policy and Best Practices

White House Concludes U.S. Laws are Sufficient for Regulating Cybersecurity
The White House Cybersecurity Coordinator posted a blog entry on May 22 stating that the Obama administration has concluded that existing regulatory laws and voluntary efforts are sufficient to address cybersecurity threats facing critical infrastructure in the private sector. The blog also indicated

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

that there will be a continued joint agency effort to "investigate and leverage opportunities to improve the efficiency, clarity, and coordination of existing regulations."

SEC Commissioner Urges Corporate Boards to Focus on Cyber-Risk Management
On June 10, Commissioner Luis Aguilar from the Securities and Exchange Commission said in a speech at the New York Stock Exchange that corporate boards must ensure that cybersecurity preparedness is a critical part of their risk oversight responsibilities. At a minimum, said Aguilar, boards should work with management to assess corporate policies to see how they match up to the National Institute of Standards and Technology's framework for cybersecurity infrastructure. Boards also should have a "clear understanding" of company personnel primarily responsible for cybersecurity risk oversight and for ensuring the adequacy of risk management practices.

FCC Challenges Companies to Proactively Manage Cybersecurity Risks
On June 12, at an American Enterprise Institute event in Washington, D.C., Federal Communications Commission ("FCC") Chairman Tom Wheeler urged the private sector to be more proactive in addressing increasing cybersecurity threats. He also indicated that the FCC's developing cybersecurity strategy will center on network protection, information and data sharing, and situational awareness.

GAO Releases Report on Maritime Cybersecurity
The Government Accountability Office ("GAO") released a report on June 5 stating that the Department of Homeland Security ("DHS"), the U.S. Coast Guard, and the Federal Emergency Management Agency need to more effectively address maritime cybersecurity. According to the report, efforts to address cybersecurity in the maritime port environment have been "limited" and generally have not identified or addressed potential maritime cyber-related threats or vulnerabilities.

GAO Reports Federal Agencies Must Improve Cyber Incident Response
On May 30, the GAO issued a report finding that 24 agencies, including the Departments of Justice, Homeland Security, Energy, and Veterans Affairs, need to improve cyberattack response as the threat of breaches increases.

NIST Issues Summary of Privacy Workshop
On May 21, the National Institute of Standards and Technology ("NIST") issued a summary of the workshop previously held on April 9–10 to determine whether to add privacy controls to the Framework for Improving Critical Infrastructure Cybersecurity. NIST will prepare a report on privacy engineering hurdles and will recommend a privacy risk framework and methodology for designing systems that encourage privacy.

NTIA Requests Public Comment on Proposed Consumer Privacy Bill of Rights
On June 3, the National Telecommunications and Information Administration ("NTIA") announced that it is leading a review of a consumer privacy rights proposal unveiled by the White House in 2012. NTIA requested public comment by August 5, 2014, on the proposed consumer "privacy bill of rights" and specifically whether the privacy bill of rights adequately addresses concerns regarding the risks posed by big data.

New York Attorney General Releases Report on Rise of Data Breaches
In a July 15 report entitled "Historical Examination of Data Breaches in New York State," the New York Attorney General revealed that the number of breaches in New York more than tripled between 2006 and 2013. More than 22 million personal records have been exposed since 2006, and breaches cost companies doing business in New York approximately $1.37 billion in 2013 alone.

California Attorney General Issues Guidelines on Privacy Practices
The California Attorney General's Office recently issued a set of guidelines, titled "Making Your Privacy Practices Public" ("Guidelines"), designed to help companies develop "meaningful" privacy policies that provide transparency, accountability, and choice for online users. The Guidelines build on prior publications by the California Attorney General and consolidate and update existing recommendations. The Guidelines also specifically

add new recommendations concerning adoption of so-called "Do Not Track" or "DNT" mechanisms.

Regulatory—Financial Services

Financial Services Roundtable CEO Urges Cyber Threat Information Sharing Legislation
On July 16, the Financial Services Roundtable issued an open letter to Congress and President Barack Obama requesting legislation that encourages financial institutions to share information about data security threats in order to improve the detection of and response to cyberattacks.

Federal Financial Institutions Examination Council Launches Cybersecurity Web Page
On June 24, the Federal Financial Institutions Examination Council announced the launch of a webpage to serve as a central repository for cybersecurity materials.

American Bankers Association, Financial Services Roundtable, and Securities Industry and Financial Markets Association Support Draft Cybersecurity Bill
In a July 7 letter to U.S. Senators Dianne Feinstein (D–CA) and Saxby Chambliss (R–GA), the American Bankers Association, Financial Services Roundtable, and Security Industry and Financial Markets Association expressed support for the Cybersecurity Information Sharing Act of 2014.

Regulatory—Health Care

DHHS Office for Civil Rights Issues HITECH Reports to Congress
On June 10, the Department of Health and Human Services Office for Civil Rights published two annual reports that it sent to Congress summarizing 2011–2012 HIPAA breach notifications and compliance activities, as required by the HITECH Act.

