International Lawyer

Volume 50
Number 0 *International Legal Developments Year in Review: 2015*
Article 8

2016

Privacy, E-Commerce, and Data Security

Marco R. Provvidera

Volha Samasiuk

Richard Peltz-Steele

Mayra Cavazos Calvillo

Adrian Lucio Furman

See next page for additional authors

Recommended Citation
Marco R. Provvidera et al., *Privacy, E-Commerce, and Data Security*, 50 ABA/SIL YIR 103 (2016)
https://scholar.smu.edu/til/vol50/iss0/8

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in International Lawyer by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.

Privacy, E-Commerce, and Data Security

Authors

Marco R. Provvidera, Volha Samasiuk, Richard Peltz-Steele, Mayra Cavazos Calvillo, Adrian Lucio Furman, Renato Opice Blum, Matthew Murphy, and Kyoung Yeon Kim

This article is available in International Lawyer: https://scholar.smu.edu/til/vol50/iss0/8

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

Privacy, E-Commerce, and Data Security

MARCO R. PROVVIDERA, VOLHA SAMASIUK, RICHARD PELTZ-STEELE, MAYRA CAVAZOS CALVILLO, ADRIAN LUCIO FURMAN, RENATO OPICE BLUM, MATTHEW MURPHY, AND KYOUNG YEON KIM*

This Article reviews select important legal developments during 2015 in the fields of privacy, e-commerce, and data security. This year's contribution covers major developments in the European Union, Russia, the United States, Latin America, and the Asia-Pacific region.

I. Developments in the European Union

Following a year (2014) rich in developments for privacy, e-commerce, and data security law in Europe, 2015 maintained that momentum, especially in light of certain major judicial decisions and subsequent advisory-body guidance, which are expected to have far-reaching consequences.

A. LEGISLATIVE ACTION

While some significant steps forward have been made by both the European Parliament and the Council on the most relevant pieces of legislation in the process of approval, the somewhat convoluted CFEU-mandated interplay of the two institutional bodies[1] has translated into delays of final enactment.

---

* The committee editor was Kyoung Yeon Kim, Partner, Yulchon LLC. The authors were European Union: Marco R. Provvidera, Principal/Founder, Provvidera Law Offices, Professor of Law and Economics, University "Gregorio VII", Rome, Italy; Russia: Volha Samasiuk, Compliance and Regulatory Affairs Officer, Wargaming America Inc.; the United States: Richard Peltz-Steele, Professor, University of Massachusetts Law School; Mexico: Mayra Cavazos Calvillo, George Washington University; Argentina: Adrian Lucio Furman, M. & M. Bomchil; Brazil: Renato Opice Blum, Opice Blum, Bruno, Abrisio, Vainzof Advogados Associados; China: Matthew Murphy, Partner, MMLC Group; South Korea: Kyoung Yeon Kim. The committee editor wishes to thank Christopher Mandel, foreign counsel at Yulchon LLC for his editing assistance. The China section author would like to thank Joyce Chang for her assistance.

1. *See* Consolidated Version of the Treaty on the Functioning of the European Union, art. 294, May 9, 2008, 2008 O.J. (C 115) 47 [hereinafter TFEU].

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW

1. *General Data Protection Regulation*

The final passage of the General Data Protection Regulation (the "GDPR") has been long awaited as a necessary update, together with the new Data Protection Directive (the "DPD"), of the almost twenty-year-old seminal Directive 95/46/EC. While after debate, at the October 10, 2014, meeting of the Justice and Home Affairs ministers of the Council, "various issues still remain[ed] to be decided,"[2] the EU Member States approved their negotiating position on the GDPR on June 15, 2015, and the first round of three-way talks began on June 24, 2015.[3] Although consensus is still problematic on the thorny issue of data processed in the context of criminal proceedings, a final agreement on the "Data Protection Package" (composed of both the GDPR and the new DPD) is due by the end of 2015, as strongly indicated in the European Parliament Resolution of October 29, 2015.[4] The Data Protection Package will replace the current patchwork of national laws with a single set of rules.

2. *Passenger Name Records (PNR) Proposed Directive*

After a first report on February 17, 2015, Report II on the Commission's proposal for a comprehensive directive on this similarly contentious area followed on September 7, 2015.[5] While the remaining points of discussion appeared to concern solely whether to include intra-EU flights in the 100%-passenger-monitoring target, and the length of allowed data retention, a September 24, 2015, opinion by the European Data Protection Supervisor revived EU doubts about whether some provisions of the draft comply with the principles of necessity and proportionality,[6] positioning the proposed directive for further delay and bickering. Bilateral agreements between the EU and the United States, Canada, and Australia are currently in place for the regular exchange of PNR for flights to and from the EU and these countries.

3. *Net and Information Security (NIS) and Net Neutrality*

Following some stalemate in 2014, action was revived on the Digital Agenda for Europe. While differences still existed after the third "triologue" (Commission/Council/

2. *See* W. Gregory Voss, *Developments in the European Union*, 49 ABA/SIL YIR, Vol. 98 (2015).

3. Press Release, Eur. Parliament, Data Protection: Parliament's Negotiators welcome Council Negotiating Brief (June 15, 2016), http://www.europarl.europa.eu/news/en/news-room/20150615IPR66464/Data-protection-Parliament%E2%80%99s-negotiators-welcome-Council-negotiating-brief.

