International Lawyer

Volume 47
Number 0 *International Legal Developments Year in Review: 2012*
Article 8

2013

Privacy, E-Commerce, and Data Security

W. Gregory Voss

Katherine Woodcock

Rob Corbet

Jan Dhont

Bruce A. McDonald

See next page for additional authors

Privacy, E-Commerce, and Data Security

Authors

W. Gregory Voss, Katherine Woodcock, Rob Corbet, Jan Dhont, Bruce A. McDonald, Demetrios Eleftheriou, Emily Hay, Cecil Saehoon Chung, and Jae Hyun Park

Privacy, E-Commerce, and Data Security

W. Gregory Voss, Katherine Woodcock, Rob Corbet, Jan Dhont, Bruce A. McDonald, Demetrios Eleftheriou, Emily Hay, Cecil Saehoon Chung, And Jae Hyun Park*

This article reviews important legal developments during 2012 in the fields of privacy, e-commerce, and data security.[1] A special focus has been made on European developments, in light of changes around a new proposed privacy framework (discussed in Part I(A)(1) and (2) below), and a new section on Asia-Pacific developments has been added this year (in Part III below).

* The committee editor is W. Gregory Voss, Toulouse University, Professor at TBS (Toulouse Business School), Member of the *Institut de Recherche en Droit Européen International et Comparé* [Research Institute in European, International and Comparative Law] (IRDEIC), Toulouse, France. The authors are: Europe section: European Union: EU Article 29 Data Protection Working Party (WP) Guidance: Katherine Woodcock, Lorenz International Lawyers, Brussels, Belgium; The Proposal for an EU Regulation on Data Protection: Rob Corbet, Partner, Arthur Cox, Dublin, Ireland and Co-Chair of the ABA Section of International Law Privacy, E-Commerce, and Data Security Committee; E-Commerce, and Data Security: W. Gregory Voss; and Belgium: Jan Dhont, Lorenz International Lawyers, Brussels, Belgium; United States section: Bruce A. McDonald, Shareholder, Buchanan Ingersoll & Rooney PC, Washington, D.C.; Asia-Pacific section: APEC: Demetrios Eleftheriou, Senior Counsel — Privacy and Data Security, EMC Corporation, Brentford, Middlesex, United Kingdom; Australia: Emily Hay, Lorenz International Lawyers, Brussels, Belgium; and South Korea: Mr. Cecil Saehoon Chung, Senior Foreign Counsel, Co-Vice Chair, Antitrust Practice Group, Head of International Antitrust at the law firm of Yulchon LLC, Seoul, Korea, Mr. Jae Hyun Park, Partner, Corporate & Finance Group, Yulchon. Mr. Dhont wishes to thank David Dumont and Jonathan Guzy for their assistance in the Belgium section. The South Korea section authors wish to thank Ms. Hyun Jeong Kim, an associate in the Corporate & Finance Group, for her assistance.

1. For earlier developments in this field, see W. Gregory Voss, Katherine Woodcock, David Dumont, Nicholas D. Wells, Jonathan I. Ezor, João Luís Traça, Bernardo Embry & Fatima Khan, *Privacy, E-Commerce, and Data Security*, 46 Int'l Law. 97 (2012).

I. Developments in Europe

A. European Union

1. *EU Article 29 Data Protection Working Party (WP) Guidance*

a. Cloud Computing

In what was probably its most anticipated opinion of the year, the WP issued its guidance on cloud computing.[2] The opinion clarifies the duties and responsibilities of controllers, processors, and sub-contractors (sub-processors). Further, it highlights the necessity of transparency in client relationships with cloud providers, including the importance of disclosing location of data and third parties involved in the processing. It also touches on the issues with international transfers, including transfers to the United States under the Safe Harbor framework.[3] In its recommendations, the WP emphasizes that businesses should do a risk assessment (also a privacy impact assessment) and conduct proper due diligence on their cloud providers to ensure transparency of processing.[4] This will allow clients (controllers) to adequately account for any risks that might arise in cloud scenarios (e.g., sub-contracting, the possibility of international transfers, and data access) in its contractual relationship with the provider. The opinion includes guidelines that may serve as a checklist for businesses (both clients and providers) involved in cloud services.[5]

b. Data Processor Binding Corporate Rules (BCRs)

Pushing forward a more streamlined approach to international transfers, the WP issued a working document on Binding Corporate Rules (BCRs) for data processors.[6] The document is to serve as a toolbox for the required conditions for processor BCRs. The possibility for processor BCRs is foreseen in the new proposed EU data protection regulation[7] (Regulation), and the working document sets out a table for compliance points. The document also highlights that contractual relationships between processors and controllers should be in the form of a service agreement that is unambiguously linked to the processor BCRs. This would provide adequate assurances to controllers that their personal data will be processed in compliance with these pre-approved standards.

---

2. Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing*, 01037/12/EN, WP 196 (July 1, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

3. *Id.* at 17-19.