Regulatory—Utilities

NIST Solicits Comments on Industrial Control Systems Security Guide
On May 14, NIST issued a revised Industrial Control Systems Security guide and requested comments by July 18. The guide addresses the vulnerability of industrial control systems used by public utilities, industrial plants, and other operations to cyberattacks and other threats.

DHS Security Unit Discloses Cyberattack on Public Utility
On May 16, the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT") unit of DHS released a ICS-CERT Monitor report stating that an unnamed U.S. public utility's control system network was recently compromised in a cyberattack by computer hackers, although there is no evidence that the utility's operations were affected. The report stated that the hackers may have gained access to the utility's control systems through an internet portal employing a simple password mechanism.

Regulatory—Consumer Privacy

FTC Files Complaint Against Amazon.com Inc. for In-App Charges
On July 10, the Federal Trade Commission ("FTC") filed a complaint alleging that Amazon.com Inc. violated section 5 of the Federal Trade Commission Act by billing "in-app charges" made in games children are likely to play without obtaining parental or other account holder's consent.

FTC Releases Data Broker Report
On May 27, the FTC completed its 18-month study on data brokers—companies that collect consumers' personal information and resell or share that information, but do not

directly interact with consumers. The Commission's report concluded that Congress should address the industry's "fundamental lack of transparency" through legislation that gives consumers greater visibility over data broker practices and greater control over data broker collection of their personal information. The report also provided best practices for the data broker industry. Chairwoman Edith Ramirez published a statement regarding the report, as did Commissioner Julie Brill.

Industry Groups Urge National Data Breach Notification Standard
The Direct Marketing Association, TechAmerica, the National Retail Federation, the Electronic Transactions Association, and a dozen other groups asked Congress on May 22 to replace the current patchwork of state breach reporting laws with a uniform federal standard. In a letter to Senate Majority Leader Harry Reid (D–NV) and House Speaker John Boehner (R–OH), the groups requested the passage of legislation without a broad reporting trigger, a strict notification timeline, or a private right of action provision.

FTC Releases Update on Data Privacy and Security Efforts
On June 27, the FTC released a report summarizing its current efforts to ensure consumer data privacy and data security.

Industry and Retail Groups Battle Over Who Should Bear More Liability for Data Breaches
In a June 11 letter, the National Association of Federal Credit Unions asked Congress to hold retailers to the same standards that financial institutions face under the Gramm-Leach-Bliley law. The Association stated that financial institutions continued to shoulder a disproportionate share of the costs stemming from fraudulent purchases and payment card replacements as a result of a data breach. The National Association of Convenience Stores ("NACS") countered in a June 16 letter that retailers already double pay for the costs of fraud and reissuing cards through swipe fees and reimbursement payments. The NACS also stated that financial institutions share some responsibility for the recent rise in data breach incidents.

Congressional Appropriations Committee Proposes Initiative to Fight Cybersecurity Threats to Retailers
The House Appropriations Committee issued a June 2014 report accompanying the Commerce, Justice, Science, and Related Agencies Appropriations Bill for the fiscal year ending September 30, 2015, which recommended that NIST build on its experience in creating the Framework for Improving Critical Infrastructure Cybersecurity to develop a retail-specific cybersecurity initiative.

Attorneys General for Florida, Connecticut, and New York Respond to eBay Data Breach
Cybercriminals logged into eBay's internal corporate account on May 21, gaining access to personal information pertaining to 145 million registered users. Attorneys general for Florida, Connecticut, and New York, among others, are investigating and advising victims on how best to secure their personal information.

Judicial Rulings and Enforcement

DOJ Indicts Chinese Hackers

On May 19, the Department of Justice announced the indictment of five Chinese military hackers for cyber espionage targeting six American companies in the nuclear power, metals, and solar products industries. The indictment is the first of its kind to bring charges for such activity against a state actor.

Parties Seek Review of Magistrate Judge Ruling that Government Can Access Documents Stored Overseas
On April 25, a Federal Magistrate Judge in the Southern District of New York ruled that the government can obtain email and other records from a search warrant issued under the Stored Communications Act that are stored exclusively outside of the United States but

under the "possession, custody and control" of a U.S. company. In what will be closely watched proceedings, the matter is set for oral argument before the district court on July 31.

Supreme Court Says Search Warrant Required to Search Cell Phone Incident to Arrest
In a June 25 decision, the Supreme Court held that law enforcement, under most circumstances, must obtain a warrant to search a suspect's cell phone incident to arrest.

Wyndham Worldwide and LabMD File Appeals in Separate Challenges to FTC Authority
On June 24, LabMD appealed to the Eleventh Circuit a district court's order granting the Federal Trade Commission's motion to dismiss a suit brought by LabMD that challenged the Commission's authority under the Federal Trade Commission Act to bring charges for failing to reasonably protect consumers' personal data. The district court determined that it lacked jurisdiction over the merits of LabMD's challenge to the FTC's authority because the FTC had not yet taken final agency action. In a separate but similar case, Wyndham Worldwide asked the Third Circuit to allow an interlocutory appeal, certified by the district court, challenging whether Section 5 of the FTC Act authorizes the Commission to bring an unfairness claim involving data security, and whether the Commission must formally promulgate regulations before bringing such a claim. [A copy of the filings can be provided upon request.]