4. *See* European Parliament Resolution of 29 October 2015 on the Follow-Up to the European Parliament Resolution of 12 March 2014 on the Electronic Mass Surveillance of EU Citizens, EUR. PARL. DOC. 2015/2635 (RSP) (2015), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0‡OC+XML+V0//EN.

5. *See* Second Report on the Proposal for a Directive of the European Parliament and of the Council on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offenses and Serious Crime, COM (2011) 0032 – C7-0039/2011 – 2011/0023 (COD), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2015-0248+0‡OC+XML+V0//EN.

6. *See* European Data Protection Supervisor Press Release EDPS/ 2015/08, EU PNR: EPDS Warns Against Unjustified and Massive Collection of Passenger Data (Sept. 25, 2015), *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2015/EDPS-2015-08-EDPS_PNR_EN.pdf.

Parliament) of April 30, 2015, the Council reached an understanding with the Parliament on June 29, 2015, on the main principles to be included in the proposed Directive on Measures to Ensure a High Level of Network and Information Security Across the EU (EU-2013-0027 (COD)),[7] which would provide, *inter alia*, for the creation of Internet and telecommunications security coordinators at the national level. Conclusive agreements to further refine the proposal, paving the way for enactment of a definitive "NIS Directive," are in the making in the second part of 2015.

On October 27, 2016, the European Parliament finally voted to approve another agreement reached in June 2015, to end roaming charges by the end of 2017 and to adopt net neutrality,[8] though some commentators have expressed criticism over the supposed "vagueness" of the net-neutrality principles as worded in the Parliament's resolution.

4. *The "Umbrella Agreement"*

The EU-US Framework Agreement on the protection of personal data when transferred and processed for law enforcement purposes (EU 2015-2645 (RSP)) was signed after four years of transatlantic negotiations on September 9, 2015; it provides strong protection for EU citizens and is based on reiterating and extending the principles of legitimacy of purpose, legality, necessity, and proportionality.[9] Further, and importantly, it introduced the possibility of judicial redress for EU citizens before the United States courts in the event of any violation and/or misuse of their personal data. The Judicial Redress Act of 2015, which purports to comply with the umbrella agreement by ensuring the standing of EU citizens to sue in United States courts for privacy violations, was signed into law by U.S. President Barack Obama on February 24, 2016.[10]

5. *Mass Surveillance*

As the most recent effect of the outcry caused in Europe by the Snowden disclosures, the European Parliament Resolution of October 29, 2015 (2015-2635 (RSP)) on the Follow-Up to the EP Resolution of 12 March 2014 on the Electronic Mass Surveillance of EU Citizens strongly emphasized the requirements of necessity, proportionality, and legitimacy of objective for any restriction on encryption and anonymity.[11] The resolution recalled the decision of the European Court of Justice of April 8, 2014, which invalidated the "Data Retention Directive" (2006/24/EC), and followed from, among various other resolutions, the Motion for a Resolution introduced by the Parliament's Committee on Civil Liberties, Justice and Home Affairs on October 23, 2015.

---

7. *See Improving Cyber Security across Europe*, EUR. COUNCIL, www.consilium.europa.eu/en/policies/cyber-security (last visited Apr. 17, 2016).

8. *See New Rules on Roaming Charges and Open Internet*, EUR. COMM'N (Oct. 27, 2015), https://ec.europa.eu/digital-single-market/en/news/new-rules-roaming-charges-and-open-internet.

9. *See* Press Release, Eur. Comm'n, Questions and Answers on the EU-US Umbrella Agreement (Sept. 8, 2015), *available at* http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.

10. Judicial Redress Act of 2015, Pub. L. No. 114-126 (2016), *available at* https://www.congress.gov/bill/114th-congress/house-bill/1428/text.

11. *See* EUR. PARL. DOC. 2015/2635 (RSP), *supra* note 4.

6. *Post-Schrems*

Following the landmark decision of the European Court of Justice, discussed below, which invalidated the so-called "Safe Harbor" avenue for data transfers between the EU and the United States, the European Commission issued, on November 6, 2015, a Communication to the European Parliament and Council (COM 2015-0566), essentially confirming the availability of the other two main tools for legitimate transfers of EU citizens' personal data to other countries under Article 26(4) of the Data Protection Directive, namely, the Standard Contract Clauses (SCC) and the Binding Corporate Rules (BCC) for "intra-group" transfers—*i.e.* between subsidiary companies of the same multinational holding company.[12]

Furthermore, the Commission committed to making all possible efforts aimed at a novel arrangement with the United States, which would ensure the "adequacy" of transferred data protection, called for by the ECJ.

B. Court Decisions and Advisory Guidance

In light of the extraordinary relevance of the ECJ judgment in the aforementioned *Schrems* case,[13] this contribution dedicates a significant part of its focus to reviewing it.

The EU-US "Safe Harbor" program was set up by the United States Department of Commerce in 2000, and was considered by the EU Commission as ensuring the "adequate level of protection" mandated by Articles 25 and 26 of Directive 95/46.[14] The scheme is of a self-regulatory nature, in essence based on a series of standard measures that companies involved in data transfers from the EU guarantee to put in place so as to provide the same level of personal data protection as that enjoyed in the EU.

