After *Google Spain* and *Charlie Hebdo*: The Continuing Evolution of European Union Data Privacy Law in a Time of Change

*By W. Gregory Voss**

I. Introduction

The past year has seen various developments that are modifying data privacy law in the European Union (EU), with consequences for various sectors of business. Over a year ago, the Court of Justice of the European Union (ECJ) issued its now-famous *Google Spain* decision, recognizing a so-called "right to be forgotten."[1] This has been followed by EU member state court decisions raising issues for Internet search engines, publishers of information, and potentially other Internet intermediaries.[2] Coordinated European action with respect to Google's privacy policy, discussed in last year's survey,[3] has continued, with implications for other companies offering services that collect and process individual users' data on the web. Thus, while Google may seem to have been singled out in a year when that firm is also under European competition law scrutiny,[4] the lessons to be drawn are more broadly applicable.

* W. Gregory Voss is a Professor of Business Law at Toulouse University, Toulouse Business School and an associate member of the Institut de Recherche en Droit Européen International et Comparé (IRDEIC) in Toulouse, France.

1. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&rid=14.

2. *See generally* Press Release, Court of Justice of the European Union, An Internet Search Engine Operator Is Responsible for the Processing that It Carries Out of Personal Data Which Appear on Web Pages Published by Third Parties (May 13, 2014), http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (noting that national courts must dispose of cases in accordance with the decision of the ECJ, which decision is binding on the courts of member states).

3. W. Gregory Voss, *European Union Data Privacy Law Developments*, 70 Bus. Law. 253, 254–57 (2014).

4. On April 15, 2015, the European Commission opened a formal competition law investigation into Google's conduct in relation to its Android mobile operating system and sent Google a Statement of Objections on its comparison shopping service regarding alleged abuse of its dominant position. *See* Press Release, European Comm'n, Antitrust: Commission Sends Statement of Objections to Google on Comparison Shopping Service; Opens Separate Formal Investigation on Android (Apr. 15, 2015), http://europa.eu/rapid/press-release_IP-15-4780_en.htm. While not, strictly speaking a privacy law development, the antitrust investigation should be considered in conjunction with concerns that uses of personal data may be examined in the competition law context, after EU antitrust commissioner Margrethe Vestager's statement that "she's studying the U.S.'s 'stringent approach to dealing with personal data as a means to payment' in its review of deals." Aoife White & Peter Levring, *EU Deal Probes May Weigh Value of Personal Data: Vestager*, Bloomberg Bus. (Apr. 9, 2015, 11:09 AM),

In addition, threats of terrorism and the *Charlie Hebdo* terrorist attacks in Paris have led to a strengthening of police powers impacting Internet companies and raised calls for airlines in the EU to furnish information about their passengers to law enforcement authorities.[5] Finally, this survey addresses ongoing work on the EU data protection law reform proposals.[6]

II. *Google Spain* and the "Right to Be Forgotten": The Sequel

On May 13, 2014, the ECJ rendered its decision in the *Google Spain* case,[7] involving the request for a ruling by a Spanish court on points of EU law related to a lawsuit brought by Mr. Costeja González against Google Spain SL and Google Inc. The plaintiff sought a court order prohibiting the Google search engine from displaying, in response to a search of his name, a link to a 1998 article published in the Catalan newspaper, *La Vanguardia,* which disclosed that the plaintiff had been subject to a real-estate auction to satisfy his social security debts.[8] The ECJ ruled that an individual has the right to object to a search engine's linking to personal information about him, and that evaluation of such an objection calls for a balancing of rights and interests.[9] Criteria applicable to this balancing include the relevance or obsolescence of the data, whether there is a public interest in access to the data, and the published information's "sensitivity for the data subject's private life."[10]

As a result of the *Google Spain* decision, Google set up an online form allowing individuals to request exercise of this right.[11] As of August 12, 2015, Google received 294,977 delisting requests and deleted 58.7 percent (or approximately 628,102) of the 1,070,021 URL search engine results that the company examined as a result of the delisting requests.[12]

In addition, Google formed a council of experts that consulted with, among others, representatives of government, business, media, academia, the technology sector, and data protection organizations at seven hearings in certain European capitals from September through November 2014 in order to gather advice on how to handle delisting requests.[13] As a result of those hearings, the council

http://www.bloomberg.com/news/articles/2015-04-09/eu-deal-reviews-may-weigh-value-of-personal-data-vestager-says/.