Legislative—Federal

President Obama Approves Senate Bill on Contractor Security Mandates
On July 7, President Obama signed the Senate version of the Intelligence Authorization Act for Fiscal Year 2014. The bill requires intelligence community contractors with access to classified information to increase protections against unauthorized disclosure of such information, rapidly report data breaches to the government, and perform ongoing background checks of employees and officers.

Senator Releases Draft of Cybersecurity Data Sharing Act
On June 17, Senator Dianne Feinstein (D–CA) introduced a discussion draft version of the Cybersecurity Information Sharing Act of 2014. Senator Feinstein collaborated with Senator Saxby Chambliss (R–GA) on the bill. The Act would incentivize the sharing of cyber threat information between the private sector and government entities, provide liability protection for certain data sharing, and offer protections to avoid unnecessary privacy intrusions. Chambliss previously stated at a Bloomberg Government conference on June 3 that he believes the Senate will produce bipartisan cybersecurity legislation this year. The bill was approved by the Senate Intelligence Committee in amended form on July 8.

Senate Committee Approves Legislation to Improve U.S. Cybersecurity Defenses
On June 25, the Senate Homeland Security and Governmental Affairs Committee approved by voice vote a pair of bills sponsored by Tom Carper (D–DE) and Tom Coburn (R–OK). One bill would codify the Department of Homeland Security's National Cybersecurity and Communications Integration Center, which assists the private sector in combating cyber threats. The other bill would revise the Federal Information Security Management Act of 2002 and focus attention on data breaches.

Senator Proposes Bill to Combat Foreign Cyber Theft
Senator Carl Levin (D–MI) and several others introduced the Deter Cyber Theft Act of 2014 on May 22. The Act would give the President the ability to impose sanctions under the International Emergency Economic Powers Act on individuals and entities that benefit from the cyber theft of intellectual property. Specifically, the Act would allow the President to freeze the assets of foreign companies that have knowingly benefited from the theft. In addition, it would require the Office of the Director of National Intelligence to compile an annual report on countries and technologies involved in economic and industrial

espionage.

House Passes Bill Strengthening Legal Protections Against NSA Surveillance
The House of Representatives voted on June 19 to amend the Department of Defense appropriations bill for fiscal year 2015, to include language restricting National Security Agency ("NSA") surveillance of citizen communications and activities. The amendment, which received bipartisan support from a group lead by Representatives Zoe Lofgren (D–CA), Jim Sensenbrenner (R–WI), and Thomas Massie (R–KY), would bar governmental review of communications made by an American citizen without a search warrant, even if the communication involved a suspected terrorist outside of the country. In addition, the amendment would prohibit the Central Intelligence Agency and NSA from using funds to persuade technology companies to build "back doors" into IT products that would allow government surveillance.

House Introduces Bill to Protect Consumers from Unwanted Data Collection
The House of Representatives Financial Services Committee approved an amendment to the Consumer Financial Protection Act of 2010 that would create an opt-out list for consumers who do not want the Consumer Financial Protection Bureau ("CFPB") to collect personal information about them. The amendment would also require the CFPB to provide public notice of any consumer information data breach and to provide a free year of credit monitoring to affected consumers.

Joint House Subcommittee Hearing Considers Privacy Threat to Students
A Joint House Subcommittee hearing on June 25 considered testimony regarding data mining that may affect student privacy. Fordham University School of Law Professor Joel Reidenberg cited a study that he co-led, which found that 95 percent of school districts rely on cloud services for storing data, yet less than seven percent of the underlying contracts restrict the sale of the data to third-party marketers.

Congressional Representatives Ask FCC Not to Impose Rigid Cybersecurity Legislation
In a June 16 letter to FCC Chairman Tom Wheeler, House Intelligence Committee Chairman Mike Rogers (R–MI) and committee member Mike Pompeo (R–KS) expressed concerns with recent public statements by the FCC that indicate the commission may be preparing to implement a "new regulatory scheme" that would encourage telecommunications providers to take certain measures to secure their networks from increasing cyber threats. The representatives stated that the most effective way to protect networks from cyber threats is to allow the industry to take the lead in battling cyberattacks.

Proposed House Appropriations Bill Includes Assessment of Cybersecurity Framework
Representative Jim Langevin (D–RI) proposed an amendment to the Commerce-Justice-Science appropriations bill for fiscal year 2015 that would require the Commerce Department to determine the extent to which companies have adopted the voluntary Framework for Improving Critical Infrastructure Cybersecurity. The amendment was adopted by a voice vote on May 28.

Legislative—States

Florida Amended Data Breach Notification Law Takes Effect
Florida's recently amended data breach notification law took effect on July 1. The law expands the definition of "personal information" and requires, among other things, that affected individuals be notified within 30 days of a data breach.

