The Sedona Conference Journal

Volume 16 2015

The Impact of Emerging Asia-Pacific Data Protection and Data Residency Requirements on Transnational Information Governance and Cross-Border Discovery

M. James Daley, Jason Priebe & Patrick Zeller

Recommended Citation:

M. James Daley et al., The Impact of Emerging Asia-Pacific Data Protection and Data Residency Requirements on Transnational Information Governance and Cross-Border Discovery, 16 Sedona Conf. J. 201 (2015).

For this and additional publications see: https://thesedonaconference.org/publications

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complementary basis to courthouses and public law libraries and by subscription to others ($95; $45 for conference participants and Working Group members). Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference at comments@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® designed by MargoBDesignLLC
See margobdesign.com or mbraman@sedona.net.

Cite items in this volume to "16 Sedona Conf. J. _____ (2015)."

Copyright 2015, The Sedona Conference.
All Rights Reserved.

THE IMPACT OF EMERGING ASIA-PACIFIC DATA PROTECTION AND DATA RESIDENCY REQUIREMENTS ON TRANSNATIONAL INFORMATION GOVERNANCE AND CROSS-BORDER DISCOVERY*

*M. James Daley***
Seyfarth Shaw LLP
Chicago, IL

*Jason Priebe****
Seyfarth Shaw LLP
Chicago, IL

*Patrick Zeller*****
Gilead Sciences, Inc.
Foster City, CA

INTRODUCTION

This paper provides a high-level overview of the current Asia-Pacific Data Protection and Information Governance landscape and trends, as reflected by data protection legislation and

* This paper was prepared for the 7th Annual Sedona Conference International Programme on Cross-Border Discovery and Data Protection Laws held in Hong Kong, China, on 8-9 June 2015. The authors wish to acknowledge the assistance of Natalya Northrip, Counsel with Seyfarth Shaw LLP, in the preparation of this article.

** M. James Daley, Esq., CIPP/US, is Senior Counsel with Seyfarth Shaw LLP in Chicago. Jim has over thirty years of complex litigation experience, a Master's Degree in Information Systems Management, and is a Certified Information Privacy Professional (CIPP/US) with the International Association of Privacy Professionals. Jim blends his legal and technical expertise in helping clients implement practical, innovative approaches for reducing the legal risk and cost of compliance with global information governance, eDiscovery, and data privacy/protection obligations. Jim is a Charter Member of The Sedona Conference Working Group 1 (U.S. Electronic Records Retention and Production), and is a Charter Member and Past Co-

regulation in Australia, South Korea, Hong Kong, and Mainland China. It is intended as a starting point for analysis, given the recent seismic shifts in this landscape due to developments such as the APEC Cross-Border Transfer Guidelines (CBTG)[1] and those arising from the Edward Snowden revelations in recent years regarding NSA surveillance. The latter, in particular, has

---

Chair of Working Group 6 (Int'l. Electronic Information Management, Discovery & Disclosure), where he served as Co-Chair from 2007 to 2012.

*** Jason Priebe, Esq., Senior Counsel with Seyfarth Shaw in Chicago, focuses his current practice on electronic discovery preparedness, planning, and execution, as well as information privacy, information governance, and data security. His trial and eDiscovery litigation experience includes nationwide multi-district and class action cases in diverse industries, involving claims ranging from global Intellectual Property and Employment to large-scale Commercial Litigation and Regulatory Investigations. Jason is a member of The Sedona Conference Working Group 1 (U.S. Electronic Records Retention and Production) and Working Group 6 (Int'l. Electronic Information Management, Discovery & Disclosure).

**** Patrick E. Zeller, Esq., CIPP/US is Director and Sr. Counsel for Global eDiscovery and Privacy at Gilead Sciences. Patrick is a member of The Sedona Conference Working Group 1 (U.S. Electronic Records Retention and Production) and Working Group 6 (Int'l. Electronic Information Management, Discovery & Disclosure), and is a Certified Information Privacy Professional (CIPP/US) with the International Association of Privacy Professionals. Patrick is an Adjunct Professor at the John Marshall School of Law, a Board Member of The Cardozo Data Law Initiative (CDLI), and was just named the 2015 Recipient of the Information Governance Program of the Year by the Information Governance Initiative.

1. *See APEC Privacy Framework (2005)*, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (last visited June 24, 2015).

spawned an alarming trend toward implementation of data residency (i.e., data localization) requirements[2] which, if aggressively enforced, may bolster data and Internet "nationalism" at the expense of global economic growth, restrict cloud computing options,[3] and stem the free flow of data for legitimate legal, business, and scientific purposes. This is a significant concern because cross-border data flows are an essential element of strong economic growth, and unduly restricting them adversely impacts economic growth.[4]

Together with recent developments in Europe, including the EU "Digital Single Market" initiative[5] and the imminent EU Regulation on Data Protection,[6] harmonizing global data protection requirements is an increasingly complex challenge.

This paper begins with a summary of the current APEC Cross-Border Privacy Rules Framework. APEC (Asia-Pacific

---

2. Kenneth Corbin, *Cross-Border Data Transfer Restrictions Threaten Global Economic Growth*, CIO MAGAZINE (Feb. 26, 2015), http://www.cio.com/article/2889461/big-data/cross-border-data-restrictions-threatens-global-economic-growth.html.

3. Steven C. Bennett, M. James Daley & Natascha Gerlach, *Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A. Patriot Act*, 13 SEDONA CONF. J. 202 (2012). *But see* South Korea's move toward expansion of cloud computing, *infra* text accompanying notes 108-11.

4. Daniel Castro & Alan McQuinn, *Cross-Border Data Flows Enable Economic Growth in All Industries*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (Feb. 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf.

5. Press Release, Eur. Comm'n, *A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen* (May 6, 2015), http://europa.eu/rapid/press-release_IP-15-4919_en.htm.

6. Ben Rossi, *Countdown to the EU General Data Protection Regulation: 5 Steps to Prepare*, INFORMATION AGE (Mar. 24, 2015), http://www.information-age.com/it-management/risk-and-compliance/123459219/countdown-eu-general-data-protection-regulation-5-steps-prepare.

Economic Cooperation) comprises twenty-one countries, fourteen of which are located in the Asia-Pacific Region.[7] This Framework, according to some commentators, may provide a model for global cross-border data protection.[8]

The selected country-specific sections below provide a general overview of representative legislation and regulation falling under the broader category of "Data Protection."[9] For the purpose of this paper, we treat data protection as subsuming the subtopics of data privacy, data security, data residency, state and commercial secrets protection, processing, cross-border transfers of personal data necessary to protect legitimate business and legal interests (e.g., U.S./EU Safe Harbor Framework, EU Model Contract Clauses, and EU Binding Corporate Rules), personal data in the "cloud," and use of personal data by data brokers and others for behavioral profiling and marketing. We believe all of these concerns relate to the protection of personal data, and believe a case can be made for a common global definition in this regard. For example, there can be no protection of personal data without the proper balance of data privacy and data security policy, process, and technology.

---

7. These include Australia, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, New Zealand, the Philippines, Papua New Guinea, Singapore, Chinese Taipei, Thailand, and Vietnam. Other members include the U.S., Brunei Darussalam, Canada, Chile, Mexico, Peru, and Russia. *See* www.apec.org.

8. Anick Fortin-Cousens & Marcus Heyden, *APEC Privacy Rules for Cross-Border Data Flows—A Model for Global Privacy Protections*, PRIVACY AND SECURITY LAW REPORT (BNA), 14 PVLR 10 (Mar. 2, 2015).

9. M. James Daley, David Moncure & Jason Priebe, *The Potential Application of the Sedona Conference International Principles and Protocol on Cross-Border Transfers with Brazil, Russia and India*, The 5th Annual Sedona Conference International Programme on Cross-Border Discovery and Data Protection Laws (June 2013); M. James Daley, *Information Age Catch 22: The Challenge of Technology to Cross-Border Disclosure and Data Privacy*, 12 SEDONA CONF. J. 121 (Fall 2011).

EXECUTIVE SUMMARY: KEY ASIA-PACIFIC DATA PROTECTION THEMES

Following are some common and unique observations relating to the impact of emerging Asia-Pacific data protection and data residency requirements on transnational information governance and cross-border discovery.

- Data residency/localization laws, requiring the in-country storage of all information passing within a country's borders, are on the rise, fueled by anti-NSA surveillance sentiment. While Brazil has backed off its early data-protectionist effort to require all Brazil data to be housed in Brazil, these initiatives are being considered or have been adopted in Australia, Russia, Malaysia, and China, among others.
- Many Asia-Pacific countries, including China and South Korea, have sectoral data protection strategies that remain in flux. Those doing business in Asia-Pacific countries need to give vigilant attention to these developments in coming months and years.
- Encryption, both in transit and in the cloud, as well as "tokenization" are being embraced as measures, and perhaps soon as standards, that can help bolster data protection, particularly for sensitive personal data.
- Guiding principles such as proportionality, accountability, data minimization (including anonymization and pseudonymization), the right of erasure, and data protection by design (i.e., default) are common themes among Asia-Pacific data protection laws and regulations.

- Common-law countries tend to follow the lead of other common-law jurisdictions with respect to regulation of processing and transfer of personal data. Australia's approach compares more closely with Canada, the U.S., the UK, and Hong Kong, than with civil law countries like China.
- The APEC Cross-Border Privacy Framework shows promise for harmonization of EU and Asia-Pacific cross-border transfers, as well as a potential global framework for balancing privacy protection with the free flow of information necessary to fuel economic growth.
- Traditional notions of "care, custody, or control," in the context of cross-border discovery and disclosure, continue to be blurred by cloud computing realities.
- U.S. legal practitioners are increasingly advised to provide documentary and testimonial evidence of the strength of foreign interests in data protection, as well as the likelihood of sanctions and penalties, in order to successfully avoid or restrict cross-border discovery.
- Global cloud computing will likely be significantly impacted by country-specific data residency initiatives. Multinationals exploring substantial enterprise investments in cloud computing infrastructure should be alert to the new data protection costs, burdens, and risks.