Plaintiff Schrems's core argument in his original complaint with the Irish Data Protection Authority was that, after Snowden, the United States clearly could not ensure the adequate protection of his personal data, and thus he objected to their transfer by Facebook Ireland to Facebook Inc. in the United States under the Safe Harbor. The Irish DPA rejected the claim on the basis of the EU Commission's Decision of 2000 (the "Decision"). Schrems appealed to the Irish High Court, which referred two questions to the ECJ, asking whether national DPAs are indeed bound by the Commission's decision, or whether they may make an independent assessment of the adequacy of data protection.

In the ensuing proceedings, the ECJ Advocate General not only concluded that national DPAs are not bound by the Decision, but went much further, arguing that the Decision itself is not valid under EU law in that (a) the Safe Harbor's limits pertaining to national security and law enforcement are too wide/vague, and (b) the scheme does not provide any avenue of redress or independent review in instances of claimed violations.

---

12. *See* Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Shrems), COM (2015) 566 final (Nov. 6, 2015), *available at* http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20150566.do.

13. Case C-362/14, Schrems v. Data Prot. Comm'r, EU:C:2015:650, InfoCuria, http://curia.europa.eu/juris/liste.jsf?num=-_inline>362/14.

14. 2000 O.J. (L 2015) 7, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

The Court by and large concurred with the Advocate General's arguments, finding that (a) the Decision could not eliminate, or limit, the national DPAs' independent powers of scrutiny in the matter of adequacy, and (b) that the Decision is, in any event, invalid because the Commission had never engaged in an analysis of the adequacy of United States privacy-protection law—*i.e.* whether it is "essentially equivalent" to the EU standard—and, furthermore, United States authorities are not subject to the Safe Harbor scheme.

The far-reaching effects of returning all powers of adequacy-assessment to each national DPA on a potentially case-by-case basis could not be overstated.

The judgment has also prompted the Working Party 29 (WP 29)—the permanent advisory body composed of all the national DPAs and the European Data Protection Supervisor—to issue a statement, on October 16, 2015, providing guidance on the fact that transfers of data could not be effected any longer on the basis of the invalidated Decision and that both alternative tools, the Standard Contract Clauses and the Binding Corporate Rules, could be used in the meantime to transfer personal data, though independent DPAs' assessment may also be applied.[15]

WP 29 further called for the institutions of the EU to engage with no delay in negotiations with the United States for legal and technical solutions, not excluding a Safe Harbor II.[16] Failing to achieve progress may translate, as soon as January 2016, into possibly coordinated enforcement action by the DPAs.

C. Conclusions

While the ECJ *Schrems* decision's consequences on thriving transatlantic trade may result in complicated outcomes, all the 2015 developments in this area of the law, read in careful comparative context, seem to unequivocally point to not only the profoundly different philosophical and legal views on privacy on the two rims of the Atlantic,[17] in desperate need of some form of pragmatic harmonization, but also to the more basic issue of the scramble to strike a tenable balance between national (and international) security and civil liberties.

II. Developments in Russia

The legal framework for data protection in Russia is established by the Federal Law on Personal Data No. 152-FZ dated July 27, 2006 (Law 152-FZ).[18] This law is largely based on Directive 95/46/EC of the European Parliament and Council; however, it has its own specifics. For instance, Law 152-FZ does not distinguish between "data controllers" and

15. *See* Press Release, Eur. Comm., Statement of the Article 29 Working Party (Oct. 16, 2015), *available at* ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

16. *Id.*

17. Even though, "[t]here are myriad ways in which the two regions reflect a similar approach." *See* Laura K. Donohue, *High Technology, Consumer Privacy, and U.S. National Security*, 4 Am. U. Bus. L.R. 11 (2015).

18. Federal'nyi Zakon RF o Personal'nykh Dannykh [Federal Law of the Russian Federation on Personal Data], Sobranie Zakonodatel'stva Rossiiskoi [SZ RF] [Russian Federation Collection of Legislation] 2006, No. 152-FZ, *available at* https://iapp.org/media/pdf/knowledge_center/Russian_Federal_ Law_on_Personal_Data.pdf.

"data processors" and refers to both of them as "data operators," providing common rules and restrictions for collecting and processing personal data.[19]

The term "personal data" is defined broadly, and it includes any information pertaining to a particular or identifiable individual (a "data subject"), including his or her last name; first name; patronymic; year, month, date, and place of birth; address; marital, social, and financial status; education; profession; income; and other information.[20] A higher level of protection applies to special categories of personal data concerning race, nationality, political opinions, religious or philosophical beliefs, health status, or intimate life.[21] Law 152-FZ does not contain any definition of employee data, but Chapter 14 of the Russian Labor Code includes specific provisions on collecting and processing such data.[22]

Similarly to most data protection laws, the provisions of Law 152-FZ revolve around the following areas: compliance with administrative requirements (governmental notification about data processing is generally required);[23] implementation of appropriate data-security measures; clear and transparent data-collection and processing practices (notice to data subjects and/or their consent to data processing are required, subject to some exceptions); and restrictions on cross-border data transfers.

Personal data can be freely transferred from Russia to Strasbourg Convention member countries.[24] Additionally, nineteen more countries (e.g., Australia and South Korea) are recognized by the local data-protection authority, *Roskomnadzor*, as providing an adequate level of data protection.[25] Cross-border transfers to other countries are allowed in limited cases, in particular, if an individual provides written consent to such data transfer or if it is necessary for the performance of an agreement with an individual.