Iowa Amended Data Breach Notification Law Takes Effect
Iowa's updated data breach law took effect on July 1. The law requires notification to the Director of the Consumer Protection Division of the Office of the Attorney General for breaches affecting more than 500 state residents. The amendment also clarifies that it

applies to "computerized" personal information maintained in any medium.

Kentucky Data Breach Notification Law Takes Effect
Kentucky's recently passed data breach notification law took effect on July 15. The law requires information holders to provide notice of unauthorized disclosures of personal information to affected persons "in the most expedient time possible" and to notify consumer reporting agencies if the breach requires notice to more than 1,000 affected persons.

California Proposes Another Amendment to Breach Notification Law
California again is considering an amendment to its breach notification statute, which passed the state Assembly on July 1. The amendment would require businesses to notify consumers at the same time they notify data owners and licensees of breaches to credit card or debit card numbers by unauthorized persons.

[Return to Top]

Canada

Canada's Strict Anti-Spam Law Takes Effect
On July 1, a majority of the provisions of Canada's anti-spam legislation took effect. The Canadian legislation prohibits sending commercial electronic messages to an electronic address unless the person to whom the message is sent has consented to receiving it and the message complies with prescribed form and content requirements. Subject to certain limited exceptions, the legislation applies to all businesses that send commercial electronic messages to or from computer systems located in Canada. As a result, companies and individuals located anywhere in the world can be exposed to liability under this legislation, and the potential penalties for noncompliance are significant. The Canadian Radio-Television and Telecommunications Commission has issued responses to frequently asked questions and a guidance document that encourages companies to avoid liability by initiating corporate compliance programs.

Canadian Supreme Court Requires Search Warrant for Internet Service Provider Information
On June 13, the Supreme Court of Canada issued a ruling holding that law enforcement must obtain a search warrant before requesting internet service providers to hand over information about users. The ruling affirmed the right to online privacy for Canadians.

Canadian Court Limits Damages for Privacy Violation
In a June 10 ruling, the Federal Court of Canada limited the damages provided to a telecommunications company's customer, who alleged the company had allowed an unknown third party to access and change the customer's account. Damages under the federal Canadian Personal Information Protection and Electronic Documents Act were limited to C$2,500 plus costs and interest because the customer had little evidence of actual damages, the telecommunications company did not benefit from the breach, and the information released was not particularly sensitive.

New Canadian Privacy Commissioner Confirmed
On May 28, Canada announced the nomination of the new Canadian Privacy Commissioner. The appointment was confirmed by the Senate on June 4 and the House of Commons on June 5.

[Return to Top]

Latin America

Argentina's Chamber of Deputies Passes Do Not Call Bill
On July 3, Argentina's Chamber of Deputies unanimously passed a bill (source document

in Spanish) that would create a do not call registry to protect consumers from unwanted calls from telemarketers.

Consumer Protection and Defense Department Fines Oi for Privacy Violations
On July 24, the Brazilian government announced that the Consumer Protection and Defense Department fined a Brazilian telecom company Oi 3.5 million reais ($1.59 million) for violating users' privacy. The government investigated an agreement between Oi and a British company and determined that Oi unlawfully sold consumers' browsing data without consent.

Mexican Data Protection Agency Studies New Mexican Telecommunications Bill
On July 10, the Federal Institute for Access to Public Information ("IFAI") stated that it is analyzing secondary regulations (source document in Spanish) under the recently enacted Telecommunications and Broadcasting Bill in view of existing data privacy laws. It is focused in particular on the issue of right holders of personal data being subject to real-time geographic localization under Mexican Constitutional and legal provisions. The IFAI informed that it will issue an institutional communication about its findings.

The following Jones Day attorneys contributed to the United States, Canada, and Latin America sections: Chris Cogburn, Andrea Dinamarco, Bart Green, Jay Johnson, Michael Klotz, Guillermo Larrea, Colin Leary, Gabe Ledeen, Nicole Perry, Scott Poteet, Katherine Ritchey, Mina Saifi, and Zach Werner.

[Return to Top]

Europe, Middle East, and Africa

European Union

European Court of Justice to Decide About Binding Character of Safe Harbor Status
In a recent court ruling, an Irish court referred to the European Court of Justice ("ECJ") the question of whether the Commission's July 2000 decision on the U.S. safe harbor status is binding or whether the member states can conduct their own investigation in light of the factual developments since such decision. In essence, the issue concerns whether a company participating in PRISM (a U.S. government surveillance program) can still make use of its safe harbor status. Should the European Court of Justice hold that member states can conduct independent investigations, it would affect reliance by companies on a safe harbor status when transferring personal data to the United States.