4. *Id.* at 19.

5. *Id.* at 19-20.

6. Article 29 Data Protection Working Party, *Working Document 02/2012 Setting Up a Table with the Elements and Principles to Be Found in Processor Binding Corporate Rules*, 00930/12/EN, WP 195 (June 6, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf.

7. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter *Regulation*].

c. Facial Recognition and Biometrics

The WP also published two opinions on biometrics: the first relating to facial recognition in online and mobile services[8] (Facial Recognition Opinion) and the second on developments in biometric technology[9] (Biometric Opinion). Both opinions build on previous work by the WP[10] and seek to provide greater guidance to the industry, the authorities, and users. The Biometric Opinion outlines the legal framework for the operation of biometric technology, including transparent notices and purposes for processing biometric data, the protection of the data subject's fundamental rights, and providing alternatives to data subjects who do not want to have their biometric data processed. The Facial Recognition Opinion highlights that digital photos may be considered sensitive data and presents instances that would be legitimate grounds for processing.

d. Data Protection Reforms

The WP has published two responses on the data protection reform—one on the draft Regulation and the other on the ongoing discussions. In its first opinion, the WP took the opportunity to comment on the draft Regulation.[11] The comments include its views on the role and competences of national data protection authorities (DPAs), the right to be forgotten, accountability, and data breach notification. In its second opinion, the WP weighs in on the ongoing discussions to provide further guidance, particularly on what the WP deems to be "key data protection concepts."[12] It expresses the view that the definition of personal data should remain broad in order to ensure privacy and that consent should be uniform and of a "high standard."[13] Where consent is used, it should be in the appropriate context (in line with the WP's other opinions on the matter) and sufficiently clear.[14] Furthermore, the WP encourages the specification of explicit consent.[15] The opinion ends by scrutinizing the need for and the effect of the proposed delegated acts and suggesting more appropriate alternatives, where necessary.[16]

8. Article 29 Data Protection Working Party, *Opinion 02/2012 on Facial Recognition in Online and Mobile Services*, 00727/12/EN, WP 192 (Mar. 22, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf.

9. Article 29 Data Protection Working Party, *Opinion 3/2012 on Developments in Biometric Technology*, 00720/12/EN, WP 193 (Apr. 27, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

10. *See* Article 29 Data Protection Working Party, *Working Document on Biometrics*, 12168/02/EN, WP 80 (Aug. 1, 2003), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf.

11. Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals*, 00530/12/EN, WP 191 (Mar. 23, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

12. Article 29 Data Protection Working Party, *Opinion 08/2012 Providing Further Input on the Data Protection Reform Discussions*, 01574/12/EN, WP 199, 4 (Oct. 5, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf.

13. *Id.* at 4-6.

14. *Id.* at 7.

15. *Id.*; *Regulation*, *supra* note 7, art. 4(8), at 42.

16. *Id.* at 8-13.

e. Exemptions from Cookie Consent Requirements

Following amendments to the e-Privacy Directive, informed consent must be acquired before the installation of a cookie in the European Union. Building on its previous guidance on consent, the WP issued an opinion explaining the application of the exceptions to the consent requirement. Informed consent of a user is not required when a cookie is used "for the sole purpose of carrying out the transmission of a communication over an electronic communications network."[17] The WP elaborates three capability factors to meet this exemption: (1) the capability to route "information over the network" (identifying communication endpoints); (2) the capability to trade data items in order (numbering packets); and (3) the capability "to detect transmission errors or data loss."[18] The second exemption occurs when a cookie is "strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."[19] This applies when the user takes positive action to make the request with clearly defined boundaries, and the cookie is strictly needed for the service. Additionally, the WP presents different forms (and associated longevity) of cookies, stating that cookies exempted from consent should only have a lifespan that is directly related to their purpose and should expire once they are no longer necessary. The WP highlights that multipurpose cookies (e.g., tracking and remembering user preferences) do exist, and that if one of the purposes is exempted (i.e., user preferences), the website—nevertheless—needs user consent because the other purposes do not qualify for an exemption. The WP concludes by outlining cookies that are not exempted from consent, namely social plug-in tracking, and third party marketing cookies as well as first party analytics.

2. *The Proposal for an EU Regulation on Data Protection*

a. Proposed New EU Laws on Data Protection

On January 25, 2012, the European Commission outlined its proposals for a radical overhaul of data protection rules in the European Union. The proposed Regulation will increase compliance obligations of all companies targeting customers in the European Union with the possibility of fines of up to 2 percent of global turnover for certain breaches.[20] The Regulation was published in conjunction with a new directive that will apply general data protection principles and rules to police and judicial cooperation in criminal matters.[21] The proposal represents the most significant development in European data protection law in nearly twenty years.

17. Article 29 Data Protection Working Party, *Opinion 04/2012 on Cookie Consent Exemption*, 00879/12/EN, WP 194, 3 (June 7, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

18. *Id.* § 2.2, at 3-4.

