International Lawyer

Volume 49
Number 0 *Year in Review*

Article 8

2015

Privacy, E-Commerce, and Data Security

W. Gregory Voss

Katherine H. Woodcock

Cecil Saehoon Chung

Kyoung Yeon Kim

Jai Lee

See next page for additional authors

Privacy, E-Commerce, and Data Security

Authors

W. Gregory Voss, Katherine H. Woodcock, Cecil Saehoon Chung, Kyoung Yeon Kim, Jai Lee, and Doil Son

THE YEAR IN REVIEW
AN ANNUAL PUBLICATION OF THE ABA/SECTION OF INTERNATIONAL LAW

Privacy, E-Commerce, and Data Security

W. Gregory Voss, Katherine H. Woodcock, Cecil Saehoon Chung, Kyoung Yeon Kim, Jai Lee And Doil Son*

This article reviews select important legal developments during 2014 in the fields of privacy, e-commerce, and data security.[1] Attention in this year's contribution is focused exclusively on major developments in the European Union and in the Asia-Pacific region.

I. Developments in the European Union

2014 was an important year for privacy, e-commerce and data security developments in Europe, which included legislative action, important court decisions, and advisory guidance.

A. Legislative Action

The European Parliament was very active on privacy, e-commerce and data security issues prior to its May 2014 elections; however the Council of the European Union (Council) lagged behind.

* The committee editor was W. Gregory Voss, Toulouse University, Toulouse Business School, Member of the IRDEIC Research Institute, Toulouse, France. The authors were: Europe section: European Union: Legislative Action, and Court Decisions and Related Advisory Guidance: W. Gregory Voss; EU Article 29 Data Protection Working Party (WP) Guidance: Katherine H. Woodcock, Associate General Counsel, Privacy & Security, Nike; Asia-Pacific section: APEC Cross-Border Privacy, and Australia: W. Gregory Voss; China: Mr. Cecil Saehoon Chung, Vice-Chair of the Antitrust Practice Group and Head of International Antitrust at the law firm of Yulchon LLC in Seoul, Korea; Ms. Kyoung Yeon Kim, Partner in the Antitrust Practice Group at Yulchon LLC; and South Korea: Mr. Jai Lee, Senior Foreign Counsel and U.S. patent attorney specialized in technology laws at Yulchon, LLC, Mr. Doil Son, Partner and Korean licensed attorney practicing primarily in Mergers & Acquisitions, Technology, Media & Telecommunications (TMT), and Cyber Security, Yulchon LLC. The committee editor and the China section authors wish to thank Mr. Kyu Hyun Kim, Senior Associate at Yulchon LLC, Mr. Tae Yong Kim, foreign counsel at Yulchon, and Yankun Guo, a third-year student at the John Marshall Law School in Chicago, IL, U.S.A., for their assistance. The committee editor and the South Korea section authors would like to thank Youyoung Kim, Washington University School of Law in St. Louis, MO, U.S.A., J.D. Candidate 2015, for citation and editing assistance.

1. For earlier developments in this field, *see* W. Gregory Voss, et al., *Privacy, E-Commerce, and Data Security*, 48 ABA/SIL YIR 103 (2014).

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW

1. *General Data Protection Regulation*

The European Parliament voted overwhelmingly on first reading in plenary session (621 votes for, 10 against, and 22 abstentions) on March 12, 2014, for a version of the proposed EU General Data Protection Regulation (GDPR).[2] Agreement between the European Parliament and the Council on the text of the GDPR in two successive readings is required for it to become binding and directly applicable in Member States.[3] The GDPR was debated at the October 10, 2014 meeting of the Justice and Home Affairs ministers of the Council, but various issues still remain to be decided.[4]

2. *Network & Information Security Directive*

One day after its GDPR vote, the European Parliament voted favorably on the Network & Information Security (NIS) Directive in the first reading by a large margin–521 in favor, 22 against, and 25 abstentions.[5] The NIS Directive, if and when finally approved through the ordinary legislative procedure with the Council, would impose cyber security obligations on public administrations and market operators, essentially with respect to "critical infrastructure essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, financial market infrastructures or health".[6] In this context, Computer Emergency Response Teams would be set up in Member States.[7] At writing, the NIS Directive is still awaiting a Council first reading position.[8]

3. *Connected Continent Regulation*

On April 3, 2014, the European Parliament adopted in first reading (by 534 votes to 25, with 58 abstentions) a legislative resolution amending the proposal of the European Com-

2. *See* Press Release, Eur. Comm'n, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote, MEMO/14/186, (Mar. 12, 2014), *available at* http://europa.eu/rapid/press-release_MEMO-14-186_en.htm; *see also Text Adopted by Parliament, 1st Reading/Single Reading*, PARL. EUR. DOC. 2012/0011(COD), *available at* http://www.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1342337&l=en&t=D. For a discussion of the GDPR when it was initially proposed in 2012, *see* W. Gregory Voss et al., *Privacy, E-Commerce, and Data Security*, 47 ABA/SIL YIR 99, 102–04 (2013).