On September 1, 2015, amendments to Law 152-FZ came into force establishing data-localization requirements for personal data collection and processing in Russia.[26] Going forward, data operators are obliged to ensure the recordation, systematization, accumulation, storage, clarification (via update or change), and extraction of personal data of Russian citizens through the use of databases located in the territory of the Russian Federation. Only after meeting such requirements, may personal data of Russian citizens be transferred abroad in accordance with the cross-border data-transfer rules provided in Law 152-FZ.

---

19. *Id.*

20. *Id.* at art. 3(1).

21. *Id.* at art. 10(1).

22. *See* TRUDOVOI KODEKS ROSSIISKOI FEDERATSII [TK RF] [Labor Code], Ch. 14, *available at* http://www.ilo.org/dyn/natlex/docs/WEBTEXT/60535/65252/E01RUS01.htm#sec13.

23. The Federal Service for Supervision of Communications, Information Technologies and Mass Media, or Roskomnadzor, is an authorized data-protection authority in Russia. *See* FED. SERV. SUPERVISION COMM., INFO. TECH., & MASS MEDIA, http://eng.rkn.gov.ru/ (last visited Apr. 17, 2016).

24. *See* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Eur. Council, Jan. 28, 1981, .E.T.S. No. 108, *available at* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

25. Roskomnadzor Order No. 274 (Mar. 15, 2013), *available at* http://digital.di.dk/SiteCollectionDocuments/privacy/Countries%20that%20provide%20an%20adequate%20level%20of%20protection.pdf.

26. [Federal Law on Amendments to Certain Legislative Acts of the Russian Federation for Clarification of the Procedure of Personal Data Processing in Information and Telecommunication Networks] SZ RF 2014, No. 242-FZ.

Noncompliance with Russian data protection laws by data operators can lead to penalties, from monetary fines to blocking access to their website for Russian users.

III. Developments in the United States

Privacy, e-commerce, and data-security law continues to develop rapidly in the United States, though with high variability among states, indecision over federalization, and escalating court challenges. At the time of this writing in autumn 2015, government and business leaders are in disarray since the collapse of the US-EU Safe Harbor program, and a way forward remains elusive.

A. Legislative Action

High-profile data breaches motivated legislators to innovate. A broad range of breach-notification legislation now comprises statutes in forty-seven states, fourteen of which allow private causes of action, and more than thirty bills were introduced in 2015.[27] Other privacy measures have appeared nationwide in characteristic patchwork, though California, the most populous state, remains at the vanguard. Numerous bills in Congress suggest that federal legislation is inevitable, though no showpiece statute has yet passed.

Effective in 2015, amendments to California law heightened data protection. One law intensified breach-reporting requirements and extended data-protection regulation to entities that "maintain," as opposed to merely own or license, personal information.[28] Another law effected a limited right of erasure, compelling electronic service providers to remove content publicly posted by a registered minor upon the minor's request, with some exceptions.[29] The law challenges the conventional United States wisdom that a right of erasure is incompatible with free expression.

A spate of newly enacted California laws, effective 2016, signal state entrenchment in privacy regulation. In the public sector, landmark warrant requirements confront law enforcement,[30] while the private sector faces technical specifications for breach notifications, enhanced encryption standards, drone overflight restrictions, and privacy protection for automatically harvested license plate numbers and smart-TV voice recordings.[31]

At the federal level, the White House sparked discussion with a redrafted Consumer Privacy Bill of Rights.[32] Contingent on commerce, the draft defines privacy contextually

27. Baker & Hostetler, Data Breach Charts (2015), http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf; NCSL, *Security Breach Notification*, Nat'l Conf. of State Legs., http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Jan. 4, 2016); *2015 Security Breach Legislation*, Nat'l Conf. of State Legs., http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx (last updated Dec. 31, 2015).

28. 2014 Cal. Legis. Serv. ch. 855 (A.B. 1710) (amending Cal. Civ. Code §§ 1798.81.5, 1798.82, 1798.85).

29. Cal. Bus. & Prof. Code § 22580 (2015).

30. 2015 Cal. Legis. Serv. ch. 651 (S.B. 178).

31. 2015 Cal. Legis. Serv. chs. 521 (A.B. 856), 522 (A.B. 964), 524 (A.B. 1116), 532 (S.B. 34), 543 (S.B. 570).

32. Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, *available at* https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

and charges the FTC with enforcement. Congressional bills do not go as far, but contemplate federalization of breach notification, which industry desires, and cybersecurity enhancement through public-private information sharing, which privacy advocates distrust.[33]

B. Regulatory and Related Court Action

The FTC kept busy in 2015 with a burgeoning mound of breach settlements. The commission also finalized settlement with TRUSTe over privacy certification misrepresentation, sustaining government faith in industry regulation premised on voluntary commitments.[34] The commission continued to wrestle in court with industry giant AT&T after fining the company a record $100 million for throttling mobile data traffic.[35]

In the most anticipated court decision of the year in this area, the FTC prevailed against the Wyndham hospitality group in an enforcement action concerning compromised consumer credit data.[36] At issue were not the merits, but whether the vague mandate of the FTC Act, to police unfair trade practices, authorized cybersecurity regulation. The court's affirmative answer is crucial to FTC oversight in data protection going forward, especially if the US-EU Safe Harbor is to be reconstructed.