19. *Id.* § 2.1, at 2-3.

20. *Regulation*, *supra* note 7, art. 79(6), at 93-94.

21. *See Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offenses or the Execution of Criminal Penalties, and the Free Movement of Such Data*, COM (2012) 10 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf.

b. Purpose of the Regulation

By putting forward the Regulation, the EU is aiming to develop a more coherent and unified data protection law throughout the European Union. The proposal would supersede the existing Data Protection Directive[22] (EU Data Protection Directive), but unlike directives, regulations do not require any implementing measures at the local member state level. Hence, they become immediately enforceable as law in all member states simultaneously, and member states will have no scope to pass diverging domestic laws.

c. Principal Changes

Although the Regulation is extensive, some of the main areas of change can be summarized as follows:

i. Scope

The Regulation will apply to any business offering goods or services for sale to EU citizens and to any entity that monitors the behavior of consumers in the European Union.[23]

ii. Data Protection Officer

Organizations with more than 250 people will be required to appoint a Data Protection Officer.[24]

iii. Fines

Data Protection Supervisory Authorities may apply fines between 0.5 percent and 2 percent of global turnover for non-compliance with certain provisions in the Regulation.[25]

iv. Breach Notifications

The Regulation would introduce mandatory data breach notifications across all industries.[26]

v. Privacy Impact Assessments

The Regulation would introduce an obligation on data controllers and data processors to conduct data protection impact assessments before the launch of any privacy invasive products or services.[27]

---

22. *See* Council Directive 95/46, 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, 1995 O.J. (L 281) 31 (EC) [hereinafter EU Data Protection Directive].

23. *Regulation*, *supra* note 7, art. 3(2), at 41.

24. *Id.* art. 35(1), at 65.

25. *Id.* art. 79, at 92-94. The fines that can be imposed by the Data Protection Supervisory Authorities in any Member State are graduated depending on the nature of the breach. *Id.*

26. *Id.* arts. 31-32, at 60-62. Currently breach notifications are only mandatory in the case of communications providers pursuant to the ePrivacy Directive. *See* Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37, 43 [hereinafter ePrivacy Directive].

27. *Regulation*, *supra* note 7, art 33, at 62-63.

vi. Right to Object to Profiling

Individuals shall be given a new right to object to being profiled, which includes analysis or predictive processes relating to a "person's performance at work, economic situation, location, health, personal preferences, reliability or behavior."[28]

vii. Right to Be Forgotten

The Regulation includes the introduction of a "right to be forgotten" whereby an individual can withdraw their consent to having their data processed.[29] There are limited exceptions, e.g., where the data is needed for "historical, statistical, and scientific research purposes."[30]

viii. New Definition of Consent

The Regulation introduces a tighter definition of consent than under the existing EU Data Protection Directive, which will apply generally and in the context of marketing permissions.[31]

ix. Greater Protections for Children

The Regulation introduces additional protections for obtaining and processing data relating to children.[32]

d. Implementation

The Proposal has been passed on to the European Parliament and the Council of Ministers for discussion. Therefore, the timetable for implementing the Regulation is not certain, but the Proposal is expected to be given priority during Ireland's presidency of the European Union in early 2013.[33] Initial lobbying efforts have not resulted in any radical changes to the Regulation, but it seems likely that some of the existing concessions for small or medium enterprises may be extended to reduce the bureaucratic effect of compliance on smaller entities.[34]

28. *Id.* art. 20, at 54.

29. *Id.* art. 17, at 51-53.

30. *Id.* art. 17(3), at 52.

31. *Id.* art. 4(8), at 42. The criterion "explicit" is added to the definition of consent to avoid confusion with the term "unambiguous" consent, which was used in the Data Protection Directive, the intention being that one single and consistent definition of consent would apply, thereby ensuring the awareness of the data subject that, and to what, he or she gives consent.

32. *See, e.g., id.* art. 8, at 45 (setting out additional conditions for processing children's personal data in relation to information society services offered directly to them).

33. *See* Colm Kelpie, *Pressure on Government to Overhaul EU Data Laws*, IRISH INDEP. (Sept. 25, 2012), http://www.independent.ie/business/european/pressure-on-government-to-overhaul-eu-data-laws-3240330.html.

34. *See* Viviane Reding, Vice-President of the European Commission, Press Conference, Justice Council: Making Good Progress on Our Justice for Growth Agenda, SPEECH/12/764 (Oct. 26, 2012), http://europa.eu/rapid/press-release_SPEECH-12-764_en.htm.