5. *See infra* Part IV.

6. *See infra* Part V.

7. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&rid=14.

8. *Id.* at para. 14.

9. *Id.* at para. 100.

10. *Id.* at paras. 81, 98; *see* W. Gregory Voss, *The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation*, 18 J. Internet L. 3, 5 (2014).

11. *See Search Removal Request Under Data Protection Law in Europe*, Google, https://support.google.com/legal/contact/lr_eudpa?product=websearch/ (last visited July 28, 2015).

12. *See Transparency Report: European Privacy Requests for Search Removals*, Google, https://www.google.com/transparencyreport/removals/europeprivacy/ (last updated Aug. 12, 2015).

13. *See Advisory Council*, Google, https://www.google.com/advisorycouncil/ (last visited July 28, 2015).

issued a report, noting that the privacy right recognized in the *Google Spain* ruling applies regardless of whether there is harm or prejudice to the data subject, but opining that the presence of such harm (assessed on an "ethical, legal, and practical basis") is relevant in the balancing of the interest of the general public to access information against the fundamental rights of the data subject.[14] The report sets out four primary criteria for assessing delisting requests: the data subject's role in public life, the nature/type of information, its source, and how much time has passed since its publication.[15] The council acknowledged that "[m]any people have questioned whether it is appropriate for a corporation to take on what may otherwise be considered a judicial role."[16]

The report also addressed what it described as the "difficult question"[17] of the geographic scope of the delisting right.[18] Based on Google's claim that 95 percent of searches from Europe are made via the nationally directed versions of the search engine (i.e., those with country-code domains, such as "google.de" and "google.fr"), and on competing considerations regarding access to information from those outside of Europe,[19] it concluded that "removal from nationally directed versions of Google's search services within the EU is the appropriate means to implement the Ruling,"[20] thereby not requiring delisting from searches made via generic domains such as ".com."

The EU's independent privacy advisory panel created pursuant to Article 29 of the Data Protection Directive[21]—commonly referred to as the Article 29 Data Protection Working Party (WP 29)[22]—took a different view in guidelines it issued about *Google Spain* on November 26, 2014.[23] The guidelines state that the decision applies not only to search engines with an EU member state country-code domain name, but that "de-listing should also be effective on all relevant domains, including .com."[24] Consistent with such position, on May 21, 2015, the French data protection authority (CNIL) formally ordered Google

14. Luciano Floridi et al., The Advisory Council to Google on the Right to Be Forgotten 5–6 (2015), *available at* https://drive.google.com/a/google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pli=1.

15. *Id.* at 7–14.

16. *Id.* at 18.

17. *Id.*

18. *Id.* at 18–20.

19. *Id.* at 19–20.

20. *Id.* at 20.

21. Directive 95/46, art. 29, 1995 O.J. (L 281) 31, 48 (EC).

22. WP 29 is made up, *inter alia*, of representatives of EU member state data protection authorities. *Id.* WP 29 has several roles, including contributing to the harmonizing of EU member state implementations of the Data Protection Directive, making recommendations on data protection, and issuing opinions to the European Commission on various data protection issues. *Id.* art. 30, at 48–49. While consultative and not binding, WP 29's opinions, recommendations, and other documents may be persuasive and are used by various institutions of the EU and its member states. *See id.* For example, WP 29 correspondence, guidance, and recommendations were at the heart of the coordinated Google privacy policy actions by data protection authorities discussed in Part III of this survey.

23. Art. 29 Data Prot. Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección des Datos (AEPD) and Mario Costeja González" (Nov. 26, 2014) (WP 225) [hereinafter WP 225].

24. *Id.* at 3.

to apply the delisting decision to all of the search engine's domain names, failing which a procedure could be commenced in view of the potential application of sanctions.[25] The CNIL publicly announced the decision in June 2015.[26] Google responded in a blog post on July 30, 2015, contesting the authority's order,[27] and the CNIL announced that it would study and answer Google's statement within two months.[28]

WP 29 also confirmed that complaints for search engine refusals to delist, which are to be made to the relevant member state data protection authorities (DPAs), are to be treated by the DPAs "under their national legislation in the same manner as all other claims/complaints/requests for mediation."[29] WP 29 also made it clear that the guidelines do not solely target Google, and that *Google Spain* "is specifically addressed to generalist search engines, but that does not mean that it cannot be applied to other intermediaries."[30] Therefore, other operators of websites that link to web content involving personal data of EU residents should study the decision and consider its potential future application to them, even though it has only been applied to search engines to date.

