Survey of Recent European Union Privacy Developments

W. Gregory Voss

Survey of Recent European Union Privacy Developments

*By W. Gregory Voss**

I. Introduction

During the past year, the European Union ("EU") witnessed important privacy developments. Certain of these developments, including a preliminary ruling on Spain's implementing legislation that added a condition to the processing of personal data, guidance on facial recognition and biometric technologies, and the meaning of consent, are discussed below. Other developments related to cookies, which are principally dealt with by telecommunications legislation rather than pure data privacy legislation, are addressed elsewhere in this year's Survey of Cyberspace Law.[1]

Proposals for new, more robust legislation at the EU level, which are briefly treated here, may lead to the replacement of the existing EU data protection framework[2]—already described as putting "stringent standards on the collection of electronic data by the government and by any other entity."[3] In this globalized world where information frequently travels across borders, the potential adoption of the proposed EU data protection legislation is of great importance to legal practitioners on both sides of the Atlantic.

II. Developments Under the Present System

A. Spanish Legislation

On November 24, 2011, the Court of Justice of the European Union ("ECJ") rendered its decision in two proceedings[4] that were referred to it for a preliminary

* Toulouse University, Toulouse Business School; Member of the Institut de Recherche en Droit Européen International et Comparé (IRDEIC), Toulouse, France.

1. *See* Robert Bond, *The EU E-Privacy Directive and Consent to Cookies*, 68 Bus. Law. 215 (2012).

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

3. William R. Denny, *Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement*, 66 Bus. Law. 237, 239 (2010). For a more extensive discussion of the Directive, see Ariane Siegel et al., *Survey of Privacy Law Developments in 2009: United States, Canada, and the European Union*, 65 Bus. Law. 285, 299–305 (2009).

4. Joined Cases, Case C-468/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) v. Administración del Estado, [2012] 1 C.M.L.R. 48 (Nov. 24, 2011); Case C-469/10, Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, [2012] 1 C.M.L.R. 48 (Nov. 24, 2011).

ruling by the Spanish *Tribunal Supremo* ("Spanish Supreme Court") on September 28, 2010. The two proceedings, one between the National Association of Credit Institutions ("ASNEF") and the Spanish State Administration, and the other between the Federation of Electronic Commerce and Direct Marketing ("FECEMD") and the Spanish State Administration, had been joined by the ECJ and involve an interpretation of Council Directive 95/46 ("Directive").[5]

In the joined cases involving ASNEF and FECEMD, the ECJ considered whether Spain had correctly implemented Article 7 of the Directive or whether in implementing Article 7 it had exceeded the limits of the Directive. Article 7 of the Directive provides that:

> Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or . . . (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).[6]

The Spanish legislation implementing the Directive added a condition to the processing of personal data in its Article 6(2), which is otherwise similar to Article 7(f) of the Directive, that data be in sources available to the public.[7] ASNEF and FECEMD each made administrative challenges to certain articles of the Spanish Royal Decree that was used to implement the Spanish legislation, on the ground that this condition to legitimate personal data processing, which did not exist in the Directive, had been added.[8]

The ECJ ruled that this national legislation, which adds the requirement that "the data should appear in public sources," is precluded by Article 7(f) of the Directive, which has direct effect.[9] Thus, litigants have grounds for challenging national laws that "impose additional requirements that have the effect of amending the scope of one of the six principles provided for in [Article] 7."[10] Article 7(f) "may be relied on before the national courts by individuals against the State where the latter has . . . failed to implement that directive correctly,"[11] as was the case with the challenges by ASNEF and FECEMD.

In its discussion of one of the questions referred to it, the court cited by analogy *Productores de Música de España (Promusicae) v. Telefónica de España SAU* for the proposition that in the transposition of the Directive member states must "take care to rely on an interpretation of [the Directive] which allows a fair balance to be struck between the various fundamental rights and freedoms pro-

5. *Id.* ¶ 2.
6. *Id.* ¶ 6 (quoting Directive, *supra* note 2, art. 7(a), (f)). The "controller" is the party that "determines the purposes and means of the processing of personal data." Directive, *supra* note 2, art. 2(d) (defining "controller").
7. Organic Law 15/1999 on the Protection of Personal Data art. 6(2) (B.O.E. 1999, 298) (Spain); *ASNEF*, [2012] 1 C.M.L.R. 48, ¶ 10.
8. *ASNEF*, [2012] 1 C.M.L.R. 48, ¶¶ 15–17.
9. *Id.* ¶ 49.
10. *Id.* ¶ 32.
11. *Id.* ¶ 51.