European Court of Justice Clarifies Responsibilities of Internet Search Engines Regarding So-Called "Right to be Forgotten"
In a May 13 ruling, the ECJ recognized the application of the EU Data Protection Law to the activities carried out by search engines and clarified the responsibilities of these types of companies regarding the "right to be forgotten." On June 6, the Article 29 Working Party announced that it is analyzing the consequences of the ruling of the ECJ and might publish guidelines for consultation. (In reaction to the decision of the ECJ, Google has launched a web form to allow data subjects to request personal data to be removed from online search results. Information will disappear from searches made in Europe only.)

Negotiations of EU–U.S. Data Protection Umbrella Agreement
According to a statement of the European Commission in June, negotiations between the European Union and the United States on the conclusion of a Data Protection Umbrella Agreement to protect personal data transferred between the European Union and the United States for law enforcement purposes are reaching the final stage. The remaining stumbling block relates to the right of effective judicial redress for EU citizens not resident in the United States and the purpose limitation of the data sent to the United States. The former may be resolved soon, as the United States has announced legislative action on effective redress.

European Commission Finalizes Internal Security Strategy Report
On June 20, the European Commission finished its final implementation report on the Commission's Internal Security Strategy 2010–2014 regarding progress on increasing the levels of security in cyberspace.

Cloud Computing Interest Groups Communicate to European Commission Guidelines on Standardization of Service Level Agreements for Cloud Services
On June 26, the European Commission received Guidelines on standards for security and data protection for cloud computing services, prepared by a selected group of cloud computing providers and customers.

EDPS Provides Opinion on Internet Governance
On June 23, the European Data Protection Supervisor ("EDPS") adopted an opinion on a Commission Communication on internet policy and governance. The opinion provides the EDPS's views on the current debate around internet governance structures and processes, and it suggests actions that EU institutions can perform to influence such debate.

ENISA and Europol Sign Strategic Cooperation Agreement
On June 26, the European Union Agency for Network and Information Security ("ENISA") and Europol signed a strategic cooperation agreement to enhance cooperation between Europol, its European Cybercrime Centre, and ENISA in order to support the EU member states and the EU institutions in preventing and combating cybercrime.

Belgium

Privacy Commission Introduces Online Notification Forms to Report Personal Data Breaches
The Belgian Privacy Commission introduced online notification forms for reporting data breaches, including a specific form (source document in French) for breaches in the telecommunication sector (notification within 24 hours) and a general form (source document in Dutch) for breaches in other sectors (notification within 48 hours but no legal obligation at this stage). This follows a recommendation (source document in Dutch) of the Privacy Commission in 2013 providing several safety measures in order to prevent such breaches.

DPAs Close SWIFT Enquiry
The Belgian Privacy Commission and the Dutch Data Protection Authority concluded on May 8 that the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") did not violate any legal security requirements of computer networks. The investigation started at the end of 2013 and focused on the security of financial data messages in response to media allegations about U.S. security intrusion.

DPAs and Others Conduct First Coordinated Inquiry into Mobile Applications
The Global Privacy Enforcement Network ("GPEN"), which regroups several data protection authorities ("DPAs") including the Belgian Privacy Commission, published the findings of its first internet privacy sweep, held between May 6 and May 12. The findings focus on transparency (adequate privacy policy) for mobile applications. GPEN has already announced the future publication of additional findings focusing on information provided to mobile applications users and consent, forthcoming this fall.

France

France Enforces Cookies Regulations
CNIL issued on December 16, 2013, its recommendations (source document in French) for the implementation of cookies in compliance with the data protection regulations applicable in France. In a communication (source document in French) dated July 11, 2014, CNIL indicated that, as of October 2014, it will be monitoring and enforcing compliance with these regulations. CNIL will specifically be analyzing compliance on key

issues including (i) the types of cookies that are implemented, (ii) the purposes of such data processing, (iii) how consent from the data subject is obtained when required, and (iv) whether the data subjects are duly informed about the implementation of cookies. Businesses with websites that target French users should promptly ensure compliance of their cookie implementation policy with French data protection regulations.

DPA Authorizes Screening Processes More Widely
In a May 6 decision (source document in French), the *Commission Nationale de l'Informatique et des Libertés* ("CNIL") authorized the French subsidiary of an international group outside of the banking and financial sectors to implement personal data processing of its commercial partners for screening purposes, in order to prevent risks of corruption and money laundering. This decision shows that, subject to compliance with strict conditions, the CNIL is willing to authorize such screening processes implemented for compliance with foreign law requirements (such as the Foreign Corrupt Practices Act in the United States or the UK Bribery Act) even though the data controller is not subject to a French law screening obligation.

DPA Warns Freight Company Following Leak
CNIL warned (source document in French) an international logistics, freight, and express mail company that it had violated a 1978 information privacy law when it was discovered that personal data for nearly 700,000 clients of the company was freely accessible on the internet. CNIL's warning cited the company's failure to institute time-limiting measures on document retention and failure to independently verify the security of an information system designed by a third party.

Germany

Federal Supreme Court Decides that User Registration Data of Internet Portals Can Remain Anonymous
In a July 1 decision (source document in German), the German Federal Supreme Court (*Bundesgerichtshof*) held that the provider of an internet portal is not obliged to provide information about user registration data to an individual whose personal rights have been violated by evaluations published in the internet portal, because there is no legal basis for such claim.