3. *See* Consolidated Version of the Treaty on the Functioning of the European Union, art. 294, at 173-75, Oct. 26, 2012, 2012 O.J. (C 326) 55, *available* at http://www.ecb.europa.eu/ecb/legal/pdf/c_32620121026en.pdf (for details of the ordinary legislative procedure (formerly known as the co-decision procedure), which is the procedure that applies to the adoption of the GDPR).

4. *See* Debate in Council, PARL. EUR. DOC. 2012/ 0011(COD), Oct. 10, 2014, *available at* http://www.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1361735&l=en&t=E.

5. Press Release, Eur. Comm'n, *Great New for Cyber Security in the EU: The EP Successfully Votes Through the Network & Information Security (NIS) Directive* (Mar. 13, 2014), *available at* http://europa.eu/rapid/press-release_STATEMENT-14-68_en.htm. *See also*, *European Parliament Legislative Resolution on the Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union*, COM (2013) 0048 (Mar. 13, 2014) [hereinafter NIS Directive], *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0244.

6. NIS Directive, *supra* note 5.

7. *See* Text Adopted by Parliament, 1st Reading/Single Reading (Mar. 13, 2014), 2013/0027(COD), *available at* http://www.europarl.europa.eu/oeil/popups/summary.do?id=1342725&t=e&l=en.

8. *See High Common Level of Network and Information Security Across the Union*, EUR. PARL., http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2013/0027(COD)&l=en (last visited Nov. 30, 2014).

mission (Commission) "for a regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent" (Connected Continent Regulation).[9] On June 5, 2014 the Council debated the proposed Connected Continent Regulation, many issues were raised about it, and several remain unresolved.[10] If finally adopted in the form approved by the European Parliament, the Connected Continent Regulation will end certain roaming charges in December 2015, apply the net neutrality principle, and allow internet access providers to provide specialized services to users, among other provisions.[11]

4. *Consumer Rights in the Digital Single Market Resolution*

On November 27, 2014, the European Parliament voted a non-binding resolution on supporting consumer rights in the digital single market. Such resolution called for, *inter alia*, "the swift adoption of the new modernised Data Protection Package", which includes the GDPR, called for the Council to move swiftly on the Connected Continent Regulation proposal, supported measures promoting net neutrality, and called upon the Commission "to consider proposals aimed at unbundling search engines from other commercial services", as one way to achieve competition policy goals.[12] The press saw the latter point as being aimed at "American technology giant Google,"[13] which also was subject to judicial action in Europe in 2014.

B. Court Decisions and Related Advisory Guidance

The Court of Justice of the European Union ("ECJ") handed down two important decisions discussed below: one invalidating the Data Retention Directive, and the other providing for de-listing of web sites in the *Google Spain* case. With respect to the latter, an EU advisory group later provided related guidance.

1. *Google Spain Case*

The ECJ rendered its decision in the *Google Spain* proceeding on May 13, 2014.[14] The case involved the request for a ruling by a Spanish court on points related to a lawsuit

9. *See*, *European Single Marker for Electronic Communication*, Eur. Parl. (Apr. 3, 2014), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0281.

10. *See* Debate in Council (June 5, 2014), 2013/0309(COD), *available at* http://www.europarl.europa.eu/oeil/popups/printsummary.pdf?id=1350214&l=en&t=E. *See also*, Council of the European Union, Progress Report (May 26, 2014), 10109/14, 20132013/0309(COD), *available at* http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010109%202014%20INIT.

11. *See* Texs Adoped by Parliament 1st Reading/Single Reading (Apr. 03, 2014), 2013/0309(COD), *available at* http://www.europarl.europa.eu/oeil/popups/summary.do?id=1345346&t=d&l=en.

12. Resolution on Supporting Consumer Rights in the Digital Single Market, Eur. Parl. (Nov. 27, 2014), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2014-0071&language=EN&ring=B8-2014-0286.

13. *See*, *e.g.*, James Kanter, *E.U. Parliament Passes Measure to Break Up Google in Symbolic Vote*, N.Y. Times (Nov. 27, 2014), http://nyti.ms/1rqGJci.

14. Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González , EUR-Lex (May 13, 2014), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEX:62012CJ0131&rid=14.

brought by Mr. Costeja González, against Google Spain SL and Google Inc. seeking to have them withdraw personal data concerning him from their index and preventing future access to such data through search engine links to certain pages from the web site of Catalan newspaper *La Vanguardia*. The ECJ found that the European 1995 Data Protection Directive applied to Google Inc., that search engines engage in data processing separate from that of the web sites they index, and that a right to object to such processing may lead to a case-by-case balancing of rights and interests analysis in the handling of data subject exercising of such right.[15]

As a result of the *Google Spain* decision, the search engine set up an online form for receiving requests for exercise of such right[16] and, as of November 25, 2014, Google reported having received 174,226 delisting requests, and having deleted 208,520 URL search engine result links, out of a total of 602,479 URLs examined following the requests.[17]

2. *Working Party Guidance on Implementation of Google Spain Decision*

On November 26, 2014, the EU Article 29 Data Protection Working Party (Working Party), an independent advisory body on data protection and privacy, made up of the EU Member State data protection agencies (DPAs), the European Data Protection Supervisor, and the Commission, issued guidelines on implementation of the *Google Spain* decision (WP 225).[18] WP 225, which "contains the list of common criteria which the DPAs will apply to handle the complaints, on a case-by-case basis, filed with the national offices following refusals of de-listing by search engines,"[19] is not aimed solely at Google. According to the Working Party, the *Google Spain* ruling "is specifically addressed to generalist search engines, but that does not mean that it cannot be applied to other intermediaries," and that data subjects may exercise their rights "with the national subsidiaries of search engines in their respective Member States of residence."[20] WP 225 clears up a point previously unresolved – *Google Spain* applies not only to EU Member State national domain names (or country code top-level domains–"ccTLDs"), as "de-listing should also be effective on all relevant domains, including .com"[21] (thus extending to generic top-level domains or "gTLDs", as well). The right "only affects the results obtained on searches made by the name of the individual", although this applies to possible different versions of the name, different spellings, family names,[22] and pseudonyms and nicknames as well, where these latter two can be linked to the real identity of the data

15. *See* W. Gregory Voss, *The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment in the Proposed General Data Protection Regulation*, 18(1) J. INTERNET L 3 (2014).

16. *See Search Removal Request Under Data Protection Law in Europe*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch (last visited on Nov. 30, 2014).

17. *See* European Privacy Request for Search Removals, GOOGLE, https://www.google.com/transparencyreport/removals/europeprivacy/ (last visited on Nov. 30, 2014).

18. *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección des Datos (AEPD) and Mario Costeja González" C-131/12*, ART. 29 DATA PROT. WORKING PARTY, WP 225, Nov. 26, 2014, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

19. *Id.* at 5.

20. *Id.* at 8.

21. *Id.* at 3.

22. *Id.* at 9.

subject.[23] Notices about de-listing should not be provided in a way that allows users to conclude that an individual has asked for de-listing, so general and consistent statements should be used and, finally, webmasters should generally not be informed that their pages have been de-listed, and search engines are encouraged to publish their specific de-listing criteria.[24]

3. *Invalidation of Data Retention Directive*

The ECJ also rendered a decision on April 8, 2014,[25] declaring invalid Directive 2006/24/EC[26] regarding data retention by, *inter alia*, telecommunications operators and internet service providers for purposes such as the fight against terrorism and organized crime, on the basis of the protection of fundamental rights.[27]

C. Overview of Guidance from the EU Article 29 Data Protection Working Party (WP)

The Working Party was extremely active in 2014. Learning lessons from the past and looking to create standard guidance throughout the EU, it issued guidance on new technologies in relatively quick succession. Summarized below are a few of the Working Party's opinions and activities from 2014.

1. *BCRs and CBPRs*

Due to the questionable future of the U.S.-EU Safe Harbor (which allows cross-border data transfers) and increasing restrictions on data location, interoperability and alternative means for cross-border transfers were the objects of companies' and governments' attention. Early in 2014, the Working Party issued an opinion linking binding corporate rules (BCRs) to the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPRs) (Opinion 02/2014).[28] It aims to serve as an informal checklist-or referential-for

23. *Id.* at 13.

24. *Id.* at 9–10.

25. Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd (C-293/12) v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others, EUR-Lex (Apr. 8, 2014), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&qid=1402263080147&from=EN.

26. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54 (Apr. 13, 2006).

27. *See* W. Gregory Voss, *European Union Data Privacy Law Developments*, 70(1) Bus. Law. 253, 257-259 (2014/2015).