3. *E-Commerce and Data Security*

At the end of 2011, the Commission communicated on the future of value-added tax (VAT), evoking the possibility of converging rates on similar goods between the online and offline worlds—for example, on e-books and paper ones.[35] In addition, while currently intra-EU Business-to-Business (B2B) transactions are based on taxation "at destination," the Commission will work on "examining in detail the different possible ways to implement the destination principle," including by the "charging of VAT by the supplier on cross-border B2B supplies."[36]

On January 11, 2012, the Commission issued a communication setting out a strategy in order to build trust in the community-wide market for goods and services sold online (Communication).[37] The Communication highlights the small share of European GDP attributable to the "internet economy"—3 percent—and the potential for growth if concerted action is taken.[38] The strategy aims to attack five main obstacles to growth: (i) inadequate cross-border supply of services, (ii) inadequate information for service operators and protection for users, (iii) inadequate payment and delivery systems, (iv) too much abuse and difficult-to-settle disputes, and (v) not enough use of high-speed networks and other high technology means.[39] In order to attack these obstacles the Commission proposed several actions.

The Commission intends to issue "guidelines on the implementation of Article 20 of the Services Directive, which explicitly prohibits . . . discrimination" based on a customer's nationality or residence when he or she purchases goods or services in a different country.[40] It will also ensure rigorous application of the rules on selective distribution and fight "unfair business practices."[41] Going forward to 2013-2014, the Commission will develop codes of good conduct and guidelines "giving consumers access to transparent and reliable information allowing them to compare more easily the prices, the quality and the sustainability of goods and services."[42] The Commission also announced that it would establish a European Cybercrime Center by 2013,[43] which is meant to be helpful in the fight against cyber-attacks.

Concrete action already taken in connection with the Commission's strategy includes the issue of a Green Paper on payment means (Payment Green Paper)—card, internet,

35. *Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Future of VAT: Towards a Simpler, More Robust and Efficient VAT System Tailored to the Single Market*, para. 5.2.2, at 11, COM (2011) 851 final (Dec. 6, 2011), *available at* http://ec.europa.eu/taxation_customs/resources/documents/taxation/vat/key_documents/communications/com_2011_851_en.pdf.

36. *Id.* para. 5.4, at 15-16.

37. *Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Coherent Framework for Building Trust in the Digital Single Market for E-Commerce and Online Services*, at 3, COM (2011) 942 final (Jan. 11, 2012), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF.

38. *Id.* para. 1, at 1-2.

39. *Id.* para. 2.2, at 4.

40. *Id.* para. 3.1, at 5-6 (referring to Directive 2006/123, of the Parliament and of the Council of 12 December 2006 on Services in the Internal Market, 2006 OJ (L 376) 36 (Dec. 27, 2006).

41. *Id.* para. 3.2, at 8.

42. *Id.* para. 3.2, at 10.

43. *Id.* para. 3.4, at 15.

and mobile payments,[44] meant to identify obstacles to European integration in the area, and a Communication on an EU framework for online gambling.[45] The latter aims to set forth action in 2013 to increase protection of consumers and minors, to prevent gambling disorders and addictions, and the adoption of recommendations both in this area and with respect to "responsible gambling advertising."[46]

The Commission's Work Program for 2013 includes a few items of interest in the e-commerce context. In the first quarter, the Commission intends to issue a proposed regulation to reduce costs of broadband infrastructure deployment across the EU. During 2013, it will issue a communication to set out an action plan for accelerating wireless broadband networks and encouraging shared spectrum use, and it will follow up on the Payment Green Paper with potential legislation in the second quarter of 2013.[47]

In addition, Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, announced that she plans to present the European Strategy for Cyber-Security, which will focus on the need to stimulate "user demand for security functionalities," include initiatives to develop an "external EU cyber security policy," and propose legislation "setting up a high level of network and information security across the EU."[48] Kroes is also considering extending current telecom sector requirements to adopt risk management and reporting measures to other sectors such as "enablers of key Internet services," banking, and health.[49]

B. BELGIUM

1. *E-Mail and Computer Use Monitoring*

On May 2, 2012, the Belgian Data Protection Authority (Belgian DPA) issued a non-binding recommendation on cyber-surveillance in the workplace, striving to clarify the rules governing access to content of e-mails at work.[50] In its game-changing recommendation, the Belgian DPA opines that the current legal framework provides a sufficient basis to access e-mail content in certain cases, taking the view that accessing such content is

44. Commission *Green Paper: Towards an Integrated European Market for Card, Internet and Mobile Payments*, COM (2011) 941 (final) (Jan. 11, 2012), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0941:FIN:EN:PDF.

45. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: Towards a Comprehensive European Framework for Online Gambling*, COM (2012) 345 final (Oct. 23, 2012), *available at* http://ec.europa.eu/internal_market/services/docs/gambling/comm_121023_onlinegambling_en.pdf.

46. *Id.* para. 2.3, at 10-13.

47. *Annex to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Commission Work Programme 2013*, at 5, COM (2012) 629 final (Oct. 23, 2012), *available at* http://ec.europa.eu/atwork/pdf/cwp2013_annex_en.pdf.

48. *See* Neelie Kroes, Vice-President, European Comm'n Responsible for the Digital Agenda, Address at the Information Security Forum Conference, Cyber-Security — A Shared Responsibility, SPEECH/12/774 (Nov. 4, 2012), *available at* http://europa.eu/rapid/press-release_SPEECH-12-774_en.htm.