APEC CROSS-BORDER PRIVACY FRAMEWORK

In recent years, APEC, whose mission is to promote free trade and economic development in the Asia-Pacific region, has been a global leader in developing practical, innovative data

protection strategies for cross-border transfers of personal information. In 2012, APEC developed its Cross-Border Privacy Rules Framework, whereby controllers of personal data/information can be certified by APEC as compliant with fair information privacy and data protection principles.[10] In February 2015, this was followed by adoption of Privacy Recognition for Processors (PRP) as a means of certifying that companies are in compliance with Cross-Border Privacy Rules (CBPR).[11] In addition, there is an ongoing effort between APEC and the EU Article 29 Working Party to try to harmonize the APEC CBPRs with the EU Binding Corporate Rules (BCRs), in furtherance of one global framework supporting the free flow of information, with adequate privacy and security transfer safeguards.[12]

So far, the U.S., Mexico, and Japan have been accepted into the CBPR program, and Canada's accession is imminent. South Korea, the Philippines, Thailand, Vietnam, Singapore, Hong Kong, and Australia have affirmed their interest and/or have taken steps toward participation. The difference is in rigid compliance monitoring, oversight, and enforcement, which critics claim has been sorely lacking with the Safe Harbor Framework.

The 2005 APEC Privacy Framework notes in its Foreword that APEC believes a common framework to enable global

---

10. APEC's Cross-Border Privacy Rules, http://www.cbprs.org (last visited June 24, 2015).

11. *See* APEC Cross Border Privacy Rules System, http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx (last visited June 24, 2015) [hereinafter APEC Cross Border Privacy Rules System].

12. *See* Opinion 02/2014 of the Article 29 Working Party on a 'referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents,' WP 212 (Feb. 27, 2014), *available at* http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/wp212_en.pdf.

and regional data transfers will benefit consumers, businesses, and governments. It notes that APEC Ministers have endorsed the APEC Privacy Framework because they recognize that effective privacy protections are needed to promote the free flow of information that is essential to global economic growth.

As of March 2015, ten multinational companies have earned APEC CBPR certification, including Apple, IBM, Hewlett-Packard, Box, JELD-WEN, Merck & Co., and Ziff-Davis, among others. Initial (and ongoing) compliance of these companies with APEC CBPR is assured by an APEC authorized Accountability Agent. Governance of the APEC CBPR system rests with the APEC Joint Oversight Panel, which is responsible for approving economy-level participation and managing accountability agent certification.[13]

ANALYSIS OF DATA PROTECTION FRAMEWORKS IN SELECTED ASIA-PACIFIC JURISDICTIONS

1. Australia

Overview

Australian Federal Laws

Data privacy in Australia is subject to federal, state, and territory laws. The Federal Privacy Act 1988 ("Privacy Act")[14] regulates how organizations collect, use, store, secure, and transfer personal information. The Privacy Act was last amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012,[15] which came into effect on March 12, 2014.

13. *See* APEC Cross Border Privacy Rules System, *supra* note 11.
14. *Privacy Act 1988* (Cth).
15. *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

The amendments included the thirteen Australian Privacy Principles (APPs),[16] which replaced the Information Privacy Principles (IPPs) that previously applied to Australian and Norfolk Island Government agencies and the National Privacy Principles (NPPs) that previously applied to private sector entities. The APPs govern the collection, use, disclosure, and security of personal information, cross-border transfers, and access to and correction of personal information.

The APPs apply to both the government and private sectors. Specifically, the APPs apply to Australian and Norfolk Island government agencies; all private companies with an annual turnover of at least AUD$3 million; and certain private companies with a turnover of AUD$3 million or less, including private sector health service providers, businesses that trade personal information, credit reporting organizations, and businesses related to a business covered by the Privacy Act.[17] Entities covered by the Privacy Act and the APPs are called "APP entities."

The APPs do not apply to state or territory government agencies, including state and territory public hospitals and health care facilities, public schools, small business operators (with some exceptions), and registered political parties.[18]

16. *Privacy Act 1988* (Cth) sch 1.

17. *Who Has Responsibilities Under the Privacy Act?*, OFFICE OF THE AUSTL. INFO. COMM'R, http://www.oaic.gov.au/privacy/who-is-covered-by-privacy (last visited June 24, 2015).

18. *Who Doesn't Have Responsibilities Under the Privacy Act?*, OFFICE OF THE AUSTL. INFO. COMM'R, http://www.oaic.gov.au/privacy/who-is-covered-by-privacy (last visited June 24, 2015).

The Privacy Act is administered by the Privacy Commissioner under the Office of the Australian Information Commissioner (OAIC),[19] which is tasked with privacy, freedom of information, and government information functions. As amended in 2014, the Privacy Act now provides for enhanced privacy protection enforcement by giving the Privacy Commissioner the power to conduct *sua sponte* investigations of any breaches of the APPs. The Privacy Commissioner can now also request a court order fining a corporation up to AUD$1.7 million for serious or repeated interferences with the privacy of individuals.

In addition to the state and territory laws below, several other federal laws and regulations have data-protection provisions, including the Telecommunications Act 1997 and SPAM Act 2003.

Australian State and Territory Laws

Australian states and territories, except for Western Australia and South Australia, each have their own data protection laws applying to state government agencies and private businesses.[20] These acts are: (1) Information Privacy Act 2014 (Australian Capital Territory), governing public sector agencies;[21] (2) Health Records (Privacy and Access) Act 1997 (Australian Capital Territory), governing health care providers;[22] (3) Privacy and Personal Information Protection Act 1998 (New South Wales), governing public sector agencies;[23] (4) Health Records

19. OFFICE OF THE AUSTL. INFO. COMM'R, http://www.oaic.gov.au/ (last visited June 24, 2015).

20. *State and Territory Privacy Law*, OFFICE OF THE AUSTL. INFO. COMM'R, http://www.oaic.gov.au/privacy/other-privacy-jurisdictions/state-and-territory-privacy-law (last visited June 24, 2015).

21. *Information Privacy Act 2014* (ACT).

22. *Health Records (Privacy and Access) Act 1997* (ACT).

23. *Privacy and Personal Information Protection Act 1998* (NSW).

and Information Privacy Act 2002 (New South Wales), governing health care providers;[24] (5) Information Act 2002, as amended in 2014 (Northern Territory), governing public sector organizations;[25] (6) Information Privacy Act 2009 (Queensland), governing public sector agencies;[26] (7) Personal Information Protection Act 2004 (Tasmania), the law of general application, governing both the public and the private sectors;[27] (8) Privacy and Data Protection Act 2014 (Victoria), governing the public sector;[28] and (9) Health Records Act 2001, as amended in 2014 (Victoria), applying to the public and private sectors.[29]

The state and territory laws generally adopt privacy principles similar to the federal law. As indicated above, most of the state and territory laws apply to the public, not private, sector.

Data Protection and Privacy in Australia

Under the Privacy Act, "personal information" is defined as "information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not."

Sensitive personal data, which is referred to as "sensitive information" in Australia, includes an "information or opinion" about an individual's racial or ethnic origin; political opinions; membership in a political association; religious and philosophical beliefs; sexual orientation or practices; criminal records; and health, genetic, and biometric information.

---

24. *Health Records and Information Privacy Act 2002* (NSW).
25. *Information Act 2002* (NT).
26. *Information Privacy Act 2009* (Qld).
27. *Personal Information Protection Act 2004* (Tas).
28. *Privacy and Data Protection Act 2014* (Vic).
29. *Health Records Act 2001* (Vic).

Unlike some other countries, Australia does not maintain a register of controllers or of processing activities. As such, there is no requirement for an organization to notify/report to the privacy commissioner its personal information processing activities. There is also no requirement in the Privacy Act that organizations appoint a data protection officer (DPO), although the privacy commissioner has issued guidance strongly recommending it.

APP entities are expected to manage personal information in an "open and transparent way."[30] An APP entity "must" implement practices and procedures to ensure its compliance with the APPs. To that end, an APP entity "must" have an APP privacy policy that contains certain specific information, including the kinds of personal information that the entity collects and holds, how and for what purposes the entity collects and holds personal information, how an individual may access his or her personal information held by the entity and seek correction of such information, and whether the entity is likely to transfer personal information abroad. If the entity expects to disclose personal information to overseas recipients, it should specify the countries in which such recipients are likely to be located if it is practicable to do so.[31]

An APP entity which is a private company must not collect personal information unless the information is "reasonably necessary" for, and directly related to, one or more of its business functions or activities. Furthermore, a private company must not collect "sensitive information" unless the individual consents to the collection of the information and the information

30. *Privacy Act 1988* (Cth) sch 1, APP 1.

31. *Id.*

is "reasonably necessary" for one or more of its business functions or activities, or the collection is otherwise justified by enumerated situations.[32]

Once personal information is collected for a particular purpose (the primary purpose), the entity "must not" use or disclose the information for another purpose (the secondary purpose) unless the individual has consented to the use or disclosure of the information, or the individual would reasonably expect such use or disclosure and such use or disclosure relates to the primary purpose, or another specific condition exists.[33]

In Tasmania, likewise, a personal information custodian must not collect personal information unless the information is necessary for one or more of its functions or activities.[34] If personal information is collected, the custodian must inform the data subject of various matters, including the custodian's identity and contact information, the individual's right to access information, the purposes for which the information is collected, and the intended recipients or class of recipients of the information.[35] Furthermore, personal information custodians "must" collect personal information about an individual only from that individual, "if it is reasonable and practicable to do so."[36] If, however, personal information is collected from a third party, the personal information custodian "must take reasonable steps" to ensure that the individual is made aware of all the matters described above.[37]

32. *Id.* APP 3.