28. *See, Opinion 02/2014 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, Art. 29 Data Prot. Working Party, Feb. 27, 2014, [hereinafter Opinion 02/2014], *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf. The referential was also issued by APEC, *see Joint Work between Experts from the Article 29 Working Party and from APEC Economies*, APEC, http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf (last visited Mar. 31, 2015).

companies looking to bridge the gap between the EU and APEC cross-border privacy frameworks. This paves the way for Opinion 02/2014 to serve as a basis for organizations seeking double certification; meaning that companies could use the referential when drafting their internal privacy rules for both frameworks.[29] Presented as a practical comparative tool outlining the different requirements of both the EU and APEC rules, it lists the common elements or blocks for both frameworks, followed by the additional elements where the frameworks deviate.[30] However, Opinion 02/2014's aim is not to have mutual recognition for both systems. The Working Party clearly indicates that both systems still require any privacy rules to be approved by EU DPAs, in line with EU law, and for the CBPRs, the certification by recognized accountability agents.[31] Nevertheless, Opinion 02/2014 marks a bridge between diverse approaches to data privacy and legal systems, looking towards interoperability solutions for global data transfers.

2. *Microsoft's Cloud Contracts*

Setting the tone for cloud providers, Microsoft worked together with the Working Party to have its cloud computing agreements for EU customers formally approved by DPAs.[32] This approval process was coordinated through the Working Party and announced in a joint letter on April 2, 2014.[33] The practical impact is that DPAs consider that Microsoft's data processing agreement for enterprise cloud services, including Azure and Office 365, is "in line with Standard Contractual Clause 2012/87/EU, and should therefore not be considered as 'ad hoc' clauses".[34] Thus, Microsoft's enterprise agreement qualifies as the controller to processor model contract and, as such, will require fewer approvals or prior authorizations of national DPAs for the transfer of data outside of the EU. It is anticipated moving forward that other cloud providers will seek similar approvals for their contracts in order to ensure a level playing field within the EU for cloud services.[35]

---

29. *Opinion 02/2014* , *supra* note 28, at 7.

30. *Id.* at 8; *see generally*, the twenty-seven referential points listed, *id.* at 11–58.

31. *Id.* at 7–8.

32. *See Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement (with EU Standard Contractual Clauses)*, MICROSOFT (May 2012), http://assets-production.govstore.service.gov.uk/Gii%20Attachments/06b%20Cats%20-%20uploaded/G2.179%20-%20Microsoft%20Ireland%20Operations%20Ltd/Archive1/(B116)EAEnrAmend(Office365DataProcessAgrWithModelClauses)(WW)(ENG)(May2012)(CR).pdf.

33. Letter from Isabelle Falque-Pierrotin, Chairwoman, Working Party, to Dorothee Belz, Associate General Counsel, Microsoft EMEA (Apr. 2, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf.

34. *Id.*

35. *See generally* Privacy Authorities Across Europe Approve Microsoft's Cloud Commitments, MICROSOFT (Apr. 10, 2014), http://blogs.microsoft.com/blog/2014/04/10/privacy-authorities-across-europe-approve-microsofts-cloud-commitments/. *See also* Letter from Isabelle Falque-Pierrotin, Chairwoman, Working Party, to Satya Nadella, CEO, Microsoft (Sept. 22, 2014) *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140922_letter_microsoft_service_agreement.pdf.

3. *Clarification on Use of Legitimate Interest Basis*

The Working Party issued guidance on the legal basis for processing personal data contained in Article 7(f) of Directive 95/46/EC, where processing may occur based on the legitimate interests of the data controller.[36] This Opinion 06/2014 looks not only to the application of Article 7(f) but takes the opportunity to provide an overview of all the legal bases under Article 7.[37] Opinion 06/2014 sets out the balancing test for weighing the legitimate interest of the data controller (or third parties) against the fundamental rights or interests of the data subject. The Working Party highlights that this is not the last possible basis for having processing deemed illegitimate. The balancing test is not to be considered straightforward, but instead requires the consideration of a number of factors, including the source and nature of the legitimate interests, whether processing is necessary for the exercise of a fundamental right (or is otherwise in the interests of the public), the actual impact on the data subject and their reasonable expectations about the data processing, as well as the nature of the data and how it will be processed. Finally, any additional safeguards limiting the impacts on the individuals should also be considered.[38]