49. *Id.*

50. Recommandation no 08/2012 du 2 mai 2012 d'initiative relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail [Recommendation no. 08/2010 of May 2, 2012 on Cybersurveillance in the Workplace] COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE [CPVP] [Privacy Commission], *available at* http://www.lexalert.net/uploads/documentenbank/0d73273d12e2f867960140383ac6f043.pdf.

legally authorized by the employer's general authority set forth in the 1978 Employment Contract Act. The Belgian DPA considers an employee's consent to be unreliable, as it may not be freely given. Such access is only allowed only if it complies with the finality, transparency, and proportionality principles (Principles). Practically, it means that the employer must: pursue a legitimate and predefined purpose, such as the prevention of illegal or defamatory acts when accessing emails; inform employees of the monitoring practices of the employer; and not systematically access all e-mails of its employees. Additional procedural rules are specified.

The Belgian DPA further proposes practical measures to facilitate compliance with the Principles, such as:

- Consider limiting employees' use of professional email account for business related purposes in a computer use policy. In this case, the employer may presume that all emails are professional and may be opened.
- If employees are allowed to use their professional email account for private purposes, additional measures should be taken to mitigate the risks that the employer interferes with private e-mails of its employees.

2. *Amendments to the Belgian Telecom Act*

On October 1, 2012, amendments to the Belgian Telecom Act implemented by the Act on Various Provisions regarding Electronic Communications came into force.[51] The Act on Various Provisions regarding Electronic Communications implements the amendments to the ePrivacy Directive.[52] The Amended Telecom Act introduces an opt-in consent requirement for cookies and a data breach notification obligation for telecom providers.[53]

a. Cookies

The amended Telecom Act now requires companies using cookies on their website to obtain the opt-in consent of the users prior to installing any cookies on his or her hardware.[54] This requirement does not apply to cookies that are strictly necessary to transmit a communication over an electronic communication network or to provide services explicitly requested by the user. Furthermore, the user must be provided with an easy way to withdraw his or her consent free of charge. In the absence of further requirements or

51. Loi portant des dispositions diverses en matière de communications électroniques [Act on Various Provisions regarding Electronic Communications] of July 10, 2012, MONITEUR BELGE [M.B.] [Official Gazette of Belgium], July 25, 2012, 40969.

52. The ePrivacy Directive, *supra* note 26, was amended by Directive 2009/136. Directive 2009/136, of the European Parliament and of the Council of 25 Nov. 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF.

53. Loi relatif au statut du régulateur des secteurs des postes et des télécommunications belges [Belgian Telecom Act] of Jan. 17, 2003, MONITEUR BELGE [M.B.] [Official Gazette of Belgium], *as amended* July 25, 2012, at 1, *available at* http://www.ibpt.be/ShowDoc.aspx?objectID=948&lang=fr.

54. *Id.* art. 129.

guidance provided by the Belgian Legislator, companies can rely on the relevant recommendations of the Belgian DPA to assess consent methods and requirements.[55]

b. Breach Notification

A new article 141/1 was included in the Telecom Act, which introduces a data breach notification obligation for providers of public electronic communication services (i.e., services that mainly consist of transferring signals over an electronic communication network).[56] This implies that such providers are required to immediately notify any security breach affecting personal data to the Belgian Institute for Postal Services and Telecommunications (BIPT). Moreover, such providers are required to notify the concerned individuals without delay in case the data breach is likely to negatively affect their personal data and privacy.

II. Developments in the United States

The U.S. Supreme Court held that the civil remedy provision of the Privacy Act, which allows the recovery of actual damages for an intentional or willful violation of the Act, does not permit monetary damages for mental or emotional distress.[57] Therefore, the Federal Government's sovereign immunity from liability for mental or emotional distress is not waived under the Act.[58]

The Supreme Court also held that the government attaching a GPS device to a defendant's vehicle and using it to monitor the vehicle's location is considered a search under the Fourth Amendment.[59] The Court held that where a constitutionally protected area is physically encroached by the government and information is acquired thereby, the result is a seizure of property—not only in the sense of a trespass, but also a meaningful interference with the individual's possessory interests in the property.[60] The Court explained that a trespass alone is not considered a search until it is also combined with efforts to acquire information.

Additionally, the Supreme Court struck down a state law that restricted the use of pharmacy records detailing individual doctors' prescribing habits."[61] The Court reasoned that the state's interest in physician confidentiality by enacting the law did not justify the additional burden planted on protected expression. The law's primary purpose was to prevent pharmaceutical manufacturers from using "detailers" to seek out information identifying prescription habits in order to market the manufacturers' own brand-name drugs. This

55. Avis no. 10/2012 du 21 mars 2012 rélatif au Projet de loi portant des dispositions diverses en matière de communications électroniques [Opinion No. 10/2012 of March 21, 2012 on Certain Provisions of the Telecom Act under Revision], COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE [CPVP] [Privacy Comm'n], *available at* http://www.privacycommission.be/sites/privacycommission/files/documents/avis_10_2012.pdf.