33. *Id.* APP 6.

34. *Personal Information Protection Act 2004* (Tas) sch 1, s 1(1).

35. *Id.* s 1(3).

36. *Id.* s 1(4).

37. *Id.* s 1(5).

Tasmania also places restrictions on the use and disclosure of information, generally limiting disclosure to purposes that relate to the primary purpose for which it was collected, unless the individual consents to disclosure.[38] Tasmania also grants individuals a right, wherever it is lawful and practicable, to choose not to identify themselves when entering transactions with a personal information custodian.[39]

Data Security in Australia

The Privacy Act requires APP entities to have appropriate security measures in place to protect the information from misuse, interference, loss, unauthorized access, modification, or disclosure.[40]

Furthermore, once the information has served the purpose for which it was collected and the entity is not legally required to retain that information any further, the entity must take "reasonable steps" to destroy the information or to ensure that the information is de-identified.[41]

In April 2013, OAIC issued a thirty-two page Guidance to Information Security on what constitutes "reasonable steps" to protect personal information ("Guidance").[42] The Guidance provides for substantially more than what many businesses are doing to protect the information. Under the Guidance, organizations should manage data governance, IT security, data breaches, physical security, personnel security and training,

38. *Id.* s 2.

39. *Id.* s 8.

40. *Privacy Act 1988* (Cth) sch 1, APP 11.

41. *Id*.

42. Office of the Austl. Info. Comm'r, *Guide to Information Security: 'Reasonable steps' to protect personal information* (Apr. 2013), http://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf.

workplace policies, the information life cycle, standards, and regular monitoring and review. Entities are also expected to undertake a Privacy Impact Assessment and an information security risk assessment in order to inform the steps and strategies they will take to secure personal information.

Currently, the Privacy Act does not obligate APP entities to report data security breaches to the affected individuals or the OAIC. However, the OAIC issued guidance on data breach notification stating that if there is "a real risk of serious harm" as a result of a data breach, the affected individuals and the OAIC should be notified.[43]

In Tasmania, in addition to protecting personal information from misuse, loss, unauthorized access, modification, or disclosure, a personal information custodian "must take reasonable steps" to destroy or permanently de-identify personal information if it is no longer needed for any purpose.[44]

On April 13, 2015, the Parliament of Australia passed the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015,[45] which creates new obligations on Information and Communications Service Providers (ICSPs) to retain prescribed information or documents (metadata) for a period of two years to allow access by national security authorities and governmental agencies, including criminal law enforce-

43. Office of the Austl. Info. Comm'r, *Data breach notification guide: A guide to handling personal information security breaches* (Aug. 2014), http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/data-breach-notification-guide-august-2014.pdf.

44. *Personal Information Protection Act 2004* (Tas) sch 1, s 4.

45. *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015* ("Data Retention Bill").

ment. The bill requires ICSPs to ensure the confidentiality of information by encrypting the retained data, subject to certain exemptions.[46]

Data Residency / Localization in Australia

The Personally Controlled Electronic Health Records Act 2012 (PCEHR), which went into effect in July 2012, contains a requirement "not to hold or take records outside Australia."[47] As such, PCEHR prohibits the overseas storage of any Australian electronic health records. Specifically, with certain exceptions, the act prohibits anyone holding records under the act for the purposes of the PCEHR system or having access to information relating to such records from: (a) holding the records, or taking the records, outside Australia; (b) processing or handling the information relating to the records outside Australia; or (c) causing or permitting another person: (i) to hold the records, or take the records, outside Australia, or (ii) to process or handle the information relating to the records outside Australia.[48]

The act does permit transfer, processing, or handling of data outside of Australia if such records do not include "personal information in relation to a consumer" or "identifying information of an individual or entity."[49] In practice, under these provisions, multi-national companies handling health-related information must either invest in their own data centers located in Australia or outsource their data to an Australian cloud services provider.

46. *Id.* s 187BA.

47. *Personally Controlled Electronic Health Records Act 2012* (Cth) s 77.

48. *Id.* s 77(1).

49. *Id.* s 77(2).

Cross-Border Data Transfers in Australia

Regulations in Australia make it difficult for companies to transfer personal information to overseas recipients, including cloud providers that store data outside of Australian borders. Under APP 8, before an APP entity can disclose information about an individual to an overseas recipient, including a cloud provider, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.[50] This can be accomplished through appropriate contractual provisions. However, the Australian sender of personal information will remain liable for the overseas recipient's acts and practices with respect to the transferred personal information as if the Australian sender had engaged in such breaches of the APPs in Australia.

These limitations on transfer do not apply under certain circumstances, including (1) if the APP entity reasonably believes that the overseas recipient is subject to a law that provides protections "substantially similar" to the APPs and the individual can enforce those protections; or (2) the entity expressly informs the individual that if he or she consents to the disclosure of the information then the APP protections will not apply, and the individual consents to the disclosure nonetheless.

In practice, compliance with APP 8 can be achieved through (1) obtaining the necessary consents from individuals whose personal information will be transferred overseas, including to a non-Australian cloud provider, and (2) placing the necessary APP-specific contractual privacy obligations on the overseas recipient of the personal information.

Similarly, New South Wales legislation forbids trans-border transfer of health information. The exceptions include

50. *Privacy Act 1988* (Cth) sch 1, APP 8.1.

where the individual consents or where the organization reasonably believes that the recipient in an outside jurisdiction is subject to a law that effectively upholds principles for "fair handling of the information" that are "substantially similar" to the Health Privacy Principles of New South Wales.[51]

Likewise, in Tasmania, a personal information custodian may disclose personal information to a third party who is outside Tasmania only under a limited set of circumstances, including the following: (1) the custodian reasonably believes that the recipient of the information is subject to a law that provides substantially similar personal information protections, (2) the individual consents to the disclosure, or (3) the disclosure is necessary for the performance of a contract between the individual and the custodian.[52] The same limitations apply in Victoria on the transfer of personal health information to recipients outside Victoria.[53]

Data in the Cloud in Australia

The Australian government discourages the use of foreign cloud providers. For instance, in its *Cloud Computing Strategic Direction Paper*,[54] the Australian Department of Finance and Deregulation cites the U.S. Patriot Act as the example of foreign legislation that presents legal and regulatory risks and potentially exposes consumer data to being scrutinized by foreign governments. Additionally, in the same paper, the Australian

51. *Health Privacy Principles, Principle 14*, *Health Records and Information Privacy Act 2002* (NSW) sch 1.

52. *Personal Information Protection Act 2004* (Tas) sch 1 s 9.

53. *Health Records Act 2001* (Vic) sch 1, Principle 9.

54. Australian Department of Finance and Deregulation, *Cloud Computing Strategic Direction Paper* (April 2011), http://www.finance.gov.au/files/2012/04/final_cloud_computing_strategy_version_1.pdf.

government generally cautions of the risks of third-party access to personal information residing in the cloud.

Use of Personal Data by Marketers and Data Brokers in Australia

Under APP 7, which governs direct marketing, if an organization holds personal information about an individual, the organization generally must not use or disclose the information for the purpose of direct marketing.[55] An organization may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if: (a) the organization collected the information from the individual; (b) the individual would reasonably expect the organization to use or disclose the information for that purpose; (c) the organization provides a simple means by which the individual may easily request not to receive direct marketing communications from the organization; and (d) the individual has not made such a request to the organization.[56]

2. South Korea

Overview

Until recently, South Korea did not have a comprehensive legislation scheme governing data privacy. That changed when the South Korean Personal Information Protection Act (PIPA) went into effect on September 30, 2011.[57] PIPA governs the protection of personal information except as otherwise specifically provided for in any sector-specific legislation.

55. *Privacy Act 1988* (Cth) sch 1, APP 7.1.

56. *Id.* APP 7.2.

57. *South Korean Personal Information Protection Act*, Sept. 30, 2011, *as amended* [hereinafter *PIPA*].

The sector-specific laws include various statutes, such as the Act on Promotion of Information and Communication Network Utilization and Information Protection 2005 ("IT Network Act"),[58] the Use and Protection of Credit Information Act,[59] the Financial Holding Companies Act (FHCA),[60] and the Real Name Financial Transactions and Secrecy Act.[61]

In 2014, after experiencing one of the biggest credit card data breaches that affected 20 million people in this nation of 50 million, South Korea reformed its data protection policy by amending PIPA and FHCA. The PIPA and FHCA amendments created significant challenges for financial and other businesses in South Korea and they have been criticized as overreaching and highly burdensome.

For instance, under the new amendments to PIPA, which became effective on August 7, 2014, the processing of resident registration numbers (RRNs) by private corporations is in principle prohibited. And under the amended FHCA, which became effective on November 29, 2014, to prevent mass data leaks, the transfer of customers' personal information within financial holding groups is now limited only to situations where data transfer is necessary for specific purposes as defined in the amendment and related regulations. Notably, the scope of those

58. *Act on Promotion of Information and Communication Network Utilization and Information Protection*, Dec. 30, 2004, *amended by* Act No. 7812, Dec. 30, 2005 [hereinafter *IT Networks Act*].

59. *Use and Protection of Credit Information Act*, Act No. 4866, Jan. 5, 1995, *amended by* Act No. 8863, Feb. 29, 2008.

60. *Financial Holding Companies Act*, Act No. 6274, Oct. 23, 2000, *amended by* Act No. 9086, Mar. 28, 2008.