On December 29, 2014, the *Audencia Nacional* (Spain's national appellate court of ordinary jurisdiction) issued its judgment applying the ECJ's *Google Spain* decision,[31] thus firmly fixing the "right to be forgotten" in Spanish law. Earlier that same month, the French *Tribunal de Grande Instance* (the ordinary court of original jurisdiction) of Paris issued an injunctive order for Google Inc. to de-index, or delete the links to, certain web pages of *Le Parisien* newspaper, regarding information about the criminal conviction of an individual published eight years earlier.[32] The claimant argued, *inter alia*, that the results linking to such pages when a search was made using her first and last names harmed her chances of getting a job.[33] The court found claimant's claim well founded.[34]

25. Commission nationale de l'informatique et des libertés, Décision n° 2015-047 du 21 mai 2015 mettant en demeure la société GOOGLE INC. [Decision No. 2015-047 of May 21, 2015 Giving Formal Notice to GOOGLE INC.], http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Bureau/D2015-047_MED_GOOGLE_INC.pdf.

26. *See* Press Release, Commission nationale de l'informatique et des libertés, CNIL Orders Google to Apply Delisting on All Domain Names of the Search Engine (June 12, 2015), http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/.

27. *See* Peter Fleischer, *Implementing a European, Not Global, Right to Be Forgotten*, Google Eur. Blog (July 30, 2015), http://googlepolicyeurope.blogspot.fr/2015/07/implementing-european-not-global-right.html.

28. *See* Mark Scott, *Google Fights Effort to Apply "Right to Be Forgotten" Ruling Worldwide,* N.Y. Times (July 30, 2015, 12:46 PM), http://nyti.ms/1KBwUR7.

29. WP 225, *supra* note 23, at 11.

30. *Id.* at 8.

31. S.A.N., Dec. 29, 2014 (Recurso No. 725/2010, R.G. 4899/2010) (Spain), http://www.poderjudicial.es/stfls/SALA%20DE%20PRENSA/NOTAS%20DE%20PRENSA/AN%20S1%2029-12-2014.pdf (Google Spain, S.L. v. Agencia Protección de Datos).

32. Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, Dec. 19, 2014 (France), http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4425 (Marie-France M. v. Google France).

33. *Id.*

34. *Id.*

The court's order, which followed the rejection by Google in September 2014 of claimant's request to exercise her right to be forgotten using the form supplied by Google following the *Google Spain* decision, marked the first time Google has been sanctioned in France for failing to respect the "right to be forgotten" after the ECJ's judgment.[35]

III. Further Action on Google's Privacy Policy

During the past year, DPAs in the EU moved forward with actions they had brought against Google based on the 2012 revision of its privacy policies into a single merged policy.[36] Notably, the United Kingdom's DPA, the Information Commissioner's Office (ICO), "required Google to sign a formal undertaking to improve the information it provides to people about how it collects personal data in the UK," based on its finding that the policy was too vague, even though the ICO's head of enforcement stated that its "investigation concluded that th[e] case ha[d]n't resulted in substantial damage and distress to consumers."[37] After setting out the background of the proceedings against Google, the undertaking specifies the search engine's commitments, which may serve as a guide to other online businesses for best practices regarding their privacy policies where they offer a variety of services to consumers.[38] For example, Google undertakes to continuously engage in privacy impact assessment for changes to processing not reasonably expected by users, to have user experience specialists and representative user groups review significant future changes to the policy, and to inform the ICO in advance of any significant changes to the policy, among other commitments.[39]

IV. Enhanced Security Measures in the Aftermath of the *Charlie Hebdo* Attacks

On January 7, 2015, three terrorists killed twelve people (including two police officers) in connection with their attack on the Paris office of the French satirical journal *Charlie Hebdo*.[40] In a related attack that occurred two days thereafter,

35. *See* Lucie Ronfaut, *Google Condamné pour la Première fois en France sur le Droit à l'Oubli* [Google Sanctioned for the First Time in France on the Right to Be Forgotten], Le Figaro (Jan. 16, 2015, 10:03 AM), http://www.lefigaro.fr/secteur/high-tech/2015/01/16/32001-20150116ARTFIG00005-google-condamne-pour-la-premiere-fois-en-france-sur-le-droit-a-l-oubli.php. For a link to Google's request form, see supra note 11.