tected by the EU legal order,"[12] but then the court emphasized that such balancing should be done on a case-by-case basis, and not in a "categorical and generalised"[13] manner, such as through the adoption of the challenged provisions of the Spanish national legislation.[14] As a result of this case, on February 8, 2012, the Spanish Supreme Court annulled part of the Spanish Royal Decree used to implement the Spanish legislation.[15]

Thus, harmonization of EU member state laws, generally a goal of directives, will be enhanced as a result of this decision relating to privacy. Harmonization, although not considered adequate today in the area of EU privacy law (as discussed in Part III.A. below), gives businesses some degree of comfort that they will be treated similarly when operating in different EU member states. Furthermore, this case also brings focus on the limited and exhaustive list of legitimate reasons for the processing of personal data contained in Article 7 of the Directive, as well as the necessity for firms subject to the provisions of the Directive to fit within one of those legitimate reasons, such as by obtaining unambiguous consent (as discussed in Part II.B.1. below).

B. EU Article 29 Working Party Guidance Under the Present System

The EU's Article 29 Working Party (the "WP29"), an independent advisory panel, gives guidance on privacy directives to member states, which then can be used by member state data protection agencies or legislators.[16] The guidance may also be referred to by practitioners to anticipate member state application of the Directive to new issues, such as those raised by data processing for new uses or using new technologies.

Three of the various areas on which the WP29 gave guidance the past year are addressed below:

1. Consent

The meaning of consent impacts both the Directive and the ePrivacy Directive.[17] This survey is limited to the former.

12. *Id.* ¶ 43 (citing Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-271, [2008] 2 C.M.L.R. 17). For a discussion of the *Promusicae* case, see Siegel et al., *supra* note 3, at 306.

13. *ASNEF*, [2012] 1 C.M.L.R. 48, ¶ 48.

14. *Id.* ¶¶ 43–49.

15. S.T.S., Feb. 8, 2012 (No. 429) (Spain), *available at* http://www.poderjudicial.es/search/sentencias/proteccion%20de%20datos%20de%20caracter%20personal/1/PUB. For a discussion of this annulment in English, see Belén Gámez, *Spanish Supreme Court Annuls Limitation on Processing of Personal Data*, Hogan Lovells Chron. of Data Protection (Feb. 29, 2012), http://www.hldataprotection.com/2012/02/articles/international-eu-privacy/spanish-supreme-court-annuls-limitation-on-processing-of-personal-data/.

16. *See Article 29 Working Party*, Eur. Commission, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last updated Feb. 3, 2012).

17. Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC) (Directive on Privacy and Electronic Communications, commonly known as the "ePrivacy Directive").

Under the Directive, consent is used as a basis for the lawfulness of data processing, and "explicit" consent is used to legitimize processing of "sensitive" data.[18] This consent must, as a general rule, be expressed prior to the beginning of the data processing and be unambiguous,[19] and the data processing must be transparent.[20]

Consent includes "any indication of a wish, by which the data subject *signifies* his agreement,"[21] whether by a handwritten signature, an oral statement, or behavior. In general, this behavior must be an action; that is, it cannot be inaction or "passive behaviour."[22]

The consent of the data subject must be "freely given"—not obtained through deception, coercion, intimidation, or risk of "significant negative consequences if he/she does not consent."[23] Certain categories of the processing of personal data may not be legitimized merely by consent, such as in the case where the data subject is in an employment relationship with the data controller, and thereby cannot freely withhold consent (absent "sufficient guarantees" that the consent is given freely).[24]

The purposes of data processing must be specified in order to obtain consent to such processing.[25] The consent can be accorded only for a limited set of data processing activities, although that may include different operations if "within the reasonable expectations of the data subject."[26]

Finally, the consent must be "informed."[27] The data subject must have information—such as his or her rights, the reasons for and nature of the data processing, and the identity of potential transferees of the data.[28] The information must be intelligible and accessible (not just "available" somewhere).[29]

Firms should ensure that consent for processing personal data is legitimate and adequate for the kind of data being processed. Sufficient, clear, and accessible information about the data processing must be given to data subjects. Businesses should review their privacy policies, contracts, general terms of use, and other documentation in this light.

18. *See* Article 29 Data Prot. Working Party, Opinion 15/2011 on the Definition of Consent 6 (July 13, 2011) (WP 187), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. The consent may be expressed through a handwritten or electronic signature or writing, or by oral agreement, but may not generally be inferred. *See id.* at 25. Opt-out procedures will not be considered explicit. *See id.*

19. In order to be unambiguous, there must be no doubt as to the intent of the data subject to give his or her consent. *Id.* at 21. This is achieved through the use of robust procedures and the retention of evidence of intent. *See id.*

20. *Id.* at 9–10.

21. *Id.* at 11.