61. *Real Name Financial Transactions and Secrecy Act*, Act No. 5493, Dec. 31, 1997, *amended by* Act No. 6682, Mar. 30, 2002.

purposes does not include the introduction or solicitation of sale of products or services to customers.[62]

Data Protection and Privacy in South Korea

The stated purpose of PIPA is to provide for the "processing and protection" of personal information to strengthen the rights and interests of data subjects.[63] Under PIPA, "personal information" is information pertaining to a living person that makes it possible to identify a specific person by his or her name, RRN, images, or other similar information, including information that does not by itself make it possible to identify a specific individual, but can make it possible if combined with other information.[64] The IT Network Act, Article 2, defines "personal information" similarly, but also specifically includes "code, letter, voice, sound, and image" within the definition.[65]

PIPA broadly defines "processing" as "the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, retrieval, correction, recovery, use, provision, disclosure, and destruction of personal information and other similar activities."[66]

A personal information processor may collect personal information only under specific circumstances, which include data subject's consent.[67] For consent to be valid under PIPA, the data processor seeking consent must notify the data subject of the following: (1) the purpose of collection and use of personal

62. Sky Yang, *Korea Tightens Data Protection Rules*, INT'L FIN. LAW REVIEW (Feb. 23, 2015), http://www.iflr.com/Article/3429777/Korea-tightens-data-protection-rules.html.

63. *PIPA, supra* note 57, art. 1.

64. *Id.* art. 2(1).

65. *IT Networks Act, supra* note 58.

66. *PIPA, supra* note 57, art. 2(2).

67. *Id.* art. 15(1).

information, (2) the particulars of personal information to be collected, (3) the period when personal information is retained and used, and (4) the fact that the data subject may deny consent and the consequences resulting from that denial.[68] Data processors collecting personal information in violation of these requirements may be fined for negligence up to KRW 50 million (approximately $45,000 U.S. dollars).

PIPA allows data processors to collect only the minimum personal information necessary to fulfill the purpose of collection. Furthermore, data processors are required to inform data subjects that they have a right to deny consent to the collection of any personal information above that necessary minimum.[69]

The amended PIPA allows the processing of "sensitive data," including ideology, beliefs, membership in trade unions or political parties, health, sexual life, and other personal information which may cause harm to privacy of data subjects, provided that the data subject gives his or her specific informed consent (apart from consent to the processing of other personal information processing) or where the processing of sensitive data is required or permitted by law.[70]

The original PIPA allowed the processing of RRNs with data subject's consent, which was easy to obtain. As a result, in the past, RRNs have been widely used as the personal identification information in every sector of the economy, including administrative, financial, and medical. The amended PIPA explicitly prohibits the processing of RRNs, regardless of the data subject's consent. There are three exceptions to this prohibition: (1) where the processing is required by law; (2) where the pro-

68. *Id.* art. 15(2).

69. *Id.* art. 16(1).

70. *Id.* art. 23.

cessing is deemed explicitly necessary for the impending protection of life, body, or interest in property of the data subject or a third person; or (3) where the processing is unavoidably in line with the enforcement regulation promulgated by the Ministry of Public Administration and Security (MOPAS) to facilitate the key administrative services conducted by public authorities.

Effectively, the prohibition on the processing of RRNs would require most companies to conform their systems and databases to store, process, and recall data without relying on RRNs as the primary identifiers of their customers.

PIPA requires every personal data processor to establish the personal information processing policy, the "Privacy Policy," setting forth such specifics as the purpose of personal information processing, the length of data retention, data transfers to third parties, and the rights and obligations of data subjects.[71] As such, any company processing personal data of Korean residents would need to establish and implement a Privacy Policy that contains the elements specified by PIPA.

Additionally, PIPA grants a variety of data rights to data subjects and places corresponding obligations on data processors. These rights include access to personal information,[72] correction or deletion of personal information,[73] and suspension of processing of personal information.[74] Companies processing personal data need to have procedures in place that allow data subjects to exercise their rights under PIPA.

71. *Id.* art. 30.

72. *Id.* art. 35.

73. *Id.* art. 36.

74. *Id.* art. 37.

Data Security in South Korea

Personal information processors in South Korea are required to implement technical, managerial, and physical measures that are necessary to ensure the safety of data as specified by the Presidential Decree.[75] Data processors who fail to implement the required security measures and who suffer data loss may be fined up to 500 million won (or $462,690 U.S. dollars).[76]

For instance, a personal information processor who collects RRNs must protect that data through "encryption so that it may not be lost, stolen, leaked, altered or damaged."[77] PIPA also requires personal information processors to designate a privacy officer, who shall establish and oversee the implementation of the "data protection plan," establish internal controls to prevent unauthorized disclosure and misuse of personal information, prepare and implement the data protection education program, and protect and manage the personal information.[78] Upon learning of any data privacy violations, the privacy officer must take immediate corrective measure and, if necessary, report such corrective measures to the head of the organization and relevant organizations.[79]

Under PIPA, a data processor who learns of a data breach must immediately notify the affected individuals and identify the kind of personal information that was breached, when and how it was breached, remedial measures, as well as what the affected individuals can do to minimize damage.[80] A large-scale

75. *Id.* art. 29.

76. *Id.* art. 34-2(1).

77. *Id.* art. 24-2.

78. *Id.* art. 31(1)-(2).

79. *Id.* art. 31(4).

80. *Id.* art. 34(1).

data breach is also reportable to the minister of security and public administration.[81] Furthermore, in case of a data breach, PIPA places the burden of proof on data processors. Where a data subject suffers damage caused by a data processor's PIPA violations, the data processor will be liable for damages unless it proves "non-existence of its wrongful intent or negligence."[82] Damages may be reduced for data processors that prove their compliance with PIPA and "non-negligence of due care and supervision."[83]

The IT Networks Act requires ICSPs to designate a person in charge of data protection and to take such technical and other measures that are necessary to secure the safety of the personal information.[84] Furthermore, once the ICSP "attained the objective" of collecting the personal information, it must "promptly destroy" that information, unless it must continue preserving under another law.[85]

Similarly to PIPA, under the amendments to the IT Networks Act, upon discovering a data breach, ICSPs must immediately report the breach to the Korea Communications Commission (KCC) or the Korea Internet and Security Agency (KISA), analyze causes of the breach, and prevent damage from being spread.

Under the 2014 FHCA amendment, financial institutions sharing data must notify the data subjects of the data transfer that took place at least once a year. The amended FHCA also limits the period of use of the shared data to a maximum of one

81. *Id.* art. 34(3).

82. *Id.* art. 39(1).

83. *Id.* art. 39(2).

84. *IT Networks Act*, *supra* note 58, arts. 27, 28.

85. *Id.* art. 29.

month, unless otherwise approved by the chief information officer.

Under the Use and Protection of Credit Information Act,[86] any operator of a credit information business shall implement technological and physical security measures to prevent unlawful access by third parties, modification, damage, destruction, or other dangers to electronic credit information.[87]

Data processors in South Korea must take data security seriously. It is important to determine all applicable general and sector-specific statutes and regulations and carefully comply with all data-security and data-breach related requirements. Every data processor is expected to establish and implement data protection and data breach remediation plans and be prepared to act in the event the physical and technical data security measures fail and personal data is unlawfully accessed or disclosed.

Data Residency / Localization in South Korea

An increasing number of countries, including South Korea, have begun implementing a range of strict policies aimed at localizing economic activity and data that accompanies that activity within their borders. So-called data localization laws set forth requirements to store data locally, i.e., within national borders. Countries that adopt such laws require the storage or processing of data on servers physically located within their borders. Data can be restricted based on type (e.g., financial or health records), based on the nationality of the data subject, or based on the type of the data processor (e.g., ICSP).

86. *Use and Protection of Credit Information Act*, Act No. 4866, Jan. 5, 1995, *amended by* Act No. 8863, Feb. 29, 2008.

87. *Id.* art. 19.

For instance, under IT Networks Act, the minister of information and communication may require any ICSP or any ICSP user to take measures necessary to prevent "material information regarding the domestic industry, economy, science, and technology" from being exported out of Korea into foreign countries via information and communication networks.[88]

Under the Regulation on Supervision of Credit – Specialized Financial Business, foreign e-commerce firms selling goods in Korea are prohibited from storing Korean credit card numbers and, thus, may not accept Korean branded credit cards.[89]

South Korea's data privacy rules have been criticized for effectively requiring that financial services providers locate their data servers physically inside Korea, thus hampering foreign providers' ability to perform data processing in their daily business activity.[90] However, recently, South Korea undertook commitments under both the United States – Korea Free Trade Agreement (KORUS) and the Korea – European Union Free Trade Agreement to substantially reduce these restrictions and to allow U.S.-based financial institutions in Korea to process data in their regional and global offices.[91]

---

88. *IT Networks Act*, *supra* note 58, art. 51.

89. Office of the United States Trade Representative, *2013 National Trade Estimate Report on Foreign Trade Barriers*, at 239 (March 2013), https://ustr.gov/sites/default/files/2013%20NTE.pdf.

90. *Id.*

91. *Fact Sheet: U.S.-Korea Free Trade Agreement*, OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2015/march/fact-sheet-us-korea-free-trade-agreement (last visited June 24, 2015).

Cross-Border Transfers of Data in South Korea

Commentators often argue that strict rules regulating cross-border transfers of personal data function as data localization laws by creating high regulatory hurdles for companies to comply with before data can be transferred abroad and thereby effectively requiring companies to store and process personal data within the country's borders. Under the amended PIPA, when a personal information processor provides personal information to a third party overseas, it shall notify the data subject and obtain consent.[92]

Specifically, to make overseas transfer of personal data lawful, the putative data exporter must inform the data subject of the following: (1) identity of the overseas recipient of personal information, (2) purpose for which a recipient of personal information uses such information, (3) items of personal information provided, (4) period for which a recipient of personal information holds and uses such information, and (5) the fact that a subject of information has a right to withhold his or her consent and details of a disadvantage, if any, due to such withholding.[93]

Given these restrictions, global companies doing business in South Korea need to determine whether it is more economical and efficient to obtain the data subjects' consent to data export or to store and process personal data locally, either through increased technology investments that ensure local data storage or through the use of local cloud providers.