36. For a discussion of earlier stages of the actions against Google brought by the DPAs of France, Spain, Italy, and Germany, see Voss, *supra* note 3, at 254–57.

37. *Google to Change Privacy Policy After ICO Investigation*, ICO (Jan. 30, 2015), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/01/google-to-change-privacy-policy-after-ico-investigation/.

38. Data Protection Act 1998 Undertaking (Google Inc.), ICO Ref: ENF0492064, https://ico.org.uk/media/action-weve-taken/undertakings/1043170/google-inc-privacy-policy-undertaking.pdf (last visited July 28, 2015). The linked version of the undertaking is unsigned and undated. *Id.* at 7.

39. *Id.* at 6.

40. Dan Bilefsky & Maïa de la Baume, *Terrorists Strike Charlie Hebdo Newspaper in Paris, Leaving 12 Dead*, N.Y. Times (Jan. 7, 2015), http://nyti.ms/1xEc8sC.

four people were killed at a kosher grocery on the outskirts of Paris.[41] Those attacks, which involved perpetrators with "deep histories of association with terrorist organizations,"[42] have given impetus to the establishment of additional security measures, certain of which were commenced previously, both on the French national level (websites and surveillance) and on the EU level (airline passenger name records), which will affect businesses in the Internet and airline industries, respectively. Nonetheless, WP 29 rapidly reminded Europeans of their fundamental values, including protection of private life and personal data, and of the need to strike a balance with public security needs, and stated that the EU DPAs looked forward "to contributing to the discussion on how to strike this balance."[43]

A. France—Websites and Surveillance

Prior to the attacks, France adopted a law providing new powers in the battle against terrorism.[44] Article 5 of that law added a new Article 421-2-5 to the French Criminal Code allowing the prosecution of those inciting or justifying acts of terrorism and increasing sanctions if any such violation was committed using the Internet.[45]

Following the attacks, French Interior Minister Bernard Cazeneuve went to Silicon Valley to ask Google, Facebook, and Twitter to cooperate directly with French officials during investigations and to take down terrorist material.[46] Cazeneuve explained: "We emphasized that when an investigation is underway we don't want to go through the usual government to government channels, which can take so long."[47] France reportedly was "pushing to treat jihadi material on the Internet like child porn, a task that before the attacks in Paris was getting scant traction but now seems to have caught the attention of Europe's top security officials."[48] This may have been reflected in the decree France issued on February 5, 2015, providing, *inter alia*, for the blocking of websites inciting

41. Griff Witte, *In a Kosher Grocery Store in Paris, Terror Takes a Deadly Toll*, Wash. Post (Jan. 9, 2015), http://www.washingtonpost.com/world/europe/paris-kosher-market-seized-in-second-hostage-drama-in-nervous-france/2015/01/09/f171b97e-97ff-11e4-8005-1924ede3e54a_story.html.

42. *Id.*

43. Press Release, Art. 29 Data Prot. Working Party, Reaction to Attacks Recently Perpetrated in Paris (Jan. 14, 2015), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/index_en.htm.

44. Loi 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme [Law 2014-1353 of November 13, 2014 Reinforcing Provisions on the Fight Against Terrorism], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Nov. 14, 2014, p. 19162, *available at* http://legifrance.gouv.fr/eli/loi/2014/11/13/2014-1353/jo/texte.

45. *Id.* art. 5. The sanctions for inciting or justifying acts of terrorism are up to five years in prison and a fine of up to €75,000. *Id.* If the prohibited speech acts are communicated using a public online service, the penalties are increased to up to seven years in prison and a fine of up to €100,000. *Id.*

46. *French Minister Meets with Google, Facebook, Twitter*, N.Y. Times (Feb. 21, 2015, 4:21 AM), http://nyti.ms/1Aog81o.