Opinion 06/2014 includes a number of examples and quick guide on how to carry out the Article 7(f) balancing test.[39] This quick guide includes assessing which ground will be applicable under Article 7, whether an interest is legitimate or illegitimate, determining whether the process is necessary, establishing the balancing test (both in a provisional manner and a final determination), and demonstrating compliance and insurance transparency as well as ensuring the exercise of individual rights. The last two steps trigger practical consequences for controllers, as they will need to be able to demonstrate via documentation or mapping of their balancing test.[40]

4. *Other Opinions and Guidance*

Keeping abreast of new technological developments, the Working Party issued an opinion on the Internet of Things setting out guidance for three specific technologies: wearable devices, quantified-self and domotics.[41] The Working Party also issued statements on

36. *See Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC*, WP 217, Art. 29 Data Prot. Working Party, Apr. 9, 2014, [hereinafter Opinion 06/2014] *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Article 7(f) of the Directive provides that the processing of personal data is permitted when "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject". Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 23/11/EC, 1995 O.J. (L 281) 31, 41, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en.

37. *Id.* at 13; *see also*, *id.* at 16–23.

38. *Id.* at 3; *see also*, *id.* at 22–48.

39. *Id.* at 55–57.

40. *Id.* at 56.

41. *See Opinion 08/2014 on the Recent Developments on the Internet of Things*, WP 223, Art. 29 Data Prot. Working Party,Sept. 16, 2014, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

Big Data[42] and–relatedly-guidance on anonymization.[43] Its discussion on Big Data and the identifiability of data subjects (individuals) also sets the stage for the ongoing discussions around the data protection reforms within the EU.

II. Developments in Asia-Pacific Region

Significant developments also arose in APEC, Australia, China and South Korea in 2014.

A. APEC Cross-Border Privacy

In addition to the Working Party and APEC's referential, discussed in Part I. C. 1 above, APEC was busy working through its Cross-Border Privacy Rules System Joint Oversight Panel, which issued its Findings Report on April 25, 2014, in which it found that Japan met the conditions to become a Participant in the Cross-Border Privacy Rules System.[44] Thus, Japan joined the U.S. and Mexico in this regard, becoming the third participant.[45]

B. Australia

With respect to Australia, it should first be noted that the 2012 amendments to Australia's Privacy Act 1988[46] came into force on March 12, 2014.[47] Next, during the first half of 2014, the Australian House of Representatives' Social Policy and Legal Affairs Committee held hearings on drones and privacy,[48] and the Nationals Deputy Whip made a statement on behalf of such Committee, saying that "[a]lthough drones have the potential to add great value to the Australian economy, widespread use of drones also raises serious

42. Letter from Isabelle Falque-Pierrotin, Chairwoman, Working Party, to John Podesta, Counselor to the U.S. President, White House (June 11, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140611_letter_to_podesta.pdf. *See also Statement on Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with regard to the Processing of their Personal Data in the EU* [sic], WP 221, Art. 29 Data Prot. Working Party, Sept. 16, 2014, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf.

43. *See Opinion 05/2014 on Anonymisation Techniques*, WP 216, Art. 29 Data Prot. Working Party, Apr. 10, 2014, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. For a discussion of Opinion 05/2014 *see European Union Data Privacy Law Developments*, *supra* note 27, at 253-254.

44. Findings Reports, Cross-Border Privacy Rules System Joint Oversight Panel, APEC, *Cross-Border Privacy Rules System Participation of Japan* (Apr. 25, 2014), http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/20140430_CBPR_Japan_Final_Report.pdf.

45. Press Release, APEC, APEC Expands Data Privacy System to Protection Consumers (May 1, 2014), *available at* http://www.apec.org/Press/News-Releases/2014/0501_CBPR.aspx. For a discussion of the U.S.'s joining this System, *see Privacy, E-Commerce, and Data Security*, *supra* note 2, at 110.

46. For a discussion of these amendments, *see Privacy, E-Commerce, and Data Security supra* note 2, at 111–12.

47. *See Message from the Privacy Commissioner, Timothy Pilgrim*, Austl. Gov't, Office of the Austl. Info. Comm'r, Annual Report 2013-2014, *available at* http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201314/message-from-the-privacy-commissioner-timothy-pilgrim.

