JONES DAY | **Privacy & Cybersecurity Update**
Issue 1 | May 2014

JONES DAY

Introducing Jones Day's Global Privacy and Cybersecurity Update

Jones Day lawyers have been at the forefront of data protection and cybersecurity law developments in the United States, Europe, Latin America, and Asia. As the internet gained prominence in the mid-1990s, we formed a team of lawyers to assist clients with their data protection and cybersecurity issues. Today, we are an interdisciplinary team of attorneys located in our offices around the world, helping our national and multinational clients confront new and novel issues in privacy and cybersecurity. We have decided to put this experience to use to keep our clients, colleagues, and friends abreast of changes in this rapidly developing area of law. We hope you enjoy this, our first of many legal updates on global privacy and cybersecurity law developments.

— *Mauricio Paez and Kevin Lyles*

United States

Legislative—Federal

U.S. House of Representatives Approves Cybersecurity Legislation
The U.S. House of Representatives approved the Cyber Intelligence Sharing and Protection Act ("CISPA") on April 18, 2014. CISPA would protect private-sector companies from liability stemming from the sharing of cyber threat information with the intelligence community. CISPA also would direct the Director of National Intelligence to establish

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

procedures to permit the intelligence community to share cyber threat information with private-sector companies. Previous versions of CISPA were passed by the House in 2012 and 2013 but not approved by the Senate.

Significant Changes to Australian Privacy Act 1988 (Cth) Take Effect

U.S. Senate Considers Cybersecurity Legislation
Senators Dianne Feinstein (D-CA) and Saxby Chambliss (R-GA) of the U.S. Senate Intelligence Committee recently introduced a draft bill that would allow companies to monitor their networks for cybersecurity threats, promote sharing of cybersecurity threat information, and provide liability protection for companies who share threat information.

Legislatures Mull Privacy Implications of Automotive Data Collection
In April, the U.S. Senate Committee on Commerce, Science and Transportation voted to submit the Driver Privacy Act for consideration by the full Senate, while in the California State Assembly, the Consumer Car Information and Choice Act failed to pass through the Senate Transportation and Housing Committee. Legislative efforts relating to privacy issues posed by the collection of event data by GPS navigation systems and other on-board services now widely available for use in automobiles follow the December 2013 report by the Government Accountability Office concerning privacy issues with on-board services in automobiles.

U.S. Lawmakers Introduce Grid Reliability and Infrastructure Act
Representative Henry A. Waxman (D-CA) and Senator Edward J. Markey (D-MA) introduced the Grid Reliability and Infrastructure Defense Act, or GRID Act, in the U.S. House of Representatives and the U.S. Senate on March 26, 2014. If approved, the Act will give the Federal Energy Regulatory Commission the authority to issue emergency orders or regulatory rules to address cybersecurity and other threats and vulnerabilities to the U.S. electrical grid.

Legislative—States

Florida Passes Data Breach Notification Law
Florida recently passed the Information Protection Act of 2014 that repeals previous data breach legislation and requires businesses and government agencies to notify consumers and the Attorney General's office of a data breach within 30 days.

Kentucky Passes Data Breach Notification Law
Kentucky recently passed a data breach notification law that requires "Information Holders" to provide notice of unauthorized disclosures of personal information to affected persons "in the most expedient time possible." Information Holders also must notify consumer reporting agencies if the breach requires notice to more than 1,000 affected persons.

Iowa Amends Data Breach Notification Law to Require Attorney General Notification
Iowa updated its data breach law to require 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.

Regulatory—Policy and Best Practices

U.S. Department of Homeland Security Notifies Owners and Operators of Critical Infrastructure
Pursuant to Section 9 of Executive Order 13636, the Secretary of the U.S. Department of Homeland Security has completed the process of identifying critical infrastructure where a

cybersecurity incident could reasonably result in catastrophic effects on public health or safety, economic security, or national security, according to a April 17, 2014 *Federal Register* notice. The Secretary has also confidentially notified the owners and operators of the cyber-dependent infrastructure and created a method through which the entities can request reconsideration of that classification.