Data Secrecy in South Korea

South Korea has several laws protecting sensitive information, including the Use and Protection of Credit Information

92. *PIPA, supra* note 57, art. 17(3).

93. *Id.* art. 17(2).

Act,[94] the Telecommunications Business Act,[95] the Medical Service Act,[96] the Real Name Financial Transactions and Secrecy Act,[97] and the IT Networks Act.

Under the Use and Protection of Credit Information Act, operators of credit information businesses are prohibited from disclosing or using "personal secrets such as credit information and private information" for non-business purposes.[98] Violators who cause damages to credit information subjects and who cannot prove that they acted without "malice or negligence" are liable for damages.[99]

The Telecommunications Business Act prohibits telecommunication carriers and their employees from disclosing any "confidential information" acquired as part of performance of telecommunication services. However, a few limited, law-enforcement related, exceptions allow the disclosure of the following information related to a user: (1) name, (2) RRN, (3) address, (4) phone number, (5) identification code to authenticate the legitimate users of a computer system or communications network, or (6) dates of service subscription or termination.[100] Most

94. *Use and Protection of Credit Information Act*, Act No. 4866, Jan. 5, 1995, *amended by* Act No. 8863, Feb. 29, 2008 [hereinafter *Use and Protection of Credit Information Act*].

95. *Telecommunications Business Act*, *amended by* Act No. 8867, Feb. 29, 2008 [hereinafter *Telecommunications Business Act*].

96. *Medical Service Act*, Act No. 1035, Mar. 20, 1962, *amended by* Act No. 10387, Jul. 23, 2010 [hereinafter *Medical Service Act*].

97. *Real Name Financial Transactions and Secrecy Act*, Act No. 5493, Dec. 31, 1997, *amended by* Act No. 6682, Mar. 30, 2002 [hereinafter *Real Name Financial Transactions and Secrecy Act*].

98. *Use and Protection of Credit Information Act*, *supra* note 94, art. 27.

99. *Id.* art. 28.

100. *Telecommunications Business Act*, *supra* note 95, art. 54.

of these exceptions will not apply to a private company in its regular course of business.

In South Korea, 82.3 percent of people are concerned about the privacy and security of their health information.[101] In addition to PIPA, health information in South Korea is also governed by the Medical Service Act, which prohibits, with some exceptions, a medical provider from disclosing a person's confidential information gathered in the course of performing medical treatment.[102] Furthermore, no one may "leak, alter or destroy" any personal information stated in an electronic medical record without "justifiable reason."[103]

The Real Name Financial Transactions and Secrecy Act guarantees the secrecy of financial transactions.[104] Specifically, it prohibits employees of financial institutions from disclosing information regarding the contents of financial transactions to other persons absent consent in writing.[105] Additionally, with limited exceptions, no one may request financial institution employees to provide transaction information.[106]

The IT Network Act prohibits any person from damaging the information of other persons or from infringing, stealing, or unlawfully disclosing the "secrets" of other persons, which are processed, stored, or transmitted via information and communications networks.[107]

---

101. Jeongeun Kim, James G. Boram Ki & Sukwha Ki, *Personal Health Records and Related Laws in South Korea*, Presentation (Sept. 25, 2013), http://www.medicine20congress.com/ocs/index.php/med/med2013/paper/view/1604.

102. *Medical Service Act*, *supra* note 96, art. 19.

103. *Id.* art. 23.

104. *Real Name Financial Transactions & Secrecy Act*, *supra* note 97, art. 4.

105. *Id.* art. 4(1).

106. *Id.*

107. *IT Networks Act*, *supra* note 58, art. 49.

Data in the Cloud in South Korea

On March 3, 2015, South Korea passed the world's first cloud-specific law aimed at promoting the adoption of cloud computing in Korea.[108] The Act on the Development of Cloud Computing and Protection of Users ("Cloud Act")[109] will take effect on September 28, 2015. The Ministry of Science, ICT and Future Planning ("Ministry"), which first introduced the Cloud Act for consideration in October 2013, is expected to issue regulations for cloud services before the Cloud Act comes into force.

The Cloud Act aims to promote the cloud market in Korea by increasing investment and support of the cloud market, in particular by encouraging the government entities to use private companies' cloud technology.[110] Under the Cloud Act, the Ministry will establish plans to enhance the cloud market and will update those plans every three years. These measures will include the development of the cloud computing market, cloud computing related research and expert training, as well as financial and other support for local providers of cloud services, such as tax incentives. The Cloud Act encourages the government entities to use private cloud services providers to benefit from cost efficiency, improve productivity, and increase South Korean industrial competitiveness.[111]

To address security and privacy issues that are perceived as the main obstacles to the use of cloud services, the Cloud Act

---

108. Daniel Jung, *Korea Leads the World with Cloud Law Encouraging Cloud Use*, ROB BRATBY BLOG (Apr. 9, 2015), http://robbratby.com/2015/04/09/korea-leads-the-world-with-cloud-law-encouraging-cloud-use/.

109. *Cloud Computing and Legal Developments Related to User Protection Act*, Act. No. 13234, Mar. 27, 2015 (effective on Sept. 28, 2015).

110. Julia Kenny, *The Uncertain Future for South Korea's Cloud*, BLOUIN NEWS BLOGS (Jan. 5, 2015), http://blogs.blouinnews.com/blouinbeattechnology/2015/01/05/the-uncertain-future-for-south-koreas-cloud/.

111. Daniel Jung, *supra* note 108.

obligates cloud services providers to institute appropriate safeguards. For instance, cloud services providers will be required to do the following: (1) report data breaches to their customers and the Ministry, (2) not transfer personal information to third parties without the data subject's consent, (3) return or delete personal information upon termination of the cloud contract, (4) disclose the location of the data, if the data is hosted outside of South Korea and the customer requests that information. Any person who provides personal data to a third party in violation of the Cloud Act shall be punished by imprisonment of up to five years or a fine not to exceed KRW 50 million (approximately $45,000 U.S. dollars).

Use of Personal Data by Marketers and Data Brokers in South Korea

The KCC recently took steps to restrict the practices of the big data analytics sector. In December 2014, the KCC issued the Big Data Guidelines for Data Protection ("Guidelines"),[112] allowing ICSPs to process personal information only if the data is de-identified before it is collected, retained, combined, analyzed or sold. Data de-identification requires that "measures [be] taken . . . so that it cannot be easily combined with other data to identify a specific individual."[113] Such measures can include "data reduction, pseudonymization, data suppression, and data masking."[114]

112. THE KOREA COMMC'NS COMM'N, *Big Data Guidelines for Data Protection*, Dec. 23, 2014.

113. Cynthia O'Donaghue & Philip Towns, *South Korean Commcations Commission Releases Guidelines on Data Protection for Big Data*, ABOVETHELAW.COM (Mar. 25, 2015), http://abovethelaw.com/2015/02/south-korean-communications-commission-releases-guidelines-on-data-protection-for-big-data/.

114. *See Big Data Guidelines for Data Protection in South Korea*, DEVSBUILD.IT (Mar. 11, 2015), http://devsbuild.it/content/Big-Data-Guidelines-Data-Protection-South-Korea.

Under the Guidelines, any data processing for the purpose of generating "sensitive information" (e.g., ideology, political views) is strictly prohibited unless specifically allowed by law or with data subject's prior consent. Additionally, collecting the contents of communications, such as emails and texts, is prohibited unless all parties to the communication provide consent.[115]

3. Hong Kong

Overview

Hong Kong's original data privacy ordinance, the Personal Data (Privacy) Ordinance (the PDPO or "Ordinance"), was enacted in 1996, shortly after the EU Directive was passed. There has, however, been a constitutionally recognized right to privacy in Hong Kong in articles 28, 29, 30, and 39 of the basic law.[116] The Ordinance consists of six thematic Data Privacy Principles (each commonly referenced as DPPs).[117] The legislation was significantly re-tooled in 2012, primarily to address unauthorized disclosure of information and direct marketing activity. For instance, a new "disclosure without consent" offense was added. The new offense contemplates improper use or disclosure through voluntary (but unpermitted) means, as well as the involuntary loss of information through an incident such as a data breach. There are civil and criminal penalties, and individual data subjects have a private right to action in some circumstances.

---

115. *Id.*

116. Hong Kong Personal Data (Privacy) Ordinance, Cap. 486, http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/B4DF8B4125C4214D482575EF000EC5FF/$FILE/CAP_486_e_b5.pdf.

117. *Id.* § 4.

Data Protection and Privacy in Hong Kong

It is tempting to draw a comparison between the EU and Hong Kong in terms of data classification and the concept of ownership of personal information. There has been historical UK influence in Hong Kong, as a result of its colonial past, and there are many similarities between EU privacy concepts and Hong Kong's Ordinance. For instance, there is an established privacy commissioner and six Data Protection Principles, which are actually based on the OECD Privacy Principles, which themselves had EU influences. However, there is not a direct parity between the EU and Hong Kong privacy regimes. In fact, an argument could be made that the more recent revisions to both Hong Kong's and China's regimes appear to point both systems in a direction that is rather more unique and focused on the wholesale use of data by direct marketing and information clearinghouse operations, accompanied by strong incentives to protect against data breaches.

DPP1 of the Ordinance requires the designation of a corporate data protection officer to whom any inquiries or requests can be presented by the privacy commissioner. A similar requirement is part of the upcoming EU Data Privacy Regulation.

Personal Data and Data User in Hong Kong

Personal Data has the same broad conceptual definition that would be recognized by anyone familiar with the EU Directive. Specifically, Personal Data is any information that relates directly or indirectly to a living data subject whose identity can be directly or indirectly determined. There is not a separate category of sensitive personal data under the Ordinance.