48. *See Public Hearings*, Parl. Of Austl., http://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Drones/Public_Hearings (last visisted Mar. 30, 2015).

privacy issues that will need to be resolved."[49] According to that same Committee, today's Australian laws do not protect citizens' privacy from drones, and following its hearings it tabled a report in Parliament calling on the Australian Government to "modernize and simplify Australia's privacy laws to protect against potentially invasive new technologies like drones."[50] That report contained, *inter alia*, the following recommendations: (i) that the Civil Aviation Safety Authority include privacy law information with a safety pamphlet that it provides to remotely piloted aircraft vendors, highlighting users' responsibility "not to monitor, record or disclose individuals' private activities without their consent" (recommendation 2);[51] (ii) that the Australian Government "consider introducing legislation by July 2015 which provides protection against privacy-invasive technologies" (recommendation 3);[52] and (iii) that the Australian Government start action to introduce harmonized surveillance laws covering "the use of:

- listening devices,
- optical surveillance devices,
- data surveillance devices, and
- tracking devices" (recommendation 4).[53]

Thus, future Australian legislation should be tracked in order to follow these developments.

C. China

In China, there were a number of developments in 2014. Two of them are particularly noteworthy. First, a major revision to the country's privacy law, as part of a broader overhaul of its consumer protection law, went into force. Second, two foreign private investigators for global corporations were sentenced to prison for illegally purchasing personal information.

1. *Protection of Personal Information as Part of Major Overhaul of Consumer Protection Law*

On October 25, 2013, China passed an amendment to the Law on the Protection of Consumer Rights and Interests,[54] representing a truly major overhaul of the country's consumer protection law that was first enacted in 1993. On March 15, 2014, the amended

49. Cth, Parliamentary Debates, House of Representatives, 17 Mar. 2014, 1983-1984 (Mr Christensen, Soc. Policy and Legal Aff. Comm.) (Austrl.), *available at* http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/19c32232-832c-45aa-8efa-783c9a3446a4/0016/hansard_frag.pdf;fileType=application%2Fpdf.

50. Press Release, H.R. Standing Comm. on Social Policy and Legal Issues (Austl.), Committee Calls for New Privacy Protections as Drone Use Surges (July 14, 2014), *available at* http://www.aph.gov.au/DocumentStore.ashx?id=06d9c0a8-81a3-4b27-986d-609cef3fc430.

51. Rep., H.R. Standing Comm. on Soc. Policy and Legal Issues (Austl.), Eyes in the Sky (July 14, 2014), ch. 4 at 47, http://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_vand_Legal_Affairs/Drones/Report.

52. *Id.* at 48.

53. *Id.*

54. Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Guanyu Xiugai «Zhonghua Renmin Gongheguo Xiaofei Zhe Quanyi Baohù Fa» de Jueding
全国人民代表大会常务委员会关于修改《中华人民共和国消费者权益保护法》的决定 [Amending the Law of the People's Republic of China on the Protection of Consumer Rights and Interests](promulgated by the

law became effective. Among other things, the amended law provides for: a shift of burden of proof to vendors regarding consumers' defective product or service claims; a seven-day refund requirement for Internet sales; protection of personal information collected during sales process; allowance of lawsuits or support by consumer interest groups; and strengthened punitive damages against sellers from twice the product price to three times.

Regarding the protection of personal information, in order to collect consumers' personal information, businesses must disclose the purpose, method, and scope of collection and intended use of personal information gathered during sales process, and obtain consent of consumers. Businesses must: (i) preserve the confidentiality of the collected personal information; (ii) not disclose personal information to third parties without the prior consent of consumers; (iii) not send commercial communications to consumers without their consent or request; (iv) honor consumers' request to opt out of receiving further communications; and (v) not use the personal information in any lawful fashion.[55] This is the first time China has explicitly recognized through legislative action that consumers' personal information is the consumers' protected right.[56] While other measures to protect consumers' privacy are industry-specific or communication-mode specific rules, this amendment covers consumers' privacy, data security and e-commerce rights in a much broader context.

2. *Foreign Nationals Imprisoned for Illegal Collection of Personal Information for Corporate Investigations*

In August 2014, a Shanghai court sentenced a British corporate investigator to thirty months in prison and his American wife investigator to twenty-four months, along with a combined fine of approximately $57,000 for illegally collecting personal information. The private investigators were corporate investigators who help global corporate clients uncover business partners' and employees' suspected corruption and other types of wrongdoing. More specifically, they purchased personal information about Chinese nationals as part of their investigative work. The most important type of personal information the investigator couple illegally purchased and possessed was Chinese citizens' national identification number (similar to the social security numbers in the U.S.).[57]

This is not the first time those who illegally purchased or misused personal information were criminally punished. But the nationality and occupation of the defendants may make this case a truly noteworthy and defining development. The defendants were foreign nationals and they were not mass marketers or spammers but corporate investigators who supposedly obtained and used personal information to help their corporate clients detect bribery and other illegal conduct.

Standing Comm. Nat'l People's Cong., October 25, 2013, effective Mar. 14, 2014) (Lawinfochina)(China), *available at* http://www.lawinfochina.com/display.aspx?lib=law&id=15517&CGid=.