56. *See* Jan Dhont & David Dumont, *Belgium — Time to Comply with the Amended Telecom Act*, INT'L ASS'N PRIVACY PROS. (Dec. 1, 2012), https://www.privacyassociation.org/publications/2012_12_01_belgium_time_to_comply_with_the_amended_telecom_act.

57. FAA v. Cooper, 566 U.S. ___, 132 S. Ct. 1441, 1456 (2012).

58. *Id.*

59. United States v. Jones, 565 U.S.___, 132 S. Ct. 945, 946 (2012).

60. *Id.*

61. Sorrell v. IMS Health Inc., 564 U.S. ___, 131 S.Ct. 2653, 2659 (2011).

restriction was imposed on pharmaceutical manufactures despite journalists, researchers, and the state itself being permitted to use the information, in addition to pharmacies being able to sell the information for health care research purposes. The Court quipped "many are those who must endure speech they do not like."[62]

At the appellate level, the Sixth Circuit held that inherent location data broadcast to police from a defendant's cell phone did not constitute a reasonable expectation of privacy.[63] The *Skinner* court held that data broadcast from the defendant's cell phone that had a known number and was used voluntarily while driving on public roads did not violate the Fourth Amendment where the police tracked the signal over a three-day period. The court reasoned that because the same information could be gathered by visual surveillance alone, the cellular data merely aided the police in tracking the defendant's location.

In a noteworthy district court class action case, mobile device users claimed that their privacy rights were violated when mobile device manufacturers and other mobile industry defendants allowed third party applications on user's phones to collect and make commercial use of their personal information without their knowledge or consent.[64] The court granted the defendants' motion to dismiss, holding that (1) mobile devises are not facilities under the Stored Communications Act (SCA); (2) a mobile device user's location data is note electronic storage under the SCA; (3) a user's geo-location data is not content under the Wiretap Act; (4) the alleged disclosure of a user's unique device identification number, personal data, and geo-location information does not violate a user's right to privacy; (5) the plaintiffs failed to state a claim under the Computer Fraud and Abuse Act (CFAA); and (6) the plaintiffs failed to state a trespass claim because they could not establish the necessary element of harm.[65]

III. Developments in Asia-Pacific

A. APEC Cross-Border Privacy

Cross-border transfers of personal data and the legal obstacles raised by such transfers continue to complicate privacy compliance processes. Currently there are two competing international privacy regimes addressing cross-border transfers. Of course, when one hears of cross-border transfer requirements, one may think of the EU Data Protection Directive and the one-two punch of Articles 25 and 26.[66] In the Asia-Pacific region, the development of a bigger, yet less flamboyant, competing cross-border transfer regime

62. *Id.* at 2670.

63. United States v. Skinner, 690 F.3d 772, 775 (6th Cir. 2012).

64. *In re* iPhone Application Litig., 844 F. Supp. 2d 1040 (N.D. Cal. 2012).

65. *Id.*

66. Directive 95/46, 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, 1995 O.J. (L 281) 31, 33, arts. 25–26 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. Article 25 prohibits the transfer of personal data to countries that do not have adequate privacy laws as determine by the European Union, and article 26 provides exceptions to that prohibition. *Id.*

known as the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (CBPR Program) has been witnessed.[67]

The U.S. Federal Trade Commission (FTC), which has been the most active federal regulator from a privacy and data security enforcement standpoint, and the U.S. Department of Commerce (Commerce Department), which manages the U.S.-EU Privacy Safe Harbor Framework, participated in the development of the CBPR Program. According to the FTC, the CBPR Program "is a self-regulatory code of conduct designed to create more consistent privacy protections for consumers when their data moves between countries with different privacy regimes in the APEC region."[68] According to the Commerce Department, the "CBPR system requires organizations to develop their own internal business rules on cross-border privacy procedures, which must be assessed as compliant with the minimum requirements of the APEC system by an independent public or private sector body, called an Accountability Agent."[69] The "'Accountability Agent' is a third-party organization that provides verification services related to the data privacy policies and practices for those businesses seeking CBPR certification."[70] The Commerce Department is currently inviting interested organizations to submit applications for recognition by the APEC System as "Accountability Agents" for U.S.-based companies subject to the FTC's jurisdiction.[71]

In July 2012, the United States was approved as the first formal participant of the CBPR Program, and the FTC was approved as the CBPR Program's first enforcement authority.[72]

There is also an effort underway to avoid a conflict as working groups from these two regions continue to work together in an effort to establish interoperability or at least a more harmonious approach between the two privacy regimes. Could interoperability between these two competing regimes work so that in-house privacy counsels are able to work through the requirements? This remains to be seen.