Other agencies sought a piece of the action. Running the political football, the FCC effected nationwide net neutrality by bringing broadband into common carrier regulation.[37] The FAA proposed drone restrictions that would hamper delivery for e-merchants by requiring line-of-sight operation.[38] And the Librarian of Congress authorized copyright exemption for software "jailbreaking" on vehicle systems for repair and modification, and on devices such as smartphones and TVs for application interoperability.[39]

IV. Developments in Latin America

A. Mexico

1. *Overview*

On May 5, 2015, the Federal Institute of Access to Information and Data Protection announced a change of its name to the National Institute of Transparency, Access to Information and Data Protection (hereinafter as the "INAI" for its acronym in Spanish).[40]

33. S. 177, 114th Cong. (as introduced in Senate Dec. 8, 2015); S. 754, 114th Cong. (as passed by Senate Oct. 27, 2015).

34. *In re* True Ultimate Standards Everywhere, No. C-4512 (F.T.C. Mar. 12, 2015).

35. *See* FTC v. AT&T Mobility LLC, 87 F. Supp. 3d 1087 (N.D. Cal. 2015).

36. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

37. Protecting & Promoting Open Internet, GN Dkt. No. 14-28 (F.C.C. Mar. 12, 2015).

38. Operation and Certification of Small Unmanned Aircraft Systems, Dkt. No. FAA-2015-0150 (F.A.A. Feb. 15, 2015).

39. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65944 (Oct. 28, 2015) (to be codified at 37 C.F.R. pt. 201).

40. *See* IFAI Cambia de Nombre a INAI; Hoy Entró en Vigor la Ley General de Transparencia, INAI-OA/001/15, 5-5-2015, *available at*, http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-001-15.pdf.

This change of name arose from the publication of the General Law of Transparency and Access to Public of Information (hereinafter as the "LGTAIP" for its acronym in Spanish) on that same date, in the Mexican Official Gazette. One of the objectives the INAI wants to achieve with this change is to consolidate itself as the transparency, access-to-information, and data-protection guarantor at the national level.[41]

2. *Legislation*

With respect to legislation, the INAI has urged the approval of a new proposed law, the "General Law on the Protection of Personal Data held by Obligated Subjects."[42] This proposed law aims to be applied to the public sector, namely authorities, entities, organs, and organisms of the executive, legislative and judicial powers, as well as political parties, trusts, and public funds. Even though this law is still under discussion and remains only in draft form, on October 8, 2015, the INAI emphasized the importance of its approval because it would enact international standards on privacy and data protection in order to assure the effective processing of personal data by the public sector.[43] Accordingly, Commissioner Acuñas Llamas mentioned that this law is applicable in both the public and private sectors because it intends to unify the principles already set forth in the Federal Law on the Protection of Personal Data held by Private Parties (hereinafter as the "LFPDPPP" for its acronym in Spanish) published in 2010.[44]

3. *Case Law*

Earlier this year the INAI rendered its most popular decision to date, *i.e.*, a decision against Google,[45] the search-engine provider, affirming the so-called "right to be forgotten".[46] In this decision, the INAI announced that Google México had engaged in several violations of the Federal Law on the Protection of Personal Data held by Private Parties.[47] Google México's arguments were that the Mexican company was not the one that provided the search engine service, but rather it was Google Inc., an American company, that did; and therefore, the personal-data legislation could not be applied in this particular situation.[48] Notwithstanding Google's arguments, the INAI held that (i)

41. *Id.*

42. *See* Urge Apropbar Ley General de Protección de Datos Personales en Poder de Sujetos Obligados, INAI/134/15, 8-10-2015, *available at* http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-134-15.pdf.

43. *Id.*

44. *See* Urgente, Una Ley General Para Garantizar a Plenitud la Protección de los Datos Personales: Acuña Llamas, INAI/087/15, 4-9-2015, *available at* http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-087-15.pdf.

45. Expediente PPD.0094/14, Google México, S. de R.L. de C.V. (Jan. 27, 2015), *available at* http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf.

46. *See* La Protección de los Datos Personales, Responsabilidad Compartida: Ximena Puente de la Mora, INAI/003/15, 7-5-2015, *available at* http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-003-15.pdf.

47. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (DOF 05-07-2010) [LFPDPPP], Diario Oficial de la Federación [DOF] 05-07-2010 (Mex.).

48. *See* En un Hecho Sin Precedente, El IFAI Inició un Procedimiento de Imposición de Sanciones en Contra de Google México, IFAI-OA/009/15, 21-1-2015, *available at* http://inicio.ifai.org.mx/Comunicados/Comunicado%20IFAI-009-15.pdf.

Google México is a legally established company in Mexico, and therefore, in terms of the LFPDPPP, Google México is a data processor; (ii) one of the activities contained in the articles of incorporation of Google México is the provision of search-engine services; (iii) Google México does process personal data when an individual writes any type of information concerning a data subject into his or her search engines; and (iv) Google México failed to prove that the search-engine service was provided by a third party.[49] Without doubt, this resolution established a major precedent in Mexico, which followed the criteria applied by the ECJ in *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos.*[50]

4. *Data Processing in Relation to Extrajudicial Collection*

Earlier in 2015, the INAI also released the "Guide for Proper Data Processing in Extrajudicial Collection Activities."[51] This guide sets forth the data-processing principles that debt-collection agencies involved have to follow. Furthermore, with this guide the INAI explains the role that collection agencies have with respect to the LFPDPPP, namely, whether a collection agency acts as a data controller or as a data processor. In particular, a collection agency acts as a data controller when there is a transfer of personal data arising from the sale of expired accounts or portfolios. On the other hand, a collection agency acts as a data processor when these agencies offer only collection services and act in the name of the data controller.[52]

B. ARGENTINA

The main data privacy regulations enacted in Argentina during 2015 were related to the use of technology for personal data collection.