47. *Id.*

48. *Id.*

acts of terrorism or justifying them (as well as those distributing child pornography).[49] Internet service providers must block the sites within twenty-four hours after the Ministry of the Interior provides them with a list of prohibited websites.[50] A subsequent decree provides that the Ministry of the Interior may notify search engines and web directories of content inciting acts of terrorism or justifying them, whereupon the search engines and directories have forty-eight hours in which to delist the content.[51] The latter decree would notably be used by the Ministry of the Interior where its corresponding request to a website under the prior decree proved futile. A special office to fight criminality involving information and communication technologies, whose name is abbreviated as "OCLCTIC," has been set up under the Ministry of the Interior for transmission of blocking requests, and a platform called "PHAROS" has been established for web users to report infringing content, which may involve text, photos, videos, etc.[52] The French DPA has a supervisory function that it exercises through the use of a designated authorized person within the DPA who may make recommendations if there is a questionable blocking request made by the authorities and, if the recommendations are not followed, present the issue for resolution by an administrative judge.[53]

On May 5, 2015, the French National Assembly voted on first reading in favor of a version of the so-called French Surveillance Bill, which would add various articles to the French Internal Security Code.[54] The bill reportedly would "give the authorities their most intrusive domestic spying abilities ever, with almost no judicial oversight," allowing intelligence services, *inter alia*, to "read emails and force Internet companies to comply with requests to allow the government to sift through virtually all of their subscribers' communications."[55] The bill

49. Décret 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique [Decree 2015-125 of February 5, 2015 on the Blocking of Websites Inciting Acts of Terrorism or Justifying Them and Websites Disseminating Child Pornography], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Feb. 6, 2015, p. 1811, *available at* http://legifrance.gouv.fr/eli/decret/2015/2/5/2015-125/jo/texte.

50. *Id.*

51. Décret 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique [Decree 2015-253 of March 4, 2015 on the Delisting of Websites Inciting Acts of Terrorism or Justifying Them and Websites Distributing Child Pornography], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Mar. 5, 2015, p. 4168, *available at* http://legifrance.gouv.fr/eli/decret/2015/3/4/2015-253/jo/texte.

52. *See Quel Contrôle du Blocage Administratif des Sites Internet?* [What Kind of Supervision for the Administrative Blocking of Websites?], CNIL (Feb. 13, 2015), http://www.cnil.fr/linstitution/actualite/article/article/quel-controle-du-blocage-administratif-des-sites-internet/.

53. *Id.*

54. Assemblée Nationale [French National Assembly], Projet de loi relative au renseignement [Bill on Intelligence], Texte adopté n° 511 en première lecture [as passed by the National Assembly on the first reading], May 5, 2015, http://www.assemblee-nationale.fr/14/pdf/ta/ta0511.pdf. The National Assembly is the lower house of the French Parliament.

55. Alissa J. Rubin, *Lawmakers in France Move to Vastly Expand Surveillance*, N.Y. Times (May 5, 2015), http://nyti.ms/1IdFCmR.

would create a supervisory organization called the National Commission to Control Intelligence Techniques (CNCTR), which would rule on requests to initiate surveillance.[56] Metadata "would be electronically sorted, and only if the sites visited or the searches carried out suggested suspicious behavior as defined by the intelligence services would a human review of a person's emails and Internet browsing occur."[57]

The bill, which was described by the president of the Paris Bar Association as a French analog to the U.S. Patriot Act,[58] and which has been subject to objections from a broad array of Internet-oriented businesses,[59] went before the French Senate, the upper house of the French Parliament, which made various amendments to the bill,[60] and finally adopted an amended version on June 23, 2015,[61] which was then adopted by the French National Assembly on June 24, 2015.[62] On June 25, 2015, French President François Hollande, the President of the French Senate, and sixty members of the French National Assembly submitted the recently adopted French Surveillance Act to the French Constitutional Council (*Conseil Constitutionnel*) for review of its constitutionality.[63] A French Internet users' rights organization (La Quadrature du Net) and French Internet service provider associations (French Data Network and FDN Federation) stated that they had filed amicus briefs against the French Surveillance Act.[64] The European Parliament announced that its Civil Liberties Committee would debate concerns over the Act on July 2, 2015, and that members "are likely to ask the Commission to investigate whether the law is in line with EU treaties and the Charter of Fundamental Rights."[65]

On July 23, 2015, the French Constitutional Council issued its decision, largely upholding the French Surveillance Act; the council, however, invalidated portions