---

67. *See APEC Cross-Border Privacy Enforcement Arrangement (CPEA)*, ASIA-PAC. ECON. COOPERATION, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx (last visited Jan 20, 2013). The CBPR Program was developed by the APEC member economies, which are: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, South Korea, Taiwan, Thailand, the United States, and Vietnam. *See Member Economies*, ASIA-PAC. ECON. COOPERATION, http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx (last visited Jan. 20, 2013).

68. *See* Press Release, Fed. Trade Comm'n, FTC Welcomes a New Privacy Sys. for the Movement of Consumer Data Between the U.S. and Other Economies in the Asia-Pac. Region (Nov. 14, 2011), *available at* http://www.ftc.gov/opa/2011/11/apec.shtm.

69. *See* Applications to Serve as Accountability Agents in the Asia Pacifica Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System, 77 Fed. Reg. 44,582 (July 30, 2012), *available at* https://www.federalregister.gov/articles/2012/07/30/2012-18515/applications-to-serve-as-accountability-agents-in-the-asia-pacific-economic-cooperation-apec-cross.

70. *Id.*

71. *See id.*

72. *See* Press Release, Asia-Pac. Econ. Cooperation, Elec. Commerce Steering Grp., APEC Cross-Border Privacy Rules Sys. Goes Pub. (July 31, 2012), *available at* http://www.apec.org/Press/News-Releases/2012/0731_cbpr.aspx.

B. AUSTRALIA

1. *Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) (Bill)*[73]

Amendments to the Privacy Act of 1988 were put before the Australian Parliament in May 2012 and were passed on November 29, 2012.[74] These reforms are expected to come into force around March 2014, fifteen months after Royal Assent.[75] These reforms marked the first stage of implementing the Australian Law Reform Commission's recommendations in a 2008 report on privacy.[76] The second stage of reforms has not yet been set but may deal with the removal of exemptions for small businesses, employee records, mandatory data breach notifications, and a statutory cause of action for serious invasion of privacy.

a. Privacy Commissioner's New Powers

The Bill introduces a number of new powers for the Privacy Commissioner, who will be able to: seek civil penalties for serious or repeated interferences with privacy;[77] accept written undertakings from organizations that they will take (or refrain from) a specified action, which are enforceable in court;[78] make a determination following an investigation conducted on the Commissioner's own initiative, rather than only after an individual complaint;[79] and conduct performance assessments of private sector organizations, not just government and credit reporting agencies.[80]

b. New Australian Privacy Principles

The reforms also introduce a set of Australian Privacy Principles (APPs) to replace the previous separate public and private sector principles. The APPs introduce new protections, including enhanced obligations of access to and correction of personal information,[81] and require the publication of more comprehensive privacy policies.[82] A new direct marketing principle places extra limitations on organizations that may use or disclose personal information to promote or sell goods or services directly to individuals.[83]

Under current law, there is no breach of a privacy principle for acts outside of Australia.[84] Under the new law, if information is disclosed to a recipient overseas who is not

73. Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) (Austl.), *available at* http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4813 [hereinafter Privacy Amendment Bill 2012].

74. *Id.*

75. *Id.* s. 2.

76. *See* AUSTL. LAW REFORM COMM'N, *For Your Information: Australian Privacy Law and Practice* (2008), *available at* http://www.austlii.edu.au/au/other/alrc/publications/reports/108/.

77. *See Privacy Amendment Bill 2012*, sch 4, s 189 (this will become s 80W of the Privacy Act of 1988).

78. *See id.* sch 4, s 64 (this will become ss 33E, 33F of the Privacy Act of 1988).

79. *See id.* sch 4, s 109 (this will become s 52(1A) of the Privacy Act of 1988).

80. *See id.* sch 4, s 54 (this will become s 28A of the Privacy Act of 1988).

81. *See id.* sch 1, s 104 (this will become pt 5 s 12 of the Privacy Act of 1988).

82. *See id.* sch 1, s 104 (this will become pt 1, s 1 of the Privacy Act of 1988).

83. *See id.* sch 1, s 104 (this will become pt 3, s 7 of the Privacy Act of 1988).

84. *Privacy Act 1988* (Cth) pt 2, s 6A(4) (Austl.), *available at* http://www.comlaw.gov.au/Details/C2012C00414.

subject to the APPs, and that recipient engages in action that breaches the APPs, the act may be deemed to have been carried out by the original actor.[85]

c. Other Changes

The Amendments extend the extra-territorial application of the Privacy Act to include information practices outside Australia by any government agency, organization, or small business with an Australian link.[86] Other substantial changes give credit providers access to more information allowing them to make more robust assessments of creditworthiness, along with increased responsibilities on those providers regarding notification, data quality, access and correction, and complaints.[87]

C. South Korea

In 2012, South Korea significantly revised its privacy law, mainly due to persistent incidents of personal data security breaches. In particular, it sharply limited the collection and use of resident registration numbers. Even with built-in grace periods, businesses will have to scramble to change their consumer information collection and use practices and information management systems. Further, businesses will have to scramble to strengthen data security measures to comply with the new law.