White House Releases Report on Big Data
On May 1, 2014, the White House released a comprehensive report, "Big Data: Seizing Opportunities, Preserving Values," that outlined key observations and recommendations on the future of privacy and big data for the private and public sectors. The report makes six policy recommendations in all, including passing a national data breach law that would require companies to report major losses of personal and credit card data, advocating for legislation that would define consumer rights regarding how data about their activities was used, extending privacy protections to individuals who are not citizens of the United States, and ensuring that data collected about students is used only for educational purposes.

U.S. Department of Justice and Federal Trade Commission Release Antitrust Policy Statement on Sharing of Cybersecurity Information
On April 10, 2014, the Antitrust Department of the U.S. Department of Justice and the Federal Trade Commission issued a joint Antitrust Policy Statement on Sharing of Cybersecurity Information that described the analysis from an antitrust perspective of cybersecurity threat information-sharing.

U.S. Department of Justice Says Sharing of Cybersecurity Information Not a Violation of Stored Communications Act
The U.S. Department of Justice encouraged companies to share cybersecurity threat information in a white paper issued on May 9, 2014. The white paper assured entities that the disclosure of generalized, non-content threat data to the government would not violate the Stored Communications Act.

U.S. Department of Justice Charges Five Members of Chinese Military with Cyber Espionage
On May 19, 2014, the U.S. Department of Justice announced that a grand jury in the Western District of Pennsylvania indicted five members of the Chinese military for computer hacking, economic espionage, and other offenses. The indictment presents the first such charges ever brought in the U.S. against a state actor.

Congressional Research Service Says Cybersecurity Framework Raises Liability Issues
The Congressional Research Service issued a legal sidebar to lawmakers on March 5, 2014, that questioned whether the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity will be used as a legal benchmark for assessing cybersecurity programs and determining liability in data breach litigation. The Congressional Research Service's legal sidebar is available from Jones Day upon request.

National Institute of Standards and Technology Holds Privacy Workshop on Framework for Improving Critical Infrastructure Cybersecurity
Following the release of the National Institute of Standards and Technology's ("NIST") Framework for Improving Critical Infrastructure Cybersecurity, NIST held a privacy engineering workshop on April 9–10, 2014, with U.S. officials and privacy policy experts to determine whether to add privacy controls to the Framework.

General Services Administration Considers New Cybersecurity Requirements for Government IT Contracts
IT products and services are procured by the federal government through government-wide acquisition contracts ("GWACs") that allow federal agencies to purchase IT products and services from preapproved commercial IT vendors for a set period of time at pre-

negotiated prices. With a GWAC in place, an agency need not establish open competition among IT vendors and instead may simply place a task order pursuant to the GWAC for the particular IT product or service to be procured. Aiming to make cybersecurity requirements applicable to federal IT contractors at the contract level rather than at the task order level, the General Services Administration invited public comment on a cybersecurity proposal that mandates that IT contractors have in place a Contract Cybersecurity Risk Management Plan as part of the GSA's next-generation GWAC acquisition process.

Regulatory—Financial Services

U.S. Securities and Exchange Commission Holds Cybersecurity Roundtable
The Securities and Exchange Commission ("SEC") held a cybersecurity roundtable on March 26, 2014, to address the cybersecurity landscape and related issues faced by exchanges and other key market systems, broker-dealers, investment advisers, transfer agents, and public companies. As part of the roundtable discussion, SEC Commissioner Luis Aguilar advocated that the SEC should immediately form a Cybersecurity Task Force that will regularly meet and advise the SEC when appropriate.

U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations Issues Cybersecurity Preparedness Alert
On April 15, 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") announced that it will examine 50 registered broker-dealers and investment advisers to determine their level of preparation for detecting and preventing cybersecurity attacks. The announcement includes an appendix with a list of sample requests that OCIE may make in conducting the examinations.

U.S. Federal Financial Institutions Examination Council Advises Financial Institutions on Heartbleed Vulnerability
The U.S. Federal Financial Institutions Examination Council issued a press release and an accompanying alert on April 10, 2014, that outlined steps that financial institutions should take to address vulnerabilities related to the heartbleed bug.

Federal Deposit Insurance Corporation Encourages Financial Institutions to Utilize Available Cybersecurity Resources
An April 10, 2014, press release from the Federal Deposit Insurance Corporation identifies five government and government-sponsored resources that financial services organizations should utilize to increase awareness of potential cybersecurity threats.

Financial Services Roundtable CEO Testifies Before U.S. Senate Homeland Security and Government Affairs Committee
The CEO of Financial Services Roundtable testified before the U.S. Senate Committee on Homeland Security and Government Affairs on April 2, 2014, about the recent establishment of a Merchant and Financial Services Cybersecurity Partnership, whose mission is to enhance payment system security.

New York Department of Financial Services Mandates Regular Cybersecurity Assessments
Following a survey and report finding that hackers have targeted several New York banks in the last three years, the New York Department of Financial Services mandates regular assessments for local banks to demonstrate cybersecurity preparedness.

Consumer Financial Protection Bureau Proposes Change to Bank Privacy Policy Notification Rule
On May 6, 2014, the Consumer Financial Protection Bureau announced a proposed amendment to Regulation P, implementing the Gramm-Leach-Bliley Act, that would allow banks to post annual privacy policy notices online, under certain conditions, instead of mailing them. The comment period closes June 12, 2014.

Regulatory—Health Care

U.S. Department of Health and Human Services Releases Security Risk Assessment Tool
On March 28, 2014, the U.S. Department of Health and Human Services released a new security risk assessment tool to help health care providers in small- to medium-sized offices assess their information security risks under the Health Insurance Portability and Accountability Act's Security Rule.

Regulatory—Utilities

U.S. Department of Energy Issues Research Call Related to Cybersecurity for Energy Delivery Systems Program
The U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability ("OE") created the Cybersecurity for Energy Delivery Systems Program to assist electric, oil, and gas asset owners by creating cybersecurity solutions for energy delivery systems through an integrated research and development effort. On April 15, 2014, the National Energy Technology Laboratory, on behalf of the OE, began seeking applications from federally funded research and development centers to conduct research and demonstrations related to future technologies that may accelerate the deployment of cybersecurity capabilities for the U.S. energy infrastructure. Responses are due May 23, 2014.

U.S. Department of Energy Issues Cybersecurity Guidance to Energy Sector and Technology Suppliers to Bolster Safety of U.S. Power Grid
On April 28, 2014, the U.S. Department of Energy issued guidance titled Cybersecurity Procurement Language for Energy Delivery Systems, which identifies proposed contract language for use by energy companies and their technology suppliers to ensure all parties are considering cybersecurity in procurement decisions.

National Institute of Standards and Technology Requests Public Comments on Smart Grid Interoperability Standards
On April 15, 2014, the National Institute of Standards and Technology ("NIST") issued a *Federal Register* notice seeking comments on the draft NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. The Framework and Roadmap incorporates updates to NIST's efforts to facilitate and coordinate smart grid interoperability standards, including the use of wireless communication power meters, the availability of customer energy usage data through the Green Button initiative, and protocols for electric vehicle charging. Comments on the draft are due May 30, 2014.

Regulatory—Consumer Privacy

U.S. Federal Trade Commission Signs Memorandum of Understanding with United Kingdom's Information Commissioner's Office
On March 6, 2014, the U.S. Federal Trade Commission signed a Memorandum of Understanding with the United Kingdom's Information Commissioner's Office to promote cooperation in the enforcement of laws protecting consumer privacy.

U.S. Federal Trade Commission Chair Testifies Before Senate Committee
On April 2, 2014, the Chair of the U.S. Federal Trade Commission testified before the Senate Committee on Homeland Security and Governmental Affairs on the increasing threat of data breaches and urged Congress to strengthen the Commission's existing authority over data security matters and to require companies to notify consumers of data breach incidents.

Federal Court Upholds U.S. Federal Trade Commission's Authority Over Unfair Data Security Practices Under FTC Act
On April 7, 2014, the U.S. District Court for the District of New Jersey issued a highly

anticipated decision that affirmed the U.S. Federal Trade Commission's authority under Section 5 of the Federal Trade Commission Act to pursue claims against companies for unreasonably lax data security practices as an unfair trade practice.

Retail Industry Leaders Association Testifies on Cybersecurity and Protecting Consumer Data
On April 2, 2014, the President of the Retail Industry Leaders Association testified before the Senate Committee on Homeland Security and Governmental Affairs on the cybersecurity threats retailers encounter and the steps retailers are taking to mitigate threats and protect consumers.

Retail Industry Leaders Association Launches Retail Information Sharing and Analysis Center
The Retail Industry Leaders Association launched the Retail Information Sharing and Analysis Center on May 14, 2014. The Center is focused on identifying real-time cyber threats, sharing intelligence data to reduce the risk of cyber attacks on retailers, and providing training, education and research resources to retailers.

National Retail Federation Announces Establishment of Retail and Merchant Industry Information Sharing and Analysis Center for Cybersecurity
On April 14, 2014, the National Retail Federation announced that it is moving forward with plans to create a Retail and Merchant Industry Information Sharing and Analysis Center to provide retailers access to information on cybersecurity threats identified by retailers, the government, and law enforcement personnel. The Center is expected to be established in June 2014.

Data Breach Investigation Report Finds that Cyber Criminals are Outpacing Retailer's Security Measures
The 2014 Data Breach Investigation Report issued by Verizon Enterprise Solutions on April 23, 2014, identifies nine cyber attack patterns grouped by industry.

U.S. Federal Trade Commission Updates Guidance on Children's Online Privacy Protection Act
In April 2014, the U.S. Federal Trade Commission updated its guidance on the Children's Online Privacy Protection Act to clarify, among other issues, who should provide consent to the collection of student data, what standards should be used for authenticating the identity and authority of a consent-giver, and whether there are any approved commercial uses for students' data.

[Return to Top]

Canada

Canadian Government Releases Action Plan for Critical Infrastructure
On March 7, 2014, the Canadian government released the Action Plan for Critical Infrastructure (2014–2017). The Action Plan describes the increasing relevance of cybersecurity to critical infrastructure and identifies the ultimate goal of securing Canada's cyberspace for the benefit of Canadians and the economy.

[Return to Top]

Latin America

Brazil Approves Internet Constitution
On April 23, 2014, Brazil's President approved Brazil's Internet Constitution (*Marco Civil da Internet*) (source document in Portuguese), which regulates web neutrality, privacy, data storage, web surveillance, targeted marketing, public access, and other issues, and

provides for a bill of rights for internet users.

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

[Return to Top]

Europe, Middle East, and Africa

EU Court of Justice Declares Data Retention Directive Null and Void
The Court of Justice of the European Union has declared the Data Retention Directive 2006/24/EC to be invalid on April 8, 2014. The EU Member States are no longer required to transpose the Directive into their national laws. The Member States nevertheless may introduce laws on data retention on a national level, provided those are in line with the relevant constitutional requirements. Laws on data retention already existing in the member states remain valid.

European Parliament Adopts Draft General Data Protection Regulation
On March 12, 2014, the EU Parliament voted decisively to adopt the compromise draft of the General Data Protection Regulation. If implemented, the Regulation will make far-reaching changes to EU data protection law, including the introduction of significant penalties for noncompliance. The next step in the legislative process will be the consideration by the EU Council of Ministers, which includes representation from all 28 EU Member States.

EU Parliament Approves Revised Draft of Cyber Security Directive
The EU Parliament approved on March 13, 2014, a revised draft of the Cyber Security Directive first issued by the EU Commission in early 2013. The Directive will impose mandatory obligations on public authorities and market operators, and thereby aims to harmonize cybersecurity across the EU. With its revisions, the EU Parliament provided for a clearer definition of the critical infrastructure businesses that will be subject to the Directive (information society services are no longer subject to the Directive). The revised draft still needs to be approved by the Council of the European Union. It thus is not yet known when the Directive will become final and whether and to what extent further changes will be applied.

Questions Arise Concerning Data Transfers to U.S. under Safe Harbor Program
While the EU Parliament called in March 2014 for the suspension of the safe harbor program, the U.S.–EU summit of March 26, 2014, indicated that the program will remain in place but is likely to be modified. In a joint statement, U.S. and EU leaders communicated that they are "committed to strengthening the Safe Harbour Framework in a comprehensive manner by summer 2014, to ensure data protection and enable trade through increased transparency, effective enforcement and legal certainty when data is transferred for commercial purposes."

Article 29 Working Party Publishes New Opinions
In March and April 2014, the Article 29 Working Party, an independent European advisory body on data protection and privacy composed of representatives of all EU Member State data protection authorities, published several opinions/working documents providing guidance on various privacy issues. The publications concern (i) the notion of legitimate interests, (ii) anonymization techniques, (iii) surveillance of electronic communications for intelligence and national security purposes, (iv) personal data breach notifications, and (v) draft ad hoc contractual clauses.

Article 29 Working Party Issues Draft Clauses for Data Transfers from EU Data Processors to Non-EU Data Subprocessors
The Article 29 Working Party issued on March 21, 2014, a working document on draft ad

hoc contractual clauses for the transfer of personal data between EU-based data processors and non-EU-based data subprocessors. The EU data protection framework of Directive 95/46/EC prohibits the transfer of personal data outside of the EU without sufficient legal safeguards. The draft clauses adopted by the Article 29 Working Party will be helpful for registration with national data protection authorities of data processing involving data transfers between EU and non-EU processors.

New Call for Interest for Position of European Data Protection Supervisor
The European Data Protection Supervisor ("EDPS") acts as data protection authority for the EU institutions and bodies and plays an instrumental role in advising on the overhaul of data protection rules. Following an initial call for applications in 2013, the European Commission is expected to publish a new vacancy notice soon.

European Data Protection Supervisor Publishes Preliminary Opinion on Interplay Between Data Protection, Competition Law, and Consumer Protection
In March 2014, the European Data Protection Supervisor published a "preliminary" opinion on the interplay between data protection, competition law, and consumer protection. This opinion seeks to analyze the interrelations between these three policy areas, e.g, how the control of personal information contributes to market power in the digital economy; what are the risks posed by concentrations and the abuse of dominance where firms process massive amounts of personal data; and how the growth of a market for privacy-enhancing services can be encouraged by strengthening informed consumer choice. The opinion also identifies the need for a better understanding of services marketed as free but requiring payment in the form of a customer's personal information, as well as a theory of harm in markets where powerful players may refuse access to personal information and apply confusing privacy policies.

Spain Establishes National Cybersecurity Council
The aim of the recently established National Cybersecurity Council (source document in Spanish) in Spain is to assist the National Security Council and to provide guidance to the President of the Government in matters related to cybersecurity. Its functions are, among others, (i) the assessment of risks and threats in the field of cybersecurity, (ii) the analysis of potential crisis scenarios and their possible evolution, (iii) the drafting and updating of response plans, and (iv) the preparation of guidelines and crisis management exercises.