56. *Id.* The thirteen-member commission would be comprised of "six magistrates from the Council of State and the Court of Appeals, three representatives of the National Assembly, three senators from the upper house of the French Parliament and a technical expert." *Id.*

57. *Id.*

58. *Id.*

59. *Id.*; *see also* Morgane Tual, *"Ni Pigeons, Ni Espions," les Acteurs du Numérique Mobilisés Contre la Loi sur le Renseignement* ["Neither Pigeons, Nor Spies," Digital Actors Are Mobilized Against the Intelligence Act], Le Monde (Apr. 22, 2015, 10:28 AM), http://www.lemonde.fr/pixels/article/2015/04/22/ni-pigeons-ni-espions-les-acteurs-du-numerique-mobilises-contre-la-loi-sur-le-renseignement_4619971_4408996.html.

60. *See Projet de Loi relative au Renseignement*, Sénat.fr (Aug. 6, 2015), http://www.senat.fr/dossier-legislatif/pjl14-424.html (providing legislative history).

61. *See Projet de Loi relative au Renseignement*, Sénat.fr (June 23, 2015), http://www.senat.fr/petite-loi-ameli/2014-2015/521.html.

62. *See Projet de Loi relative au Renseignement*, Assemblée Nationale (June 24, 2015), http://www.assemblee-nationale.fr/14/pdf/ta/ta0542.pdf.

63. Conseil Constitutionnel [CC] [Constitutional Court], Case No. 2015-713 DC, June 25, 2015, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/affaires-en-instance/affaires-en-instance.28377.html.

64. *See French Surveillance Bill: LQDN Files an Amicus Brief to the Constitutional Court*, La Quadrature du Net (June 25, 2015, 11:42 AM), http://www.laquadrature.net/en/french-surveillance-bill-lqdn-files-an-amicus-brief-to-the-constitutional-court.

65. Press Release, European Parliament, Civil Liberties MEPs to Debate Concerns over French Surveillance Law (July 2, 2015), http://www.europarl.europa.eu/pdfs/news/expert/infopress/20150701IPR72724/20150701IPR72724_en.pdf.

of the law, such as those provisions that permitted emergency surveillance without the approval of the prime minister or another governmental minister.[66]

Internet companies with activities in France should review this legislation and the decision of the Constitutional Council and any subsequent legislative reaction either at the French or EU level, and any potential EU judicial challenge, to determine their possible obligations under the legislation.

B. Europe—Airline Passenger Name Records

In 2004, a few short years after the World Trade Center terrorist attacks in New York, the United States and the EU negotiated an agreement allowing the transfer of personal data of airline passengers traveling from Europe to the United States,[67] where the cross-border data transfer restrictions of the Data Protection Directive would otherwise have prevented such transfer.[68] Years later, in 2011, the European Commission proposed a directive that would harmonize the few member state laws regarding the collection of such passenger name record (PNR) data.[69] PNR data may include travel itineraries and dates, contact details, payment methods, and other personal information that may be useful to law enforcement authorities.[70] The proposed PNR Directive "aims to harmonise Member States' provisions on obligations for air carriers, operating flights between a third country and the territory of at least one Member State, to transmit PNR data to the competent authorities for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime."[71] On April 29, 2013, the European Parliament's Civil Liberties Committee recommended that the European Parliament reject the Commission's proposed PNR Directive.[72] However, this proposal gained support recently, especially since the *Charlie Hebdo* attacks and the discovery that terrorists have traveled by air between Europe and areas of conflict in Syria.[73]

66. Conseil Constitutionnel [CC] [Constitutional Court], decision No. 2015-713 DC, July 23, 2015, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/decision-n-2015-713-dc-du-23-juillet-2015.144138.html; Sam Schechner & Matthew Dalton, *French Constitutional Court Approves New Powers for Intelligence Services*, Wall St. J. (July 24, 2015, 5:40 AM), http://www.wsj.com/articles/french-constitutional-court-approves-new-powers-for-intelligence-services-1437730809.

67. Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (May 28, 2004), http://ec.europa.eu/justice/policies/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf.

68. *See* Directive 95/46, arts. 25–26, 1995 O.J. (L 281) 31 (EC).

69. *Commission 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 Offences and Serious Crime*, COM (2011) 32 final (Feb. 2, 2011).