On February 17, 2012, the South Korean government amended what is commonly referred to as the Information and Communications Network Act (Revised Act) to prevent unlawful disclosures or thefts of resident registration numbers and to improve the data management standards for businesses, with a six-month grace period for resident registration number collection practices and a twelve-month grace period for information system improvement measures.[88] Subsequently, on April 20, 2012, the Ministry of Public Administration and Security, Korea Communications Commission, and Financial Services Commission jointly adopted "Comprehensive Measures to Minimize Collection and Use of Resident Registration Numbers" (Joint Measures).[89] An amended enforcement decree for the Revised Act became effective on August 18, 2012.[90]

85. *See Privacy Amendment Bill 2012*, sch 1, s 82 (this will become s 16C of the Privacy Act of 1988).

86. *See id.* sch 4, s 2 (this will become ss 5B(1), 5B(1A) of the Privacy Act of 1988).

87. *See id.* sch 2, pt IIIA.

88. *See* Jeongbotongsinmang I-yongchokjin Mit Jeongboboho Deung-e Gwanhan Beomnyul [The Act on Promotion of Information and Communications Network Utilization and Information Protection], Act No. 5835, *amended* Feb. 17, 2012 (S. Kor.); *see also* Press Release, Kor. Commc'ns Comm'n, The Info. & Commc'ns Act is Revised to Reinforce the Privacy Prot. Sys. (Feb. 17, 2012), *available at* http://eng.kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=4&boardSeq=33589

89. Press Release, Kor. Commc'ns Comm'n, Comprehensive Measures to Minimize Collection & Use of Resident Registration Nos. (Apr. 20, 2012), *available at* http://www.kcc.go.kr/user.do?mode=view&page=P05030000&dc=K05030000&boardId=1042&cp=39&boardSeq=33643.

90. For the full text of the Revised Enforcement Decree in Korean, see Jeong Bo Tong Sin Ne Teu Wo Keu I Yong Mic Jeong Bo Bo Ho Deung Ui Chu Jin E Gwan Han Beop Ryur Si Haeng Beop Ryong [Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection], Presidential Decree No. 24102, Sep. 14, 2012 (S. Kor.), available at http://www.law.go.kr/LSW/lsEfInfoP.do?lsiSeq=128671#0000. *See also* Press Release, Kor. Commc'ns Comm'n, Clean Internet Implementation Plan to Limit Use of Resident Registration Nos. on the Internet (June 14, 2012), *available at* http://www.kcc.go.kr/user.do?mode=view&page=P05030000&dc=K05030000&boardId=1042&cp=27&boardSeq=34073.

Under the Revised Act, online collection of resident registration numbers is prohibited, except in certain limited situations.[91] Specifically, collection and use of resident registration numbers are allowed to protect consumers in online transactions, but alternative methods of identity authentication are encouraged.[92] Similarly, resident registration numbers may be used for online payment services, online payment arrears management, and offline transactions for identification purposes, but only until the specifically applicable laws are revised pursuant to the Joint Measures.[93] This means that previously valid e-commerce purposes, such as online identity authentication, age verification, and real name verification for web board posting are no longer permissible justifications for collecting and using resident registration numbers.[94] Furthermore, any existing or retained resident registration numbers must be destroyed within two years.[95]

The Revised Act also requires companies to strengthen their data protection and management standards. For example, companies that meet certain thresholds must maintain their servers for personal information management systems separate and distinct from outside Internet networks.[96] Security breaches of personal information must be reported to authorities without delay.[97] Unless exempted by other law, a person's personal information must be destroyed or separately managed if they have been inactive for over three years.[98]

The new privacy regime represents a fundamental shift in the government's view toward protection of personal information and its resolve to protect the unauthorized disclosure of personal information that causes the most serious harm. But it also represents a rather ambitious endeavor because resident registration numbers have been used for over twenty years as the basis for personal information management systems. Implementing wholesale changes in a short period of time will entail significant costs to various businesses, including information and communications service providers, online businesses, and even offline merchants. The transition issue may be even more acute because currently there are no clear-cut alternatives to the universally used resident registration numbers. It remains to be seen what additional transitional issues will emerge and how businesses and consumers will adapt to the new world after the six and twelve-month grace periods expire in February 2013 and August 2013, respectively.

---

91. The Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 23(2) (alternative methods of identity authentication must be provided to users); *see also* Press Release, Kor. Commc'ns Comm'n, *supra* note 89, at 4.

92. Press Release, Kor. Commc'ns Comm'n, *supra* note 89, at 4.

93. *Id.*

94. *Id.*

95. The Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 23(2).

96. Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 15(2) (entities retaining personal information of more than one million users or providers of information and communications services whose revenue exceeded 10 billion KRW). This particular provision is effective as of February 18, 2013. *Id.* art. 1.

97. The Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 27(3); *see also* Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 14(2).

98. The Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 29(2); *see also* Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, art 16(1).