22. *Id.* at 12.

23. *Id.*

24. *Id.* at 12–14.

25. *Id.* at 17–19.

26. *Id.* at 17.

27. *Id.* at 19.

28. *Id.*

29. *Id.* at 19–20.

2. Facial Recognition in Online and Mobile Services

The WP29's opinion on facial recognition in online and mobile services[30] refers to the relevant processing as one of using personal data (whether it be a digital image of a face or a "reference template" created from such an image and used for future identification and comparison), subject to the Directive.[31] As a result, the processing may occur only if "legitimate" within the context of Article 7 of the Directive.[32] Furthermore, the WP29 considered the particular risks associated with biometric data, and accordingly, generally requires "informed consent of the individual prior to commencing the processing of digital images for facial recognition,"[33] except in certain cases where there is a need for the data controller to perform some preliminary facial recognition processing—for example, in order to determine whether the data subject has given consent or not.[34]

Information regarding the facial recognition processing must be clear and easily available; consent must be specific prior to enrollment, unless it is clear that the service's primary purpose involves facial recognition.[35] The recommendations of the WP29 highlight the importance of the data controller ensuring the security of data during transit, including through encrypted communication channels or even encrypting individual images and templates.[36]

Special care must be taken when providing facial recognition services, and data security must be ensured. Specific prior informed consent to the processing generally should be required before providing such services.

3. Biometric Technologies

On April 27, 2012, the WP29 adopted its opinion on developments in biometric technologies.[37] The opinion emphasizes the specific danger of biometric technologies to data protection and privacy because of the linkage of the technologies to "certain characteristics of an individual."[38] The WP29 states that "biometric data are in most cases personal data,"[39] therefore subject to the Directive framework, and that they may be processed only if legitimate under the Directive.[40] In accordance with the Directive, biometric data subjects must know of

30. Article 29 Data Prot. Working Party, Opinion 2/2012 on Facial Recognition in Online and Mobile Services (Mar. 22, 2012) (WP 192), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf.

31. *Id.* at 4.

32. *Id.* at 5.

33. *Id.*

34. *Id.*

35. *Id.* at 7.

36. *Id.* at 8.

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

38. *Id.* at 3.

39. *Id.* at 7.

40. *Id.* at 10–13 (referencing the grounds for legitimacy).

the collection or use of their data, have access to it, and it must be properly secured.[41] The purpose of the biometric data processing must be clearly defined and limited, based on principles of proportionality (non-excessiveness), necessity, and "data minimization" (only the required information being processed).[42]

The WP29 underscores the importance of biometric data security, and recommends "a high level of technical protection for . . . processing [as well as the use of] privacy by design."[43] In addition to calling for a risk analysis or dedicated "Privacy Impact Assessment (PIA)" for biometrics systems conceived as part of the design stage by the party defining the purpose of the system (e.g., the manufacturer, integrator, or final client), the WP29 encourages the development of certification schemes.[44] Special risks relating to biometrics data that are to be analyzed in the PIA are identity theft, improper use of the data ("purpose diversion"), and data breaches.[45] The WP29 sets out different technical measures that may be adopted to protect against these risks (e.g., use of encryption technologies, storage of data on personal devices such as smart cards instead of centralized storage, and establishment of automated data erasure mechanisms to delete data no longer needed).[46]

Thus, because of the special nature of biometric technologies, which are closely linked to individuals' personal characteristics, the WP29 has emphasized the importance of data security, and has suggested various ways by which security risks may be addressed.

III. Legislative Proposals

On January 25, 2012, Viviane Reding, EU Justice Commissioner and Vice President of the European Commission, introduced two proposed laws to reform the Directive framework[47]: (i) a proposed directive relating to data processing by authorities in connection with criminal matters,[48] and (ii) a proposed regulation relating to general data protection (the General Data Protection Regulation, hereinafter "GDPR").[49] This survey focuses on the latter.

41. *Id.* at 14.

42. *Id.* at 7–10.

43. *Id.* at 28. "Privacy by design" is defined as "the concept of embedding privacy proactively into technology itself." *Id.*

44. *Id.* at 29.

45. *Id.* at 30–31.

46. *Id.* at 31–33.

47. Press Release, Eur. Comm'n, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=1&language=EN&guiLanguage=en.

48. *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.