The Hong Kong ordinance does not distinguish between data custodians and data owners. Instead, a collective category of "Data User" describes any entity or person who controls the

collection, holding, use, or processing of personal data. Importantly, a data user is not someone who holds personal data at the instruction of a third party or on behalf of a third party. Finally, the Ordinance does not restrict or govern any actions relating to personal data that are committed outside Hong Kong—only activities which take place from within Hong Kong.

The following activities are regulated by the Hong Kong ordinance in its current form: collection, use, disclosure, retention, access, and correction of personal data by the data subject. Practitioners should be aware, however, that transfer restrictions are forthcoming. These are discussed in further detail below.

Data Processing Restrictions in Hong Kong

There are also some fairly broad exceptions that permit the types of ordinarily restricted processing activity. Exceptions include uses of personal data for governmental, journalistic, and crime prevention purposes. For business purposes, there are exceptions for corporate due diligence investigations, provided that: the information processed or used is not more than is necessary; similar products or services will be provided by a party to the transaction or a new corporate entity formed by the transaction; consent is not practicable; and data is used exclusively for the due diligence investigation. There is a generalized exception for personal data held for "domestic and recreational purposes," which, while interesting to contemplate in the abstract, would certainly not apply to any typical commercial or corporate entity.

The new amendments included additional requirements for data users to adopt "contractual or other means" to prevent

- personal data transferred to a data processor from being retained longer than necessary for the original processing purpose; and

- unauthorized or accidental access, processing, erasure, loss, or unauthorized use of personal data.

Anticipated Future Hong Kong Data Transfer Restrictions

There are not currently any regulations or restrictions on the transfer of personal data under the Ordinance (except to the extent that disclosure to a third party for direct marketing purposes could be considered a transfer). However, Section 33 of the Ordinance, which is expected to come into effect very soon, does indeed place EU-style restrictions on the transfer of personal data. Today, however, the Ordinance only covers activities relating to personal data that may loosely be understood as "processing" under the EU model. With the understanding that the Section 33 transfer restrictions are imminent, the privacy commissioner for personal data has issued a Guidance Note encouraging corporations and entities to adopt practices to restrict the transfer of personal data, unless several EU-style conditions are met. Examples of the conditions include instances where

- the destination country is recognized as providing the same or similar data productions as the Ordinance;
- the data subject has consented, in writing, to the transfer so there is no need for model contractual clauses or data transfer agreements governing the extraterritorial transfer or onward transfer of personal data; or
- the "data user" has taken all reasonable precautions and exercised all due diligence to verify that the data will not be processed or held in a manner that would violate the Ordinance if the data were still in Hong Kong.

The December 2014 Guidance Note also includes suggested model contractual clauses for inclusion in data transfer agreements, along with a list of suggested good practices and practical tips for compliance. Overall, the Guidance Note is a very useful guide for compliance with the upcoming transfer restrictions.

Because most Hong Kong employers, businesses, and international litigation counsel are not typically involved in any export or disclosure of information to third parties for direct marketing purposes, this article will not address the many new restrictions on that sort of activity in the newly updated Ordinance. Suffice to say, however, that separate disclosure requirements, including a specific notice and consent procedure and terms of service are necessary for those sorts of activity.

Data Security in Hong Kong

DPP4(1) requires data users to take "practical steps" to protect personal data from unauthorized access, loss, or use in violation of the Ordinance. Fundamental information protection methods, such as data encryption and file access controls, are not specifically spelled out in the Ordinance; however, these are certainly examples of "practical steps" that every corporation or organization should implement. In July 2014, the privacy commissioner published a Guidance Note titled "Guidance on the Use of Portable Storage Devices" that contains additional suggested precautions, including the development of a top-down risk assessment, written policies for the secure storage, control and deletion of personal data, encryption, technical controls, and monitoring.[118]

118. Office of the Privacy Comm'r for Personal Data, Hong Kong, *Guidance on the Use of Portable Storage Devices* (July 2014), https://www.pcpd.org.hk/english/publications/files/portable_storage_e.pdf.

Data Residency and Localization in Hong Kong

There are no current data localization requirements in the Hong Kong data privacy regime. However, given the strong movement in China for greater regulation and access to information, it is difficult to know how long this situation will remain.

Data in the Cloud in Hong Kong

The privacy commissioner tackled the realities and challenges cloud computing poses to personal data privacy in a November 2012 information leaflet on the topic. [119]

That publication made it clear that compliance with the DPPs under the Ordinance is still mandated for personal data stored in cloud environments. This includes limitations on the prolonged retention of personal data by third parties through the use of contractual provisions (DPP2); the limitation on processing outside the original purpose without notice and voluntary consent (DPP3); the use of reasonable protections to prevent loss, unauthorized processing, or unauthorized access of personal data (DPP4). The publication also includes a helpful discussion of the special risks posed by cloud computing and provides suggestions for handling unique challenges associated with outsourcing data storage responsibilities.

4. Mainland China

Overview

Interestingly, as in the U.S., the approach of the People's Republic of China (PRC) to data protection is quite sectoral in

119. Office of the Privacy Comm'r for Personal Data, Hong Kong, *Cloud Computing* (Nov. 2012), https://www.pcpd.org.hk/english/resources_centre/publications/files/cloud_computing_e.pdf.

nature. Provisions related to personal data protection are peppered in various statutes and regulations, but unlike the EU, there is no broad, baseline data protection framework that clearly defines the scope of all privacy rights, particularly on the individual level. One reason is that China lacks the legal infrastructure to protect individual privacy in a comprehensive manner. And despite a significant increase in litigations and investigations requiring the collection and processing of Chinese electronic information, China lacks a comprehensive framework that governs the collection, use, and transfer of personal information. Currently, PRC laws dealing with data protection are piecemeal and provide little concrete guidance. But there are early signs that this may be changing in ways that may create unexpected challenges and consequences going forward.

Effective March 15, 2015, China's State Administration for Industry and Commerce (SAIC) implemented new "Measures for Penalties for Infringing upon the Rights and Interests of Consumers," outlined below. In addition, China's legislature, the National People's Congress, has completed two of three required readings of a draft anti-terrorism law which would require ICSPs to implement "back doors" to aid Chinese counter-terror investigators, to surrender encryption keys upon request, and to house all domestic information on servers in China, pursuant to comprehensive data residency requirements. This proposed legislation, discussed in detail below, has caused an international stir, prompting U.S. President Barack Obama to state in early March 2015, that "this is something they are going to have to change if they are to do business with the United States."[120]

120. Chen Qin, *China Anti-Terror Law Worries Foreign Tech Firms*, MARKETWATCH.COM (Apr. 2, 2015), http://www.marketwatch.com/story/china-anti-terror-law-worries-foreign-tech-firms-2015-04-02.

Data Protection and Privacy in PRC

The PRC's legal foundation for data protection is loosely framed by the Chinese constitution, which refers indirectly to privacy, seeming to guarantee privacy rights in the home and for correspondence.[121] The Criminal Law Code imposes up to a year in prison on those who violate citizens' "rights of" communication freedom and up to three years on those who illegally search a residence.[122] The General Principles of Civil Law prohibits insults, libel, and damage to reputation, under a general tort liability analysis.[123] And the Law on the Protection of Minors prohibits collecting "personal secrets" of minors.[124]

China has no national data protection authority, and although a draft Personal Data Protection Law has been under consideration for several years, its prognosis and timing remain quite uncertain. Currently, the PRC does not administer or maintain any register of data controllers, personal data processing or transfer activities, or location of databases in the PRC that contain general personal information of PRC citizens. Nor is there any requirement for companies to appoint a data protection officer. There is also no mandatory requirement for reporting of data breaches or losses to authorities or to individuals

121. Constitution of the People's Republic of China, XIANFA arts. 37-40 (1982).

122. Criminal Law of the People's Republic of China (adopted by the Fifth Nat'l People's Cong., July 1, 1979, amended by the Eighth Nat'l People's Cong. on Mar. 14, 1997) arts. 252 and 245, respectively [hereinafter Criminal Law of the People's Republic of China].

123. General Principles of the People's Republic of China Civil Law (adopted by the Sixth Nat'l People's Cong., Apr. 12, 1986, promulgated by the President of the People's Republic of China, Apr. 12, 1986) art. 10.

124. Law of the People's Republic of China on Protection of Minors (adopted by the Standing Comm. of the Seventh Nat'l People's Cong., Sept. 4, 1991, promulgated by the President of the People's Republic of China, Sept. 4, 1991).

whose personal information is impacted. Nor are there any specifically articulated enforcement provisions or penalties for noncompliance with PRC law relating to data protection.

Components of Current PRC Data Protection Landscape

The PRC's current data protection landscape relies on the interplay of several components: (1) the Decision of the Standing Committee of the National People's Congress (NPC) on Strengthening Online Information Protection ("Decision"), taken December 28, 2012; (2) draft Guidelines published on November 5, 2012, by the Ministry of Information and Industry in China (MIIT), called "Information Security Technology—Guide for Personal Information Protection" ("Guidelines"); and (3) the new "Measures for Penalties for Infringing upon the Rights and Interests of Consumers" ("Measures") implemented on March 15, 2015, by the State Administration for Industry and Commerce (SAIC).

The Decision has the full force and effect of law. In contrast, the Guidelines are general principles that, while not mandatory, are generally considered to foreshadow the direction of PRC data protection law. The Measures clarify obligations with respect to corporate handling of personal data, define what constitutes personal consumer information, and demonstrate China's increased focus on data protection. The Measures effectively repeal the previous "Measures for Penalties Against Conduct Defrauding Consumers," which were adopted by the SAIC in 1996.

The PRC "Decision"

The Decision refers to "personal information," which is defined as any electronic information which can be used to identify a citizen; it relates generally to data privacy in the sense of

personal reputation. Unlike the EU Data Protection Directive, the Decision has no separate definition or treatment of personal sensitive data.