Orientation Guideline for App Developer and App Provider
The *Düsseldorfer Kreis* ("Düsseldorf Circle"), an informal body of all German DPAs responsible for the private sector, published on June 16 an orientation guideline (source document in German) regarding the data protection requirements relevant to app developers and app providers.

GDD Issues Questionnaire for Verifying Compliance with the Safe Harbor Certification
The German Association for Data Protection and Data Security ("GDD") issued a questionnaire in May that will enable German data exporters to document that they have carried out a verification of compliance of the data importer with the relevant obligations under the Safe Harbor framework.

Proceedings Against Germany for Failing to Adopt EU Data Retention Directive Withdrawn
The European Commission has withdrawn the proceedings before the European Court of Justice against Germany for failing to adopt the EU Data Retention Directive ("Directive"). The Directive had been invalidated by the same court in a decision in April. The European Commission has applied for an order that Germany will bear the costs of the proceedings.

Italy

DPA Issues Mobile Remote Payment Guidelines
On June 17, the DPA issued a decision (source document in Italian) in the Official Gazette setting out guidelines with respect to mobile payments. According to the DPA, express consent will be necessary not only to transmit the data to third parties but also if the

information is processed by the same subject who acquires the data for purposes different from those strictly related to the payment, such as marketing. Data can be stored for no more than six months, and the IP address of the client must be automatically deleted after the completion of the transaction. Specific measures are required to be implemented in order to protect the confidentiality of the relevant data, including tracking access by employees of the operator and encryption. A detailed list of instructions also provides guidelines for phone operators, which have access to a wide range of information, to prevent cross-profiling of user preferences.

DPA Issues Privacy Tips
The widespread use of mobile internet devices such as smart phones and tablets linked to social networking potentially increases the risks that user privacy can be violated, especially when users are not conscious of the possible dangers. On July 5, the DPA issued general guidelines (source document in Italian) containing useful privacy tips to prevent "undesired" and "unpleasant" consequences.

The Netherlands

Public Broadcaster and Advertising Brokerage Use Tracking Cookies Without Consent
The DPA has reviewed how the Dutch Public Broadcasting Service ("NPB") and an online advertising brokerage company have been collecting personal data using tracking cookies. The DPA concluded that both the NPB (source document in Dutch) and the advertising brokerage (source document in Dutch) infringed the Dutch Data Protection Act, as neither asked its website visitors for unequivocal consent. The DPA has yet to decide on sanctions, if any.

DPA Says Municipalities May Not Ignore Privacy Regulations
The DPA issued a warning (source document in Dutch) to the government that municipalities should not neglect the data protection and privacy aspects of the upcoming transfer of responsibilities for certain social programs from the central government to the municipalities. The DPA is specifically concerned about the lack of a clear privacy framework and the fact that under the transfer of responsibilities, municipalities will obtain significantly more, and potentially sensitive, personal data. The DPA will continue to monitor developments and where necessary use its authority to enforce the Dutch Data Protection Act.

DPA Issues Second Opinion on the Benefits of eID
The DPA has issued a second opinion (source document in Dutch) on a report on the public benefits of a new electronic ID system ("eID"). This system is being developed by the Dutch government together with the private sector as an online identification and authentication system that may be used for the exchange of personal data in the context of the online provision of services. The DPA questions whether the eID system will in practice increase security overall compared to the current DigiD-system and is concerned that due to a higher level of security, more confidential information will be shared, which in turn introduces new security issues.

Russia

State Duma Adopts Amendment of Information Law and Personal Data Law
In early July, the lower chamber of the Russian Parliament adopted a set of amendments (source document in Russian) to the Federal Law "On Information, Information Technologies and Protection of Information" ("Information Law") and to the Federal Law "On Personal Data" ("Personal Data Law"). The draft legislation requires further approvals as well as a signature by the Russian President. The legislative changes could be in effect in September 2016. The amendments to the Information Law provide that "databases which are used for gathering, recording, systemizing, accumulation, storage, updating and uploading of personal data of the Russian citizens" must be located in Russia. Furthermore, the Personal Data Law is amended to provide that "an operator gathering personal data, including by Internet, must ensure recording, systemizing, accumulation, storage, updating and uploading of personal data of the Russian citizens with the

databases located on the territory of the Russian Federation." No specific liability is introduced for failure to comply with such requirements, hence the moderate administrative fines that already exist in Russian law may be applied by the Russian regulator against noncompliant data operators. The Amendments were signed into law by President Putin on July 22, 2014. A more detailed summary of the Amendments is available in a Jones Day *Alert*, "Russia Adopts Restrictive Changes to its Data Privacy Law," July 2014.