55. *Id.* art. 29.

56. *China Amends Consumer Rights Law*, XINHUANNET (Oct. 25, 2013), http://news.xinhuanet.com/english/china/2013-10/25/c_132830969.htm.

57. *Brenda Goh & Engen Tham, China Sentences GSK-Linked Investigators to Prison*, REUTERS (Aug. 08, 2014), http://uk.reuters.com/article/2014/08/08/uk-china-gsk-trial-idUKKBN0G80F620140808.

3. *Other Developments*

Most other noteworthy developments relate to China's continuing efforts to strengthen the protection of personal information and data security through industry or communication mode-specific initiatives. For example, in October 2014, the Supreme People's Court issued interpretations on the protection of personal information on the Internet.[58]

Similarly, earlier in March 2014, China's State Postal Bureau issued three formal rules, which had been previously issued in draft form in late 2013 for public comments, concerning the protection of personal information in the context of postal delivery of traditional mail items.[59]

D. South Korea

Early in 2014, a major breach of personal information in South Korea was recorded by three credit card companies.[60] Through the incident, more than 100 million items of personal information were compromised, including credit card numbers, passwords, date of birth, residence registration numbers (similar to the social security number in the U.S.), addresses and others. More than 4.7 million people replaced or cancelled their credit cards.[61]

The problem related to the loss of personal information that could also be used for other purposes. For example, in Korea, the residence registration number was used by many entities for many purposes (e.g., banks, Internet games, Internet shopping, insurance, rental cars, customs office to deliver a package from overseas, etc.) up until July 2014. Realizing the common information could be very useful for criminals, the

58. Zuigao Renmin Fayuan Guanyu Shenli Liyong Xinxi Wangluo Qinhai Renshen Quanyi Minshi Jiufen Anjian Shiyong Falu Ruogan Wenti de Guiding
最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定 [Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks](promulgated by the Sup. People's Ct., June 23, 2014, effective Oct. 10, 2014) (Lawinforchina)(China), *available at* http://www.lawinfochina.com/display.aspx?id=17960&lib=law.

59. Jidi Fuwu Yonghu Geren Xinxi Anquan Guanli Guiding (寄递服务用户个人信息安全管理规定) ([Provisions on the Management of the Security of Personal Data of Postal and Delivery Service Users](promulgated by the State Post Bureau of P.R.C., March 26, 2014)(China), *available at* http://www.spb.gov.cn/zcfg/gfxwj/201403/t20140326_301911.html (the "Security Provisions"); Wufa Toudi You Wufa Tuihui Kuaijian Guanli Guiding (无法投递又无法退回快件管理规定) [Provisions on the Management of Undeliverable and Unreturnable Express Items]](promulgated by the State Post Bureau of P.R.C., effective Mar. 10, 2014) (China), *available at* http://www.spb.gov.cn/zcfg/gfxwj/201403/t20140319_298677.html (the "Undeliverable Items Provisions"); Youzheng Hangye Anquan Xinxi Baogao He Chuli Guiding (邮政行业安全信息报告和处理规定) [Provisions on the Reporting and Handling of Security-related Operational Information in the Postal Industry] (promulgated by the State Post Bureau of P.R.C., effective Mar. 10, 2014) (China), *available at* http://www.spb.gov.cn/zcfg/gfxwj/201403/t20140326_301911.html (the "Reporting Provisions").

60. Ted Thornhill, *Nearly Half of South Koreans Have their Bank Details Stolen (including the President) as Anti-Fraud Worker Arrested*, MailOnline (Jan. 21, 2014) http://www.dailymail.co.uk/news/article-2543167/Data-100MILLION-South-Korean-credit-cards-stolen-scam-affecting-40-population-including-President-Park-Geun-hye.html.

61. *Id.*

lawmakers amended both the Personal Information Protection Act (PIPA)[62] and the Act of Promotion of Information and Communication Network Utilization and Information Protection (the Network Act)[63] totally abandoning the collection of the residence registration number as from August 7, 2014, unless otherwise absolutely required under other laws, such as tax, insurance and medical-related laws.