Spanish Data Protection Agency Publishes Draft Privacy Impact Assessment Guide
The Spanish Data Protection Agency issued a draft Privacy Impact Assessment Guide (source document in Spanish) that sets out a framework to (i) help identify data protection risks prior to the implementation of a new product or service, (ii) prevent and minimize those risks, (iii) foster confidence among users, (iv) avoid costly redesigns and damage to the image and reputation of organizations, (v) help organizations demonstrate diligence regarding data protection, and (vi) provide guidelines on privacy issues.

Spanish Data Protection Agency Fosters Notification System Regarding Security Breaches
In March 2014, the Data Protection Agency in Spain launched a new security breach notification system (source document in Spanish).

Italy Implements Defaulting Debtors Database in Telco Industry
On March 27, 2014, the Italian Data Protection Authority (*Garante Privacy*) issued the general rules regarding the *Sistema Informatico Integrato* ("SIT") applicable to the providers of electronic communications services. Once implemented, the Telco operators will be allowed to consult the SIT in order to assess the creditworthiness of prospective clients. The Italian Data Protection Authority started a consultation (source document in Italian) among the sector operators to gather additional comments or proposals.

New Law Allows French Data Protection Authority to Conduct Online Inspections

Relating to Breach of Data Protection Regulations
As a result of a law adopted on March 17, 2014 (source document in French), the French data protection authority ("CNIL") now can conduct online inspections relating to the breach of data protection regulations. This legislative change increases the powers of the CNIL and provides to the data protection authority the means to assess more efficiently and rapidly potential breaches of the data protection framework.

French Data Protection Authority Extends Scope of Simplified Formalities for Registration of Whistleblower Programs
The French data protection authority has decided to expand the availability of the existing simplified registration framework as a result of multiple requests for registration filed with the French data protection authority over the last few years in connection with whistleblower programs that included in their scope alerts relating to breaches of environment regulations, anti-discrimination provisions, and provisions relating to health and security in the workplace. The revised single authorization n°AU-004 (source document in French) now is available for businesses that include in their whistleblower scheme the aforementioned considerations. Previously, data controllers had to file a full request for authorization.

Dutch Government Responds to Decision on Validity of Data Retention Decision
In response to the decision by the European Court of Justice on the validity of the Data Retention Directive, the Dutch State Secretary of Security and Justice stated that Dutch providers must continue to retain traffic data for the coming eight weeks while the government studies the decision. Various parties in Parliament have already stated that the data retention provisions in the Directive should be abolished completely or in part.

Dutch Data Protection Authority Speaks on Heartbleed Bug
The Dutch Data Protection Authority has issued a statement (source document in Dutch) that organizations that do not update their software and retract any issued security certificates that may have been affected by the heartbleed bug in OpenSSL may be in breach of article 13 of the Dutch Data Protection Act. The Dutch Data Protection Authority recommends that parties that have been affected notify their customers/users as soon as these measures have been taken and to recommend that they change their passwords. The Dutch Data Protection Authority has announced that it will continue to observe the situation and will, for example, monitor the number of affected security certificates that are retracted.

Dutch Data Protection Authority Raises Concerns about Big Data
The Dutch Data Protection Authority in its 2013 annual report (source document in Dutch) raised concerns about "Big Data" and the associated collection and automated processing of personal data.

Dutch Council of State Seeks Clarification of Telecommunications Act Amendment
On February 20, 2014, the Council of State advised (source document in Dutch) that a proposed amendment to the Dutch Telecommunications Act that relates to the use of cookies by websites requires further clarification. The proposed amendment allows for the storage of and access to information on a user's computer in cases where such actions (i) are taken solely for the purpose of obtaining information on the quality or effectiveness of information society services, and (ii) have no or limited privacy consequences.

Revised Draft Bill on the Obligation to Notify of Data Breaches
The Dutch State Secretary of Security and Justice submitted a revised draft bill (source document in Dutch) to Parliament on February 10, 2014, regarding notification obligations for data breaches. Under the new draft, controllers will be required to notify the Dutch Data Protection Authority only if a data breach has serious adverse consequences for the protection of the personal data that is being processed. Under the original language of the draft bill, notification was required if a data breach could reasonably be assumed to lead to a substantial risk of adverse consequences for the personal data. Notably, the Dutch

Data Protection Agency in a February 20, 2014, letter (source document in Dutch) raised concerns that this change raises the threshold for notification too high.