Under the Decision, in order for network service providers and others to collect and use the personal information of citizens, the following prerequisites apply: (1) it must be lawful, reasonable (i.e., proportional), and necessary; (2) it must specify the purpose, method, and scope regarding the collection and use of the personal information; (3) the personal information subject must consent; (4) it must be collected and used in a manner consistent with other laws, regulations, and mutual agreements; and (5) it must disclose the rules regarding collection and use.

The Decision has no specific requirements relating to the transfer of personal information, but it does require the data controller to ensure that the personal information is kept "safe" in transit, and that the recipient has the capability to properly process and protect the information from a data security perspective.

Failure to comply with the Decision is considered an "offense" under Articles 9 and 11, with considerable discretion left to authorities as to the nature and scope of enforcement. However, unlike in the U.S., experience suggests that the lack of specific advance notice of consequences will not provide any defense against enforcement of the Decision by the PRC.

In terms of electronic behavioral marketing, organizations are also prohibited from acquiring personal information by deceptive or illegal means, and from selling or unlawfully providing such information to third parties. Network service providers (fixed line or mobile telephone, Internet) must require consumers to provide verified information relating to their identity as a condition of service. The Decision also prohibits an-

yone from sending commercial electronic information or solicitations (spam) to a telephone or email address without the prior consent of the recipient.

Lastly, under Article 5 of the Decision, network service providers have an affirmative duty to report any suspected transmission of any false or unlawful information and take necessary measures to remove such information. Individuals have the right to require network service providers to delete such information and to take corrective action to prevent further occurrences.

The PRC "Guidelines"

Under the Guidelines, any data or information that can be used separately, or in conjunction with other data, to identify an individual is "personal data." Such data can only be collected and processed when: (1) laws and regulations specifically authorize such collection and processing, or if the data subject consents; and (2) the data controller has a specific, clear, and reasonable purpose for doing so.

Before personal data can be collected and processed, the Draft Guidelines state that the data controller "should" notify the data subject of the following: (1) the purpose, scope, use, and collection methods relating to the data; (2) the name, address, and contact information for the data controller; (3) the consequences of not providing the personal data; (4) the rights of the data subject; and (5) procedures and process for submitting complaints.

Under the Guidelines, data controllers are prohibited from collecting personal data that is not related to the stated purpose, particularly if the data relates to race, religion, DNA, fingerprints, physical condition, or sex life. This is very similar to the EU Data Protection Directive's treatment of "sensitive personal data."

The data controller may only *process* personal data for the purpose and within the scope of notification to the data subject. Measures must be taken to maintain the confidentiality and privacy of such data during transmission, processing, and storage.

Data controllers may not transfer personal data to third parties unless the data controller: (1) explains to the data subject, the purpose and scope of the data transfer; (2) obtains the explicit consent of the data subject to such transfer; and (3) ensures that the recipient can process, store, and transfer the personal data in a safe and secure manner.

Data controllers are required by the Draft Guidelines to take appropriate technical and organizational measures against unauthorized or unlawful processing and to protect against accidental loss, destruction, or alteration of such data. The standard of care is that the measures taken must ensure a level of security proportional to the nature of the data and to the harm that may result from its unauthorized or unlawful processing, loss, breach, destruction, or alteration.

The PRC "Measures" (including Personal Data Marketers and Data Brokers)

As noted above, the new SAIC Measures for Penalties for Infringing upon the Rights and Interests of Consumers ("Measures"), effective March 15, 2015, sets corporate obligations for handling of personal data and, for the first time, defines "personal consumer information."

The Measures were promulgated for three stated reasons: (1) "to prevent infringement upon consumer rights and interests in accordance with law," (2) "to protect the lawful rights and interests of consumers," and (3) "to maintain the socialist economic order."

Article 11 of the Measures compels businesses that collect or use personal information of consumers to "follow the principles of legality, appropriateness, and necessity" and to "clearly state the purpose, manner and scope for collecting and using the information." The Measures prohibit businesses from collecting and using personal consumer information without consent; leaking, selling, or illegally providing it to third parties; and sending commercial information to a consumer without the consent or request of the consumer.

Article 11 defines "personal information of consumers" as:

> a consumer's name, gender, occupation, date of birth, identification document number, residential address, contact information, status of income and assets, health status, consumption habits, and other information collected by businesses during their provision of goods and services that may independently or in combination with other information identify the consumers.

The Measures amplify the previous Law of the People's Republic of China on the Protection of the Rights and Interests of Consumers issued by SAIC in 2014, which did not define the scope of "personal consumer information." Businesses that violate Article 11 of the Measures are subject to penalties including civil liabilities, administrative correction or warnings, confiscation of unlawful gains, monetary fines up to ten times the illegal income or up to RMB 500,000 ($80,000 U.S. dollars) per violation, suspension of business, and revocation of business licenses. In addition, the violations and penalties are memorialized in the credit files of the business and disclosed to the public.

China's Proposed "Anti-Terror" Law

The proposed China "Anti-Terror" law has touched a nerve globally, because it is feared that it will grant the PRC unfettered access to the most competitively sensitive data of companies that wish to do business in China, as well as require construction and staffing of data centers in China, under the proposed law's data residency or localization requirements. Like similar laws in Brazil, Russia, and elsewhere, this is seen, in part, as a response to the 2013 Snowden revelations and the May 2014 indictment of five Chinese military officers by the U.S. Department of Justice on charges of hacking U.S. companies.

Unfettered PRC Access to Information within its Borders

Under the proposed PRC legislation, China could access and examine any private data transmitted through its domestic Internet, without prior notice or court order, so long as a terrorist threat was deemed to exist. In contrast, at least by law, the U.S. and a number of other governments engage in fairly unrestricted surveillance of international data flows, but can only "obtain" private domestic data after a formal subpoena or warrant process. To this end, the proposed PRC law requires ICSPs to install government-accessible back doors and provide encryption keys to public security authorities for any data stored on their servers.

Data Residency Requirement in PRC

The proposed law also requires ICSPs to locate their servers physically in China and store all PRC user data in China, thereby giving the government access to a wealth of private data and competitively sensitive business documents, including those stored on a PRC-based cloud server, as well as access to personal and business email, chat logs, texts, and the like. The

law does not require a showing of any threat to national security, nor notice to companies, and companies would have no avenue of appeal. Chinese officials have defended the draft, stating that the law would only be used following a "strict approval process"; however, the current draft contains no reference to such a process, and other PRC laws and regulations that permit government requests for similar data do not typically set out the internal approval process for such requests. Other governments worldwide recognize a legitimate need to access privately stored communications under certain circumstances, but these laws generally require a specific prior request to the company and judicial oversight process.

Following a forceful reaction by President Obama, U.S. trade officials and trade groups, China has deferred the third and final reading of this draft law for the time being. However, China's Foreign Ministry has said that "deliberation on this law is ongoing," raising concern that such legislation in 2015 or 2016 may be imminent.

The proposed law has been roundly criticized as a radical departure from international norms and a heavy blow against individual rights. Another critique is that it could cause irrevocable harm to China's own information technology industry because of the threat of surreptitious invasion of data.

Proposed Anti-Terror Legislation Technology Requirements in PRC

Articles 15 and 16 of China's proposed "Anti-Terror" law would require the following specific technical measures, under penalty of law:

- **Adding "Back doors" to telecommunications and Internet data that are available to PRC authorities.** Article 15 requires "network and in-

formation services operators" to install "technical interfaces in the design, construction, and operation of telecommunication and Internet [services]," which would act as "back doors" to purportedly "prevent" or "investigate" terrorist activities. The law does not require any notice when using these "back doors" and does not require the government to demonstrate any connection between the data sought and the suspected terrorism.

- **Making encryption keys available to PRC authorities.** Article 16 requires ICSPs to file their encryption scheme with the government and to provide encryption keys, upon request.
- **Storing all telecommunications and Internet data locally on servers placed in China.** Article 15 requires any business "providing telecommunications or Internet service within the borders of the PRC to locate its related servers and domestic user data within the borders of [China]." This measure tracks a similar one slated to take effect on September 1, 2015, in Russia, and is designed to ensure that the PRC has full access to all information transmitted within its borders and enforce virtual jurisdiction on all companies doing business in China. It effectively hardens the "Great Firewall of China," and is consistent with the "cyber-sovereignty" principle that nation states have the right to control all information within their boundaries.
- **Affirmatively monitoring and reporting regarding "terrorist" Internet content.** Under the

proposed law, ICSP's would need to add "terrorist content" (to be defined by the PRC on an *ad hoc* basis) to the list of other forms of prohibited content, and to affirmatively report the details of such content to the government.

- **Hardening the "Great Firewall" of China.** Responsible departments are empowered by the draft legislation to "adopt technical measures to stop the dissemination of information with terrorist content available on the international Internet."

Cross-Border Discovery in PRC

The concept of U.S.-style discovery is certainly alien to China. Chinese legal proceedings are much like those of other civil law jurisdictions. With few exceptions, parties are restricted to information within their possession to support their claims and defenses, unaided by the kind of liberal U.S. discovery and disclosure rules aimed at creating a more level "playing field."

China is a signatory to the Hague Convention on Taking of Evidence,[125] but has made reservation under Article 23 to exclude production of "pre-trial discovery of documents," and instead only allows discovery and production of documents relevant for the purpose of trial.[126] Typically, a U.S. court must submit a Letter of Request to the PRC Ministry of Justice. The

125. Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, *opened for signature* Mar. 18, 1970, 23 U.S.T. 2555, 847 U.N.T.S. 241.

126. "A Contracting State may at the time of signature, ratification or accession, declare that it will not execute Letters of Request for the purpose of obtaining pre-trial discovery of documents, as known in Common Law countries." *Id*. art. 23.

letter is forwarded to the PRC Supreme Court for review, which may take six to twelve months. The PRC Supreme Court will limit the scope of the request, or reject it altogether, if it violates PRC state sovereignty, would disclose state or commercial trade secrets, or create any risk to national security.