1. *Closed-Circuit Television Cameras*

In February 2015, the Argentine Data Protection Agency (the "ADPA") enacted Disposition 10/2015 (the "CCTV Disposition"), which regulates—from a data privacy perspective—the use of closed-circuit television cameras (CCTVs) for security purposes.[53]

The resolution establishes principles and guidelines for the collection of personal data via CCTVs. It mandates that such data must be collected while guaranteeing (a) the appropriate quality of data collection; and (b) the right of data subjects to be informed about the main characteristics of the data collection and the requirement to obtain their prior consent.

49. *Id.*

50. *See* Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Proteccio'n de Datos (AEPD), EUR-Lex (May 13, 2014), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131.

51. *See* IFAI, GUÍA PARA ORIENTAR EL DEBIDO TRATAMIENTO DE DATOS PERSONALES EN LA ACTIVIDAD DE COBRANZA EXTRAJUDICIAL (2015), http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Cobranza_Extrajudicial_IFAI.pdf.

52. *Id.*

53. Disposición 10/2015, Ministerio de Justicia y Derechos Humanos, Dirección Nacional de Protección de Datos Personales (Feb. 24, 2015), *available at* http://www.infoleg.gob. ar/infolegInternet/anexos/240000-244999/243335/norma.htm.

The quality requirement establishes that the data collected via CCTVs must be adequate, relevant, and not excessive in relation to the purpose of its collection.

The data collector can satisfy the right to be informed by placing signs informing people that CCTVs are being used. The signs must contain at least the following information: (a) the name of the entity responsible for maintaining the database of the recorded information; (b) its address; (c) its telephone number; and (d) its email address. A model sign is provided as an annex to the CCTV Disposition.

The requirement of prior consent is waived in certain circumstances, including when the CCTVs are used within the private property—and perimeter—of the data collector. Consequently, companies using CCTVs to monitor the activities carried out in their facilities are not expected to obtain data subjects' prior consent for collecting their images.

Moreover, the CCTV Disposition establishes that CCTV databases must be registered with the ADPA. The registration procedure includes the obligation to submit a policy for treating the data obtained via CCTV. The policy must at least provide the following information: (a) the method of collecting the data; (b) the places, dates, and times when and where the CCTVs operate; (c) the data retention period; (d) the security and confidentiality measures to be implemented regarding the CCTV database; (e) the measures to be implemented to guarantee the data subject's access, modification and deletion rights; and (f) if pictures are taken of individuals who enter the building, an explanation of the justification for such procedure.

2. *Drones*

In May 2015, the ADPA enacted Disposition 20/2015, which regulates the use of drones for collecting personal data (the "Drones Disposition"), turning Argentina into one of the first countries outside the EU to regulate drone usage from a data-privacy perspective.[54]

The Drones Disposition establishes that the collection of personal data with these devices requires the data subject's prior consent. However, so long as the collection does not constitute a disproportionate invasion to the subject's privacy, prior consent shall not be required (a) when the data are collected during a public act or are related to an occurrence of public interest; (b) when the data are collected during a private event in which it is customary to collect private images (*e.g.* wedding parties); (c) when the data are collected by the state; and (d) when the data are collected while providing assistance at accidents.

Moreover, the Drones Disposition obliges data collectors to draft a policy for drone usage and register their databases with the ADPA. The policy must contain at least the following information: (a) purpose of the collection; (b) the places, dates, and times when and where the drones are to be used; (c) the data-retention period; (d) the security and confidentiality measures to be implemented; (e) the methods to be used for anonymizing the personal data; and (f) the measures to be implemented to guarantee the data subjects' access, modification, and deletion rights.

54. Disposición 20/2015, Ministerio de Justicia y Derechos Humanos, Dirección Nacional de Protección de Datos Personales (May 5, 2015), *available at* http://www.infoleg.gob.ar/infolegInternet/anexos/245000-249999/247311/norma.htm.

Lastly, the Drones Disposition contains certain guidelines to be followed by drone users. It establishes that third-party privacy rights must be respected when using drones for recreational purposes. Moreover, the drone user must avoid accessing third parties' private spaces, such as windows, gardens, terraces, or other private property, unless previous authorization of access has been granted. During drone usage, the user must avoid collecting sensitive data.[55] Consequently, drones shall not be used to collect personal data in health or religious facilities, or at strikes or other labor or political gatherings.

C. Brazil

In light of the global spying disclosed by Edward Snowden, data protection became one of the major concerns worldwide, and in Brazil, it was no different. Although Brazil already has established general principles and legal provisions related to data protection and privacy, as provided in the Federal Constitution, the Brazilian Civil Code, the Consumer Defense and Protection Code, and other laws, it was imperative that specific legislation on the subject be enacted.