49. *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

The GDPR will interest non-EU practitioners and firms, as well as Europeans, as in its current form it would apply even to controllers not established in the EU, provided that they engage in data processing of EU residents' personal data, where such processing is related to the offer of goods or services in the EU or to behavior monitoring.[50] In such cases, a controller located outside of the EU may have to appoint a representative in the EU, who may be addressed on the controller's behalf by a supervisory authority, if the controller meets the criteria set out in the GDPR.[51] This is in addition to the obligation for certain controllers and processors of personal data, when required, to designate a data protection officer, who is either an employee or someone engaged by the controller or processor through a service contract.[52]

The GDPR, which may possibly come to a vote of the European Parliament in plenary session in early 2014, was proposed for various reasons, with some of the main ones summarized below.

A. Greater Harmonization

The fragmentation of EU personal data protection has been decried, often due to legal uncertainty, lack of harmonization, and complexity.[53] These perceived flaws are considered impediments to business in a globalized world.[54] A single legal instrument in the form of a regulation is thought to be the way to establish the necessary data protection framework and to harmonize the law while simultaneously allowing direct applicability throughout the EU.[55]

B. Dealings with One National Data Protection Authority

Article 51(2) of the proposed GDPR provides that, where a personal data controller or processor is established in more than one member state, "the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States."[56] The GDPR provides for cooperation and mutual assistance between supervisory authorities,[57] and would establish a "consistency mechanism," involving a European Data Protection Board.[58]

Thus, a controller or a processor would deal with their home supervisory authority, saving time and money, but consistency among the various authorities

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.

50. *Id.* art. 3(2), at 41.
51. *Id.* art. 25, at 56–57.
52. *Id.* art. 35, at 65–66.
53. *Id.* at 4.
54. *Id.*
55. *Id.* at 5–6. An EU regulation, unlike a directive, does not need to be implemented by each member state to become effective. *See id.* at 6.
56. *Id.* art. 51(2), at 77.
57. *Id.* arts. 55–56, at 80–82.
58. *Id.* arts. 57–63, at 82–86.

of the different member states would be ensured through a mechanism foreseen under the GDPR.

C. Increased Data Breach Requirements; Accountability and Responsibility

Several requirements are placed upon the data controller or processor, including the implementation of security measures and a notification requirement to the supervisory authority of personal data breaches "without undue delay and, where feasible, not later than 24 hours after having become aware of [any such breach]."[59] If notification occurs after twenty-four hours, a "reasoned justification" must be provided.[60] A processor must "alert and inform the controller immediately after the establishment" of a breach,[61] and a controller must communicate a breach to a data subject "without undue delay" if the breach is "likely to adversely affect the protection of the personal data or privacy of the data subject,"[62] but shall not be so required if it can prove to the supervisory authority's satisfaction that it had implemented protections rendering the data "unintelligible to any person who is not authorised to access it."[63]

Increased data breach requirements are just part of the increased accountability and responsibility requirements for personal data controllers under the GDPR; they include carrying out a data protection impact assessment, or obtaining prior authorization in certain circumstances, for example.[64]

D. Data Portability

Article 18 establishes a right to data portability, through allowing the data subject to obtain his or her personal data and transmit them into another data processing system in a commonly used electronic format, without hindrance.[65]

E. Right to Be Forgotten

The data subject has a right to require the controller to erase his or her personal data under certain grounds set out in Article 17(1), including where the data are no longer needed for the original purpose, where the data subject exercises his or her right to object, or where he or she "withdraws consent on which the processing is based."[66]

59. *Id.* art. 31(1), at 60.
60. *Id.*
61. *Id.* art. 31(2), at 60.
62. *Id.* art. 32(1), at 61.
63. *Id.* art. 32(3), at 61–62.
64. *Id.* arts. 33–34, at 62–64.
65. *Id.* art. 18(1)–(3), at 53.
66. *Id.* art. 17(1), at 51.

F. Increased Fines

Article 79 of the proposed GDPR would establish a sliding scale of fines based on whether one's first violation was "non-intentional non-compliance," and whether or not the violator is an enterprise (and then, whether or not a small enterprise).[67] The fine may be based upon the duration, nature, and gravity of the offense, and could reach a maximum of 2 percent of annual worldwide turnover for certain intentional or negligent breaches by an enterprise.[68] Thus, the proposed GDPR could result in sharply increased fines.

IV. Conclusion

Throughout the year developments in EU privacy law have tended to limit divergence from European law, to encourage convergence in the application of laws through guidance, or to update law by dealing with new technologies and uses of data processing. The proposed GDPR can be seen as a culmination of these trends, by allowing for potential unification of law, by incorporating many of the principles (e.g., transparency and data minimization) and advances developed through WP29 guidance, and by bringing the Directive (in a new form) into the twenty-first century. Firms should make an effort now to understand the proposed GDPR and to initiate relatively long lead-time measures (such as privacy by design, or certain security actions) in anticipation of the GDPR's possible application.

67. *Id.* art. 79, at 92–94.
68. *Id.*