Spain

Spain Launches New Telecommunications Act
The Official Journal of Spain ("BOE") published the General Telecommunications Act 9/2014 (source document in Spanish) on May 10. The Act establishes, among other aspects, new requirements for the processing and sending of commercial communications. Regarding cookies, the Act also includes new requirements for obtaining the consent of the data subject in order to process personal data by means of storage and data recovery devices in terminal equipment. Finally, the Act expressly establishes the power of the Spanish DPA to examine the security measures adopted by the telecommunications operators and to issue recommendations (best practices) that it deems appropriate. Furthermore, the Spanish DPA may adopt instructions and guidelines regarding the circumstances in which the operators are requested to notify personal data breaches.

Spain Establishes National Commission for Critical Infrastructure Protection
The National Commission for Critical Infrastructure Protection (source document in Spanish), established on July 1 and chaired by the Secretary of State for Security, is the competent body to approve Sectoral Strategic Plans and to designate critical operators.

United Kingdom

English High Court Awards Compensation for Emotional Distress for Data Protection Breaches
A recent English High Court decision suggests that compensation for emotional distress may be awarded in cases where a complainant can also demonstrate financial loss, even if nominal. In *AB v Ministry of Justice*, the claimant established that breach of his data subject access rights caused a nominal financial loss of £1, which was sufficient to trigger the jurisdiction to award compensation for distress. Damages of £2,250 were awarded. The ruling appears to extend significantly the potential availability of compensation for nonfinancial loss.

Government Publishes Draft Bill to Toughen Computer Crime Offenses
On June 4, the government published the Serious Crime Bill, proposing amendments to the Computer Misuse Act 1990. The proposed legislation creates a new aggravated hacking offense if a person intentionally causes "damage of a material kind," carrying a maximum sentence of life imprisonment. The bill also extends the territorial scope of the 1990 Act to cover acts committed outside of the UK, as long as the accused was a UK national at the relevant time.

National Health Service Audit Uncovers Major Data Privacy Lapses
An audit commissioned by the government has found "significant lapses" in National Health Service ("NHS") data-sharing practices. The audit found that between 2005 and 2012, 588 data releases were made to private-sector organizations for the purpose of "analytics, benchmarking and research," in many cases with inadequate or no data-sharing agreements in place. The findings were compounded by a leaked report from the Information Commissioners Office suggesting that as many as 10,000 NHS patients may have been affected by a separate series of data protection breaches by a private contractor.

The following Jones Day attorneys contributed to this section: Paloma Bru, Undine von Diemar, Olivier Haas, Timur Khoussainov, Bastiaan Kout, Ted Kroke, Afra Mantoni, Laurent De Muyter, Silvia Montealegre Santana, Rhys Thomas, and Sergei Volfson.

[Return to Top]

Asia

Japan

Japan Releases Policy Outline for Amendment of Personal Information Protection Act
On June 24, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunication Network Society within the Cabinet Office released the "Policy Outline for Institutional Amendment Regarding Protection and Utilization of Personal Data." The Policy Outline sets out the basic framework for the amendment of the Personal Information Protection Act, including establishment of a privacy commissioner to strengthen enforcement of the Act. The Policy Outline is open for public comments until July 24. Following review of the public comments, the bill for amendment will be submitted in the January session of the Diet in 2015.

Hong Kong

Hong Kong Privacy Commissioner Condemns Blind Recruitment Advertisements
On May 29, the Hong Kong Privacy Commissioner condemned 48 blind recruitment advertisements (i.e., recruitment advertisements that do not identify either the employer or the employment agency acting on its behalf) for directly soliciting personal data from job applicants, which constitutes unfair collection of job applicants' personal data. Enforcement notices were issued by the Commissioner to the advertisers, directing them to delete the personal data collected unless such data had to be retained under other legal requirements or for a continuing recruitment process in which the job applicant was informed and given the option to demand deletion of personal data.

China

China Tightens Access to Personal Information
Two individuals will be prosecuted shortly in Shanghai for conducting illegal investigations and purchase of personal information in China. The individuals were formally arrested by the Shanghai Public Security Bureau in August 2013. In accordance with Article 253 of the PRC Criminal Law, if the individuals are found guilty by the court of "illegally obtaining citizens' personal information," they are likely to face a sentence of up to three years in prison and criminal fines.

Taiwan

Amendments to Communication Security and Surveillance Act Take Effect
The new amendments to the Communication Security and Surveillance Act took effect on June 29. Changes include: (i) prosecutors who are applying for an interception warrant must now provide sufficient evidence showing that the underlying offenses are punishable with a minimum of a three-year fixed-term imprisonment; and (ii) any information that is obtained for a particular purpose cannot be used for other investigative purposes.

Amendment to Financial Holding Company Act Takes Effect
The new amendment to the Financial Holding Company Act took effect on June 4. The Act now requires all information to be subject to the Personal Information Protection Act except for names and addresses of the clients.