The Brazilian Federal Constitution considers the right to privacy and intimacy to be a fundamental right to which every citizen is entitled, in every situation, limited only by other fundamental rights such as freedom of speech.[56] These rights authorize individuals to take legal action to enforce the protection of their personal information. Therefore, compensation can be claimed for damages caused by violation of these rights.

The Civil Code states that privacy and intimacy are inviolable rights, and the judiciary, upon request, can adopt any necessary means to impede or prevent any act in contravention of this protection.[57]

The aforementioned Consumer Defense and Protection Code established that a consumer has the right to access all personal information regarding him/her (as well as the respective sources), contained in registries, databases, etc.[58] The consumer also has the right to be informed of the processing of data relating to him or her, the inclusion of such personal data in a registry, or the opening of an entry containing such personal information in a database.

The recently enacted Brazilian Internet Act (Marco Civil da Internet) deals specifically with issues affecting the collection, maintenance, treatment, and use of personal data on the Internet.[59] It became effective on June 23, 2014. The Brazilian Internet Act ratifies the general privacy principles provided in the Brazilian Consumer Protection and Defense Code (that is, the collection and use of personal data require the data subject's prior and express consent).

The Act sets out principles for the use of the Internet, as well as the rights of Internet users and the duties of (1) Internet-connection providers and (2) Internet-application

55. *See id.* at Annex II(f) (defining "sensitive data" as data revealing racial or ethnic origin; religious, political, philosophical, or moral opinions; union affiliation; and information related to health or sexual life).

56. *See* Constituição Federal [C.F.] [Constitution] art. 5.

57. *See* Código Civil [C.C.] art. 20.

58. *See* Código de Proteçao e Defesa do Consumidor [C.D.C.] art. 43.

59. *See* Lei No. 12.965, de 23 de Abril de 2014, Diário Oficial da União [D.O.U.] de 24.4.2014.

providers. The Act establishes standards for Internet usage in Brazil, including general principles for the protection of privacy and personal data.

For the purposes of data-privacy regulations, we understand personal data as any data that can be used to identify an individual (for example, the name of the individual and his or her ID and taxpayer numbers).

The Internet Civil Rights Legal Framework provides for administrative liability (with penalties that vary from warnings to prohibition of processing personal data) if a legal entity does not follow the requirements of the statute. Other sectoral regulations (as in telecommunication, technology, and aviation) also provide for civil, criminal, and administrative liability for unlawful data processing through the governmental agencies that regulate these sectors.

In general, the framework of laws and regulations currently in force that establish general principles and requirements regarding data protection, requires that all individuals and legal entities handle personal data with the utmost care, and in compliance with the rights to privacy, protection of personal data, and secrecy of private communications.

V. Developments in the Asia-Pacific region

A. China

In China, there is currently no comprehensive legal framework to regulate the use and disclosure of personal data and no national-level law that delineates how a company can legally collect, process, and retain personal data. But China has a number of diverse laws and regulations referring to the right of privacy. Most recently, on July 6, 2015, the Standing Committee of the National People's Congress of the People's Republic of China published a draft for China's proposed Network Security Law.

The right to privacy is already given great significance in Chinese law, and that right is specifically upheld by the Civil Law Principles and the PRC Constitution, which provide that a citizen's personal dignity is protected as a fundamental right. Other major relevant laws include the following:

(a) Consumer Rights Protection Law;

(b) Regulation on Personal Information Protection of Telecom and Internet Users;

(c) Administrative Measures for Online Transactions;

(d) Personal Information Security Measures for Mailing and Courier Services;

(e) Medical Records Administration Measures of Medical Institutions; and

(f) Measures for Administration of Population Health Information (the "PHI Measures").

Furthermore, in March 2015, the State Administration for Industry and Commerce (the "SAIC") made effective the Measures for the Punishment of Conduct Infringing the Rights and Interests of Consumers, which seeks to supplement the Consumer Rights Protection Law and to provide for the protection of consumers' rights and interests. In particular, Article 11 provides a list of actions enterprises may not undertake due to their infringement of users' rights in their personal information, and further provides a list of

specific examples of types of consumer personal information, including a consumer's name, gender, occupation, birth date, identification card number, residential address, contact information, and income and financial status.

The Network Security Law seeks to complement this collection of legislation. It aims to ensure network security, to protect the lawful rights and interests of legal persons, and to promote the healthy development of economic and social informatization. In its current form, the law will apply broadly to entities that construct, operate, maintain, and use networks within China, as well as to those who supervise and manage network security. Therefore, it will be likely to have a significant impact on information technology and communication companies in China.

The Network Security Law provides for the protection of network data, which are the different types of electronic data collected, stored, transmitted, and processed through networks. Such provisions apply to all network operators, which have been broadly defined to ensure obligations are imposed on all relevant persons. The law's requirements include the following:

> (a) the collection and use of personal information must comply with the principles of legality, legitimacy, and necessity; the purpose, method, and use of the personal information must be disclosed and based on consent; the use of personal information must be for the provision of services only; and individuals must be aware of the relevant policies;[60]
> (b) individuals have the right to have their personal information remain strictly confidential, and to not be disclosed, distorted or damaged, offered for sale, or illegally provided to others;[61]
> (c) individuals have the right to demand the disposal, removal, or destruction of their collected personal information, and the correction of any inaccurate personal information.[62]

Further provisions regulate the responsibilities of network operators and include the following measures:

> (a) to strengthen management of the information published by users, and to stop transmission or employ appropriate treatment measures when network operators discover publication or transmission of certain information that the law or administrative regulations prohibit;[63] and
> (b) to establish a network-information-security complaint and reporting system.[64]

The Network Security Law provides for penalties for noncompliance, which include warnings, rectification orders, fines or the confiscation of illegal gains, and the suspension of the business or revocation of the business license. Specifically, network operators who infringe upon the protections and rights of citizens are ordered to make corrections and

60. Draft Network Security Law of the People's Republic of China (promulgated by the Standing Committee of the 12th Nat'l People's Congress, July 6, 2015) art. 35 (2015), *translated at* CHINA L. TRANSLATE (July 6, 2015), http://chinalawtranslate.com/cybersecuritydraft/?lang=EN.
61. *Id.* art. 36.
62. *Id.* art. 37.
63. *Id.* art. 40.
64. *Id.* art. 42.

may be fined between one to ten times the amount of unlawful gains, or RMB 500,000 where there are no unlawful gains, or RMB 50,000 to 500,000 where the circumstances are serious.[65]

Privacy is an important matter in contemporary society, especially with the advancement of technology and the risks it brings. Therefore, in order to maintain control over personal information while simultaneously gaining the benefits of technology, countries all over the world have sought to implement and regulate privacy protections for personal information in order to ultimately create an environment of trust and a culture of respect for personal information. The draft Network Security Law demonstrates China's ongoing effort to enhance the supervision of the Internet and telecommunication networks, and especially to protect data privacy.

B. South Korea

1. *Amendment to the Personal Information Protection Act (July 2015)*

Under the pre-amendment Personal Information Protection Act (PIPA), information subjects who are harmed by any violation of PIPA by a "personal information processor" (*i.e.*, a person or entity that possesses their personal information) had the burden to prove the specific amount of damages in order to be compensated. As amended, however, PIPA entitles such victims to claim statutory damages up to KRW 3 million for infringement of their data-privacy rights under PIPA (*e.g.* through leakage or misuse of their information) due to the misconduct or negligence of the personal information processor, and a court has discretion to award such damages without definite proof thereof, based on the totality of the evidence and argument (Article 39-2 of the amended PIPA).[66]

Furthermore, the amendment to PIPA has introduced punitive damages for infringement of data-privacy rights due to wilful misconduct or gross negligence, for which the court may award punitive damages not exceeding three times the amount of actual damages (Article 39(3) of the amended PIPA).[67] And based upon another newly introduced provision, any criminal proceeds acquired through illegal data leakage or distribution of personal information may be forfeited (Article 74-2 of the amended PIPA).[68]

Additionally, the Korea Communications Commission (the "KCC") partially amended its "Standards for Imposition of Penalties for Breach of Personal Information Protection Laws" in August 2015. Pursuant to this amendment, if a business voluntarily reports a leak of personal information, the KCC will reduce the penalty that it otherwise would impose by up to 30 percent, for the purpose of providing incentives for voluntarily reporting data breaches.

65. *Id.* arts. 54, 56.

66. This provision will come into force on July 25, 2016.

67. This provision will come into force on July 25, 2016.

68. This provision came into force on July 24, 2015.

2. *Amendment to the Protection, Use, Etc. of Location Information Act (August 4, 2015)*

Any person who intends to conduct location-based services in Korea must submit a report to the KCC under the Protection, Use etc. of Location Information Act (the "Location Information Act"), and any person failing to do so shall be punished by imprisonment for not more than three years or by a fine not exceeding KRW 30 million. In January 2015, the KCC filed a complaint against Uber charging a breach of this reporting obligation. In July 2015, Uber Korea and the representative of Uber Technology were indicted, and the relevant case is on trial.[69]

However, under the Location Information Act, as amended in August 2015, the obligation to submit a report for location-based services focusing only on the location information of objects (not personal location information) has been abolished, which provides a foundation for mobilizing a new industry using location information, such as the Internet of Things. In addition, the amended Location Information Act enables location-based-information service providers to inform personal-location-information subjects of all transfers to third parties of such personal-location information by regularly reporting them in thirty-day intervals, if they obtain consent from the personal-location-information subjects.[70]

3. *Information Protection Related to Cloud Services (September 2015)*

In line with a full-fledged enforcement of the Development of Cloud Computing and Protection of Users Act (the "Cloud Computing Act"), the Ministry of Science, ICT and Future Planning (the "MSIP") announced its "Government Measures on Information Protection for Fostering Cloud Services" in September 2015. For the protection of cloud-service users, the MSIP will include provisions such as those prohibiting the provision of information to a third party without the consent of users; requiring notification of any accident such as leakage of user information; requiring the return and destruction of user information upon termination of service; and providing for compensation for damages pursuant to the Cloud Development Act and its Enforcement Decree.

In addition, in order to protect cloud-service users from data losses due to any abrupt suspension of cloud services, the MSIP will introduce a system to keep the user's information with a third-party agency. Also the MSIP will introduce a method to secure interoperability between cloud services for the stable transfer of information between providers in the event that a user changes cloud service provider.

69. After the KCC filed its complaint, Uber Korea suspended its UberX service, and completed and filed with the KCC the required report for location-based business operators.

70. Under the former act, location-based-information service providers are required to immediately inform the personal-location-information subjects of the details of such personal location information every time they provide it to a third party.