70. *Id.* at 32.

71. *Id.* at 4.

72. *See* Press Release, European Parliament, MEPs Debate Plans to Use EU Passenger Name Record (PNR) Data to Fight Terrorism (Nov. 11, 2014), http://www.europarl.europa.eu/news/en/news-room/content/20141110IPR78121/html/MEPs-debate-plans-to-use-EU-Passenger-Name-Record-(PNR)-data-to-fight-terrorism.

73. *See id.* (referencing "concerns over possible threats to the EU's internal security posed by Europeans returning home after fighting for the so-called 'Islamic State'").

WP 29 recognized the changed circumstances, noting that, following the *Charlie Hebdo* and other attacks in Paris in early January 2015, "the potential establishment of an EU PNR system took over the international headlines."[74] It cautioned, however, that, because of the fundamental rights involved, the measure would be justified "only if its necessity was to be demonstrated and the principle of proportionality respected."[75]

In February 2015, a member of the European Parliament, Timothy Kirkhope, circulated an alternative to the proposed PNR Directive, which included coverage of all (including intra-EU) flights, access to terrorism-related PNR data for five years, and other security and data protection measures.[76] While acknowledging that this new draft offers some improvements, WP 29 took the position that the draft "is likely to seriously undermine the rights as set out in Articles 7 and 8 of the Charter of Fundamental Rights in the European Union," that the instrument's necessity still needs to be proved, and that there should be further restrictions "to ensure that the data processing is proportionate to the purpose pursued," especially because the new draft would apply to intra-EU flights.[77] WP 29 added that the use of data should be limited to certain crimes, the system should be periodically evaluated, including a first evaluation after two years at the latest, and that the measure must comply with the requirements of the ECJ decision striking down the Data Retention Directive regarding retention periods for the data, *inter alia*.[78]

On July 15, 2015, the European Parliament's Civil Liberties Committee by a vote of thirty-two to twenty-seven approved the new PNR rules as amended by it, and also mandated the opening of negotiations with the EU Council of Ministers. Use of the PNR data would be limited to the prevention, detection, and investigation of terrorism and serious transnational crimes. Other safeguards inserted in the draft legislation included, *inter alia*, the requirement that data protection officers be appointed by member state Passenger Information Units (PIUs), that PNR data processing be logged or documented, that passengers must be informed about their rights and the collection of their PNR data, and that "stricter conditions would govern any transfer of data to third countries."[79]

74. Press Release, Art. 29 Data Prot. Working Party, EU PNR (Feb. 5, 2015), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/index_en.htm.

75. *Id.*

76. Press Release, European Parliament, Changes to Planned European Passenger Name Record (PNR) System Discussed by MEPs (Feb. 26, 2015), http://www.europarl.europa.eu/news/en/news-room/content/20150223IPR24702/html/Changes-to-planned-European-Passenger-Name-Record-(PNR)-system-discussed-by-MEPs.

77. Letter from Art. 29 Data Prot. Working Party to Claude Moraes, Chairman, LIBE Comm'n of the European Parliament (Mar. 19, 2015), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150319__letter_of_the_art_29_wp_on_eu_pnr.pdf.

78. *Id.* at 3–6. The referenced ECJ case is Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine & Natural Resources (Apr. 8, 2014), http://goo.gl/qP2ZaL; *see also* Voss, *supra* note 3, at 257–59 (discussing the joined cases).

79. Press Release, European Parliament, Passenger Name Records: MEPs Back EU System with Data Protection Safeguards (July 15, 2015), http://www.europarl.europa.eu/pdfs/news/expert/infopress/20150714IPR81601/20150714IPR81601_en.pdf.

The current Luxembourg Presidency of the EU Council expects to be able to reach agreement with the European Parliament on the PNR proposals by the end of the Presidency's term,[80] which terminates on December 31, 2015.

Airlines and other travel businesses such as tour operators and travel agencies are likely to be affected once the PNR Directive is enacted, in terms of collecting and turning over information, but also with potential effects on their relationship with their customers, as they become data collecting agencies for authorities in EU countries, potentially even for intra-EU flights.