Taiwan Proposes Amendment to Personal Information Protection Act
While both criminal data and medical records are considered "sensitive data" under the Personal Information Protection Act, a newly proposed amendment puts medical records into yet another category in which "public interest" is no longer a justifiable reason for

collecting them. The amendment passed review at the Legislative Yuan's committee and now awaits discussions between the political parties and additional procedures at the Legislative Yuan. For more detail, see the meeting minutes from the Judiciary and Organic Laws and Statues Committee of the Legislative Yuan dated May 8, 2014 (source document in Chinese) and the meeting minutes dated May 14, 2014 confirming the proposals by the Judiciary and Organic Laws and Statues Committee of the Legislative Yuan (source document in Chinese).

Singapore

Personal Data Protection Commission Takes Action Against Organizations for Breaching Personal Data Protection Act 2012
Since the Do Not Call ("DNC") requirements under the Personal Data Protection Act took effect on January 2, the Personal Data Protection Commission has conducted investigations against 630 organizations, mainly from sectors such as property, tuition, and insurance, in response to 3,700 valid complaints received. On June 4, the Commission charged a tuition agency and its director for offenses relating to the DNC provisions. If found guilty, the organization and individuals may be subject to a fine of up to S$10,000 per contravening telemarketing message sent to a Singapore telephone number. In addition, two organizations have accepted offers to compound their offenses in lieu of prosecution for composition amounts ranging between S$500 and S$1,000. Approximately 380 other organizations have received warning notices from the Commission.

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 Cross-Border Public Interest Determinations
The Australian Information Commissioner has made two temporary "public interest determinations" to permit the cross-border disclosure of personal information of beneficiaries of international money transfers by authorized-deposit taking institutions to overseas financial institutions for a period of 12 months from March 2014. The Reserve Bank of Australia ("RBA") and the Australia and New Zealand Banking Group Ltd ("ANZ") made public interest applications to the Office of the Australian Information Commissioner to seek declarations that they were able to continue their existing practice of information disclosure when processing international money transfers without breaching the Australian Privacy Act 1988 (Cth). In making public interest determinations, the Information Commissioner must be satisfied that the public interest in doing the act that potentially breaches Australian privacy laws substantially outweighs the public interest in adhering to the relevant privacy law. The Information Commissioner is currently seeking submissions, closing on August 4, from interested parties on whether longer-term public interest determinations should be made.

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

Jeffrey L. Kapp
Cleveland

Anita Leung
Hong Kong

Jason McDonell
San Francisco

Caroline N. Mitchell
San Francisco

Katherine S. Ritchey
San Francisco

Michiru Takahashi
Tokyo

Undine von Diemar
Munich

Amanda B. Childs
Dallas

Christopher J. Lopata
New York

Michael G. Morgan
Los Angeles

Po-Chien Chen
Taipei

Laurent De Muyter
Brussels

Bart Green
New York

Elaine Ho
Singapore

Bastiaan K. Kout
Amsterdam

Federica Morella
Milan

Brandy Hutton Ranjan
Columbus

Nicola Walker
Sydney

Brian T. Holman
Irvine/Los Angeles

J. Todd Kennard
Columbus

Jonathon Little
London

Carmen G. McLean
Washington

Matthew D. Orwig
Dallas/Houston

Elizabeth A. Robertson
London

Rhys Thomas
London

Toru Yamada
Tokyo

Michele L. Gibbons
Houston/New York

Margaret I. Lyle
Dallas

Sergei Volfson
Moscow

Nigel Chin
Singapore

Andrea Dinamarco
São Paulo

Joshua Grossman
New York

Nancy L. Hoffman
New York

Colin Leary
San Francisco

Susan M. O'Connor
New York

Mina R. Saifi
Dallas

Zachary M. Werner
New York

Robert W. Kantner
Dallas

Beong-Soo Kim
Los Angeles

Kevin D. Lyles
Columbus

Daniel J. McLoon
Los Angeles

Mauricio Paez
New York

Adam Salter
Sydney

Michael W. Vella
Shanghai

Sidney R. Brown
Atlanta

Jay Johnson
Dallas

Stefano Macchi di Cellere
Milan/London

Olivier Haas
Paris

Christopher S. Cogburn
Atlanta

Adrian Garcia
Dallas

Javier Gutiérrez Ponce
Madrid

Alice Hu
Hong Kong

Gabriel Ledeen
San Francisco

Nicole M. Perry
Houston

Raquel Travesí
Madrid

Natalie A. Williams
Atlanta

Elena Kaplan
Atlanta

Ted-Philip Kroke
Frankfurt

John M. Majoras
Columbus/Washington

Janine Cone Metcalf
Atlanta

Chaka M. Patterson
Chicago

Gregory P. Silberman
Silicon Valley

Amy E. Vieta
New York

Paloma Bru
Madrid

Guillermo E. Larrea
Mexico City

Georg Mikes
Frankfurt

David L. Odom
Dallas

Dash A. Cooper
Dallas

Steven G. Gersten
Dallas

Aaron M. Healey
Columbus

Nandini Iyer
Silicon Valley

Afra Mantoni
Milan

Scott B. Poteet
Dallas

Anand Varadarajan
Dallas

Marc L. Swartzbaugh
Cleveland

Follow us on:

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