The following Jones Day attorneys contributed to this section: Paloma Bru, Undine von Diemar, Olivier Haas, Bastiaan Kout, Ted Kroke, Jonathon Little, Afra Mantoni, Federica Morella, and Laurent De Muyter.

[Return to Top]

Asia

Revised Chinese Consumer Rights and Interests Protection Law Takes Effect
A number of newly added provisions in the revised Consumer Rights and Interests Protection Law (source document in Chinese) came into force on March 15, 2014, in the People's Republic of China. Business operators now face heavier obligations to protect the personal information of the consumer, including the obligations to (i) inform the consumer of the purpose, method, and scope of the collection of personal information and to seek consent from the consumer before collection; (ii) publish internal rules with respect to the collection and use of the consumer's personal information; and (iii) take necessary measures to protect the consumer's personal information and not to disclose, sell, or provide that information to third parties.

Provisions of Administration on Personal Information Security for Users of Mailing and Delivery Services Take Effect
On March 26, 2014, the State Post Bureau in the People's Republic of China issued the Provisions of Administration on Personal Information Security for Users of Mailing and Delivery Services (source document in Chinese), which regulate postal and express delivery companies operating a business in or having its services consumed in China in relation to the personal data security of their consumers.

Hong Kong's Administrative Appeal Board Affirms Privacy Commissioner's Decision on Clandestine Photo-Taking of Artists by Media Organizations
On January 6, 2014, the Administrative Appeal Board affirmed the decision by the Privacy Commissioner in Hong Kong to issue enforcement notices to two magazines in relation to their clandestine photo-taking of artists at their private residence because the clandestine photo-taking amounted to "unfair means" by which personal data of the artists were collected and therefore contravened Data Protection Principle 1(2) under the Personal Data (Privacy) Ordinance. The Principle provides that "[p]ersonal data shall be collected by means which are (a) lawful; and (b) fair in the circumstances of the case."

Hong Kong's Office of the Privacy Commissioner for Personal Data Releases Privacy Management Program Guidance
On February 18, 2014, the Office of the Privacy Commissioner for Personal Data in Hong Kong released the nonstatutory *Privacy Management Programme: A Best Practice Guide*, which provides insight and guidance to organizations for developing and improving privacy programs.

"Do Not Call" Provisions of Singapore's Personal Data Protection Act 2012 Take Effect
The Do Not Call Provisions ("Provisions") of Singapore's Personal Data Protection Act 2012 came into effect on January 2, 2014. The Provisions address the establishment of Singapore's Do Not Call Registry ("DNC Registry") and prohibit organizations from sending certain marketing messages to Singapore telephone numbers registered with the DNC Registry. Organizations are still allowed to send text and fax messages to existing customers as long as the customers are given an option to unsubscribe from the messages.

Personal Data Protection Commission Takes Action Against Violators of Do Not Call Registry Requirements

As of February 14, 2014, the Personal Data Protection Commission in Singapore has issued fines, between SGD500 and SGD1,000, to at least two organizations and notices of warning in lieu of prosecution to more than 100 others who are in breach of the Do Not Call Registry requirements.

Singapore's Personal Data Protection Commission Launches Public Consultation Process
On May 16, 2014, Singapore's Personal Data Protection Commission launched its public consultation process on the Proposed Advisory Guidelines for the education, health care, and social service sectors, as well as photography. The closing date for public submissions is June 6, 2014.

Data Protection Provisions of Singapore's Personal Data Protection Act Take Effect on July 2, 2014
Data protection provisions of Singapore's Personal Data Protection Act take effect on July 2, 2014, and establish data protection obligations such as having reasonable purposes and obtaining consent for the collection, use, or disclosure of personal data; allowing individuals to access and correct personal data; and maintaining policies and practices to ensure compliance with the Act.