V. Ongoing Work on European Union Data Protection Law Reform

On January 25, 2012, the European Commission proposed a new General Data Protection Regulation (GDPR) which, if adopted, would have replaced the Data Protection Directive and applied directly throughout the EU.[81] Two years later, on March 12, 2014, the European Parliament voted overwhelmingly in favor of a compromise text of the GDPR.[82]

In its May 2015 blueprint for a European digital single market, the European Commission stated that the GDPR is "due to be adopted by the end of 2015."[83] In a communication setting out the details of its strategy, the Commission announced that, in 2016, it will propose a European "[f]ree flow of data" initiative, which "will address the emerging issues of ownership, interoperability, usability and access to data in situations such as business-to-business, business to consumer, machine generated and machine-to-machine data."[84]

Though the Council had been partly responsible for delay in the adoption of the GDPR,[85] the Council eventually finalized a common position on all points of the proposed GDPR on June 15, 2015.[86] The European Parliament and the

80. Press Release, European Parliament, Luxembourg Presidency Priorities Discussed by EP Committees (July 17, 2015), http://www.europarl.europa.eu/pdfs/news/expert/infopress/20150714IPR81309/20150714IPR81309_en.pdf.

81. *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).

82. *See* Press Release, European Comm'n, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote (Mar. 12, 2014), http://goo.gl/JszkAX. For a discussion of the GDPR as approved by the Parliament, see Voss, *supra* note 3, at 259–60.

83. Press Release, European Comm'n, A Digital Single Market for Europe: Commission Sets Out 16 Initiatives to Make It Happen (May 6, 2015), http://europa.eu/rapid/press-release_IP-15-4919_en.htm.

84. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Single Market Strategy for Europe*, COM (2015) 192 final (May 6, 2015).

85. *See* W. Gregory Voss, *Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later*, 17 J. Internet L. 1, 19 (2014).

86. Press Release, European Comm'n, Commission Proposal on New Data Protection Rules to Boost EU Digital Single Market Supported by Justice Ministers (June 15, 2015), http://europa.eu/rapid/press-release_IP-15-5176_en.htm; *see* Note from Presidency to Council (June 11, 2015), http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (addressing the preparation of a general approach to the GDPR).

Council must agree on the same text under the ordinary legislative procedure in order for it to become law.[87] A trilogue involving the Council, the European Parliament, and the European Commission began on June 24, 2014.[88] WP 29 previously criticized the Council's interim partial draft allowing further processing of data "even if the purpose is incompatible with the original one as long as the controller has an overriding interest in this processing."[89] In addition, the European Parliament's rapporteur and lead negotiator for the GDPR, Jan Philipp Albrecht, "stressed that several important issues still needed to be worked out with the Council, such as the need for consumers to give consent for the use of their data, the duties of data controllers and what fines should be imposed on companies that break the rules."[90] Thus, there is still work to be done in order to reach a full agreement on all points between the European institutions on the GDPR text, in a way that allays the concerns of privacy advisors.

VI. Conclusion

This survey has focused on data privacy developments linked to two major events in the news—the ECJ's *Google Spain* ruling and the *Charlie Hebdo* terrorist attacks. Privacy developments that seemingly involve only one company—namely, Google—have wider implications, and should be of interest to other firms as well. These developments impact various industries and categories of professionals: Internet search engines, certainly, but also other Internet intermediaries and companies that process personal data (including those that publish them on the Internet), media, journalists, airlines, travel industries, and others. Hopefully, this survey will encourage readers to monitor developments in these areas.

87. For a short discussion of the "ordinary legislative procedure" that applies to the adoption of the GDPR, see Voss, *supra* note 85, at 15.

88. Press Release, European Parliament, Data Protection: Parliament's Negotiators Welcome Council Negotiating Brief (June 15, 2015), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+IM-PRESS+20150615IPR66464+0+DOC+PDF+V0//EN&language=EN. The press release also discusses the Council's prior stalling. *Id.*

89. Press Release, Art. 29 Data Prot. Working Party, Press Release on Chapter II of the Draft Regulation for the March JHA Council (Mar. 17, 2015), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20150317__wp29_press_release_on_on_chapter_ii_of_the_draft_regulation_for_the_march_jha_council.pdf.

90. Press Release, European Parliament, Albrecht on Data Protection Reform: People Will Be Better Informed (June 17, 2015), http://www.europarl.europa.eu/pdfs/news/public/story/20150616STO66729/20150616STO66729_en.pdf.