Several U.S. cases highlight the uncertainty faced in trying to conduct discovery involving PRC businesses. In *Tiffany v. Andrew*,[127] the plaintiffs brought a trademark infringement action against PRC defendants in the Southern District of New York and requested bank records located in China. The PRC-based defendants objected to the discovery requests on the basis that it was prohibited by PRC law, and that the Hague Convention was the primary mechanism for seeking such information. The Court agreed, applying the Restatement (Third) of Foreign Relations test adopted by the U.S. Supreme Court in *Aerospatiale*.[128] The Court relied upon an offer of evidence that the PRC has recently been shown more willing to execute Letters of Request, and because it ruled the PRC interest in protecting confidential bank records in China, as well as harsh penalties for violation of PRC bank secrecy laws, outweighed the U.S. interest in enforcing intellectual property rights.[129]

State Secrecy in PRC

In China, the Law on Guarding State Secrets prohibits a company or individual from disclosing information considered to be a state secret. PRC authorities take an expansive view of the scope of state secrets, which even includes a company's in-

127. Tiffany (N.J.) v. Andrew, 267 F.R.D. 143 (S.D.N.Y. 2011).

128. Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for the S. Dist. of Iowa, 482 U.S. 522, 544 (1987).

129. *See* Appendix for citations for selected cases that address the intersection of data protection and cross-border discovery.

ternal policies, procedures, and processes. State Owned Enterprises (SOE) and parties involved in industries such as telecommunications, banking, information technology, energy, national defense, agriculture, infrastructure, transportation, manufacturing, technology, and national resources have all been classified as possessing state secrets. The PRC Constitution requires all Chinese citizens to comply with state secrecy protection laws.[130] The Law on Guarding State Secrets ("State Secrets Law") is aimed at protecting matters of important state interest, as noted above, because of the potential damage disclosure could cause to China and, therefore, to its national security. Based upon a judgment regarding the extent of harm that might result from accidental or intentional disclosure, it separates secret information into three classifications: most confidential, classified, and confidential.[131] A violation of the State Secrets Law, whether negligent or intentional, carries a penalty of up to seven years in prison under PRC Criminal Law.[132] The PRC State Secrets Law provides the following diverse examples:

- Major national policy decisions
- Matters of national defense and armed forces activities
- Diplomatic activities, foreign affairs, and obligations to foreign nations to maintain secrets
- Secrets in economic and social development
- Secrets in science and technology

130. Constitution of the People's Republic of China, XIANFA art. 53 (1982).

131. Law of the People's Republic of China on Guarding State Secrets (adopted by the Standing Comm. of the Seventh Nat'l People's Cong. and promulgated by the President of the People's Republic of China, Sept. 5, 1988, effective May 1, 1989) art. 9.

132. Criminal Law of the People's Republic of China, *supra* note 122, art. 398.

- Secrets in activities to safeguard national security and to investigate criminal offenses
- Other matters determined to be state secret by the State Secret Administration, including a political party's secrets that conform to this Article[133]

In addition to State Secrets, China also regulates the disclosure of "business" or "commercial" secrets under its Anti-Unfair Competition Law, which encompasses any technical or business information, including management and business models, that (1) is unknown to the general public, (2) may create business interests or profit for its owners, and (3) is maintained secret by its legal owners.[134]

The definition of a "business secret" was expanded in 2010, when the State-Owned Assets Supervision and Administration Commission (SASAC), by regulation, expanded its scope to include a substantial number of SOEs.

Penalties include potential civil liability for damages as well as criminal penalties, depending on the seriousness of monetary loss, from three to seven years in prison.[135]

The proposed "Anti-Terror" law would essentially squeeze out all but those cloud providers with infrastructure located in China. Requiring a China-specific private cloud would effectively eliminate many of the usual price-saving opportunities afforded by global cloud providers. Of course, China is a

133. *Id.* art. 8.

134. Anti-Unfair Competition Law of the People's Republic of China (adopted by the Standing Comm. of the Eighth Nat'l People's Cong., Sept. 2, 1993) art. 10.

135. Criminal Law of the People's Republic of China, *supra* note 122, art. 219.

large market, and competition for this service would undoubtedly be keen; however, it would come at a heavy price risk of unfettered governmental surveillance and seizure.

CONCLUSION

The future of data protection in the Asia-Pacific region remains dynamic, with various countries adopting token attempts at solutions, such as enacting data residency laws, which are likely to be counterproductive in the long run. In contrast, others are embracing innovative initiatives such as the APEC Cross Border Privacy Rules Framework, which provides some hope for an ultimate global solution. The cooperation and collaboration between APEC and the EU Article 29 Working Party to harmonize the CBPR and BCR frameworks is encouraging, particularly in the wake of digital-protectionist responses following the Snowden NSA surveillance revelations. Certainly, it will take time to rebuild trust which has been lost. This trust is an absolute prerequisite to constructive dialogue. Without it, the tide of digital protectionism and isolationism is likely to rise. With it, there is hope that together we can find a reasoned way forward to balance data protection interests with the free flow of information and ideas so essential to economic and cultural growth.

APPENDIX

This Appendix provides citations for selected cases that address the intersection of data protection and cross-border discovery. In particular, these cases provide analysis of *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for the S.D. of Iowa*, 482 U.S. 522 (1987), and The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, 23 U.S.T. 2555, reprinted in the notes section following 28 U.S.C. § 1781.

2015

- *St. Jude Med. S.C., Inc. v. Janssen-Counotte*, 2015 U.S. Dist. LEXIS 64355, 2015 WL 2359568 (D. Or. May 18, 2015).
- *Peters v. Peters*, 127 A.D.3d 656 (N.Y. App. Div. 2015).

2014

- *Gilmore v. Palestinian Interim Self-Government Auth.*, 8 F. Supp. 3d 1 (D.D.C. 2014).
- *In re Activision Blizzard, Inc. Stockholder Litig.*, 86 A.3d 531 (Del. Ch. 2014).
- *Republic of Arg. v. NML Capital, Ltd.*, 134 S. Ct. 2250 (2014).
- *BrightEdge Techs., Inc. v. Searchmetrics, GmbH*, 2014 U.S. Dist. LEXIS 112377, 2014 WL 3965062 (N.D. Cal. Aug. 13, 2014).
- *Sebastian Holdings, Inc. v. Deutsche Bank AG*, 123 A.D.3d 437 (N.Y. App. Div. 2014).
- *Tansey v. Cochlear Ltd.*, 2014 U.S. Dist. LEXIS 132021, 2014 WL 4676588 (E.D.N.Y. Sept. 18, 2014).

2013

- *Linde v. Arab Bank*, PLC, 706 F.3d 92 (2d Cir. 2013).
- *Pershing Pac. West, LLC v. MarineMax, Inc.*, 2013 U.S. Dist. LEXIS 33473, 2013 WL 941617 (S.D. Cal. Mar. 11, 2013).

2012

- *Lantheus Med. Imaging, Inc. v. Zurich Am. Ins. Co.*, 841 F. Supp. 2d 769 (S.D.N.Y. 2012).
- *Trueposition, Inc. v. LM Ericsson Tel. Co.* (Telefonaktiebolaget LM Ericsson), 2012 U.S. Dist. LEXIS 29294, 2012 WL 707012 (E.D. Pa. Mar. 6, 2012).
- *Wultz v. Bank of China Ltd.*, 910 F. Supp. 2d 548 (S.D.N.Y. 2012).
- *Ayyash v Koleilat*, 957 N.Y.S.2d 574 (N.Y. Sup. Ct. 2012).

2011

- *SEC v. Stanford Int'l Bank*, Ltd., 776 F. Supp. 2d 323 (N.D. Tex. 2011).
- *Costa v. Kerzner Int'l Resorts, Inc.*, 277 F.R.D. 468 (S.D. Fla. 2011).
- *Recaro N. Am., Inc. v. Holmbergs Childsafety Co.*, 2011 U.S. Dist. LEXIS 134978, 2011 WL 5864727 (E.D. Mich. Nov. 22 2011).
- *Metso Minerals Indus. v. Johnson Crushers Int'l, Inc.*, 276 F.R.D. 504 (E.D. Wis. 2011).
- *Estate of Esther Klieman v. Palestinian Auth.*, 272 F.R.D. 253 (D.D.C. 2011).

2010

- *Milliken & Co. v. Bank of China*, 758 F. Supp. 2d 238 (S.D.N.Y. 2010).
- *In re Urethane Antitrust Litig.*, 267 F.R.D. 361 (D. Kan. 2010).

2009

- *Affordable HealthCare, LLC v. Protus IP Solutions, Inc.*, 2009 U.S. Dist. LEXIS 30461, 2009 WL 975150 (E.D. Mo. Apr. 9, 2009).
- *Schindler Elevator Corp. v. Otis Elevator Co.*, 657 F. Supp. 2d 525 (D.N.J. 2009).
- *In re Global Power Equip. Group Inc.*, 418 B.R. 833 (Bankr. D. Del. 2009).

2008

- *Strauss v. Credit Lyonnais*, S.A., 249 F.R.D. 429 (E.D.N.Y. 2008).
- *Emerson Elec. Co. v. Le Carbone Lorraine, S.A.*, 2008 U.S. Dist. LEXIS 72705, 2008 WL 4126602 (D.N.J. Aug. 27, 2008).
- *Seoul Semiconductor Co. v. Nichia Corp.*, 590 F. Supp. 2d 832 (E.D. Tex. 2008).

Pre-2008

- *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.*, 2005 U.S. Dist. LEXIS 20049, 2005 WL 6246195 (N.D. Ill. Sept. 12, 2005).
- *Mujica v. Occidental Petroleum Corp.*, 381 F. Supp. 2d 1134 (C.D. Cal. 2005).
- *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for the S.D. of Iowa*, 482 U.S. 522 (1987).