Japan Releases Roadmap and Directions for Amendment of Personal Information Protection Act
On December 20, 2013, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) of the Cabinet released a decision (source document in Japanese) titled "Policy for Review of Systems Concerning Utilization of Personal Data." This decision evidences the potential for significant changes to the Personal Information Protection Act to balance the business needs for utilization of personal data and privacy protection. According to the decision, the government will release a basic outline of the amendment for solicitation of public comments and will submit a bill to amend the Act in January 2015.

The following Jones Day attorneys contributed to this section: Nigel Chin, Elaine Ho, Alice Hu, Anita Leung, and Michiru Takahashi.

[Return to Top]

Australia and New Zealand

Significant Changes to Australian Privacy Act 1988 (Cth) Take Effect
Several major changes to Australia's privacy laws took effect on March 12, 2014. Amendments to the Privacy Act 1988 (Cth) introduced by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) include: (i) broadening the scope of coverage to foreign entities with no physical presence that have an "Australian link"; (ii) enhancing enforcement powers for the Information Commissioner; (iii) changing credit reporting laws; (iv) recognizing external dispute resolution schemes; (v) allowing the Information Commissioner to develop and impose binding Privacy Codes; and (vi) most importantly, adopting 13 new Australian Privacy Principles, which introduced significant changes regarding the use and disclosure of personal information for the purpose of direct marketing and cross-border disclosure of personal information.

Legislators Reintroduce Australian Data Breach Notification Bill into Parliament
The Privacy Amendment (Privacy Alerts) Bill 2014 ("Bill") was reintroduced into the Australian Parliament's upper house on March 20, 2014. The Bill was previously introduced on May 29, 2013, but lapsed in the run-up to the 2013 federal election. In its current form, the Bill requires organizations to notify the Information Commissioner of serious data breaches in relation to personal, credit reporting, credit eligibility, or tax file number information. Significant fines and other penalties may be imposed on individuals and corporations by the Information Commissioner under new enforcement powers upon

any failure to comply with the data breach notification requirements. The Bill has passed through the lower house of Parliament and is currently in the upper house waiting its assent, which cannot occur until after the next Senate Committee meeting in July 2014.

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	Brian T. Holman Irvine/Los Angeles	Robert W. Kantner Dallas	Elena Kaplan Atlanta
Jeffrey L. Kapp Cleveland	J. Todd Kennard Columbus	Beong-Soo Kim Los Angeles	Ted-Philip Kroke Frankfurt
Anita Leung Hong Kong	Jonathon Little London	Kevin D. Lyles Columbus	John M. Majoras Columbus/Washington
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 Paez New York	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	Christopher J. Lopata New York	Margaret I. Lyle Dallas
Stefano Macchi di Cellere Milan/London	Georg Mikes Frankfurt	Michael G. Morgan Los Angeles	Olivier Haas Paris
David L. Odom Dallas	Nigel Chin Singapore	Christopher S. Cogburn Atlanta	Marcelo de Antuñano Mexico City
Laurent De Muyter Brussels	Andrea Dinamarco São Paulo	Manuel Echeverría Mexico City	Bart Green New York
Joshua Grossman New York	Javier Gutiérrez Ponce Madrid	Aaron M. Healey Columbus	Elaine Ho Singapore
Nancy L. Hoffman New York	Alice Hu Hong Kong	Nandini Iyer Silicon Valley	Bastiaan K. Kout Amsterdam
Colin Leary San Francisco	Gabriel Ledeen San Francisco	Afra Mantoni Milan	Federica Morella Milan
Susan M. O'Connor New York	Nicole M. Perry Houston	Scott B. Poteet Dallas	Brandy Hutton Ranjan Columbus
Mina R. Saifi Dallas	Raquel Travesí Madrid	Nicola Walker Sydney	Zachary M. Werner New York
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].