While the vibrant discussion on the subject of prohibiting the collection of residence registration numbers was ongoing, a particular event occurred in relation to the famous Korean drama called *My Love from the Star*.[64] In the drama, an alien who came to the Earth 400 years ago, but still looked as young as a 30-year-old man, fell in love with a famous Korean actress. Because the drama was so popular, models of dresses and accessories worn by the actress were quickly sold out through Internet shopping malls, but shoppers from neighboring foreign countries could not purchase the clothes, handbags and accessories.[65] This was because they, unfortunately, did not have a Korean residence registration number and a digital authentication certificate required to register and sign in on Korean Internet shopping mall sites, and which also can only be obtained by using a residence registration number. This caused a huge loss of sales potential and, as a result, the issue was put on the agenda of a cabinet meeting with South Korean President Park.[66] After the cabinet meeting, the Financial Services Commission immediately relaxed its strict rules to allow foreign shoppers to purchase products without an e-certification.

Since August 7, 2014, collection of resident registration numbers is prohibited under the PIPA, unless such collection is required by other laws.[67] In addition, the PIPA also was revised to provide that companies that currently retain resident registration numbers should delete the numbers from their systems by August 6, 2016.[68] Sanctions for violation of the PIPA were also increased. Any violation of the provision prohibiting the retention of residence registration numbers is subject to a penalty of up to 30 million Won.[69] In the event personal information is compromised and data security measures have not been implemented, the maximum penalty would be up to 500 million Won.[70]

In addition to the changes in the PIPA, the "Network Act" was also amended. The PIPA is a general law in relation to personal information and the Network Act is only

62. Gae-in Jeong-bo Bo-ho Bop [Personal Information Protection Law], Art. 24(2) (S. Kor.), amended Aug. 6, 2013 and effective Aug. 7, 2014.

63. Jeongbotongsinmang Bop [The Act on Promotion of Information and Communications Network Utilization and Data Protection], art. 23-2 (S. Kor.), *available at* http://koreanlii.or.kr/w/images/d/df/DPAct2014_ext.pdf.

64. *See My Love from the Star*, WIKIPEDIA, http://en.wikipedia.org/wiki/My_Love_from_the_Star (last updated Mar. 28, 2015).

65. Hwangbo Yon, *"Cancerous regulations" Still Complicate Online Shopping*, THE HANKYOREH (Apr. 3, 2014), http://english.hani.co.kr/arti/english_edition/e_business/631104.html.

66. Sam Lim, *Online Shopping in Korea to Become More Accessible to Foreigners*, SEOULSYNC (July 31, 2014), http://www.seoulsync.com/news/online-shopping-become-accessible-foreigners.

67. *See* Gae-in Jeong-bo Bo-ho Bop [Personal Information Protection Law], *supra* note 61.

68. *See* Hee-Eun Kim, *Korea Strengthens Protection for 'Resident Registration Numbers' (RRNs): Leaks May Face a Fine of up to 0.5 Billion Korean Won*, INSIDEPRIVACY (Aug. 7, 2014), http://www.insideprivacy.com/international/korea-strengthens-protection-for-resident-registration-numbers-rrns-leaks-may-face-a-fine-of-up-to-0/.

69. *See* Gae-in Jeong-bo Bo-ho Bop [Personal Information Protection Law], *supra* note 61, art. 72.

70. *Id.* art. 34–2.

applicable to companies that provide services through the Internet.[71] The newly revised Network Act took effect on November 29, 2014.[72] Among other changes, the retention period for unused personal information was shortened to one year from the previous three-year period.[73] So, Internet shopping malls need to delete personal information if the owner of the personal information has not logged into the mall web site for one year, after sending a notice to the lapsed users.

Moreover, in the event personal information is compromised, the penalty rate was increased from 1 percent to 3 percent of sales revenue.[74] This would be a significant increase for Internet shopping malls. Furthermore, companies should notify or report to the proper authority within twenty-four hours following the breach of personal information.[75] This twenty-four hour reporting requirement seems to be very short, especially considering the time required to determine which personal information was breached.

71. *See* Gae-in Jeong-bo Bo-ho Bop [Personal Information Protection Law], *supra* note 61; *see* Jeongbotongsinmang Bop [The Act on Promotion of Information and Communications Network Utilization and Data Protection], *supra* note 62.

72. *See* Jeongbotongsinmang Bop [The Act on Promotion of Information and Communications Network Utilization and Data Protection], *supra* note 62.

73. *Id.* art. 1.

74. *See* James Lim, *South Korea Increases Data Breach Fines, Lowers Liability Threshold*, BNA BLOOMBERG (May 19, 2014), http://www.bna.com/south-korea-increases-n17179890601/.

75. *See* Jeongbotongsinmang Bop [The Act on Promotion of Information and Communications Network Utilization and Data Protection], *supra* note 62, art.76(1)–2–2.

THE YEAR IN REVIEW

AN ANNUAL PUBLICATION OF THE ABA/SECTION OF INTERNATIONAL LAW

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW