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

Privacy, E-Commerce, and Data Security

W. Gregory Voss, Katherine Woodcock, Rob Corbet, Chris Bollard, Jennifer L. Mozwecz, and João Luís Traça*

This article reviews important legal developments during 2013 in the fields of privacy, e-commerce, and data security.[1] In light of changes around a new proposed privacy framework, a special focus has been made on European developments, discussed principally in Part I(A)(2), below. A new section on developments in Cape Verde has been added in Part III below.

I. Developments in Europe

With respect to Europe, this article centers on (1) advice from the European Union (EU) Article 29 Data Protection Working Party, an independent advisory panel providing interpretative guidance on privacy directives to Member States of the EU, which then can be used by Member State data protection agencies (DPAs) or legislators; (2) proposed data protection law reform in the EU; and (3) action of DPAs with respect to privacy policies.[2]

---

* The committee editor was W. Gregory Voss, Toulouse University, Toulouse Business School, Member of the IRDEIC Research Institute, Toulouse, France. The authors were, Katherine Woodcock, Lorenz International Lawyers, Brussels, Belgium (on Overview of Guidance from the EU Article 29 Data Protection Working Party, in the Developments in Europe section); Rob Corbet, Partner, Arthur Cox, Dublin, Ireland and Co-Chair of the ABA Section of International Law Privacy, E-Commerce, and Data Security Committee and Chris Bollard, Associate, Arthur Cox, Dublin, Ireland (on The Proposal for an EU Regulation on Data Protection, in the Developments in Europe section); W. Gregory Voss (on Action of DPAs with Respect to Privacy Policies, in the Developments in Europe section); Jennifer L. Mozwecz, Shams, Rodriguez & Mozwecz, P.C., Chicago, Illinois, USA (on Federal Developments in the Developments in the United States section); and W. Gregory Voss (on State Developments: California in the Developments in the United States section); and João Luís Traça, Partner in charge of the Data Protection practice, admitted to the Portuguese Bar, Miranda, Correia, Amendoeira & Associados, Lisbon, Portugal (on Cape Verde in the Developments in Africa section).

1. For earlier developments in this field, see W. Gregory Voss et al., *Privacy, E-Commerce, and Data Security*, 47 Int'l Law 99 (2013), *available at* http://apps.americanbar.org/intlaw/TIL_46_1/PrivacyE-Commerce&DataSecurity.pdf.

2. *See Article 29 Working Party*, Eur. Comm'n (Aug. 6, 2013), http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last visited Feb. 14, 2014).

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW

A. European Union

1. *Overview of Guidance from the EU Article 29 Data Protection Working Party*

Two-thousand and thirteen was a busy year for EU privacy developments. Interestingly, the EU Article 29 Working Party (WP) released fewer opinions and formal guidance than in past years.[3] On the other hand, the WP was extremely active in drafting correspondence on privacy concerns. With over twenty letters published on its website, 2013 marked the WP's most active year in correspondence.[4] Topics include the review of the World Anti-Doping Code, publications on the European Commission's websites, proposals for new Anti-Money Laundering and Counter Terrorist Financing Directive, Google Glass and—of course—the U.S. PRISM program.[5] The WP has also been active in advising and participating in the data protection reform in the EU.[6] Below is a summary of the WP's significant opinions and guidance from 2013.

a. Applications on Smart Devices

In response to the breakneck growth of the use of smartphones and related applications (apps), the WP issued an opinion providing guidance for the collection and processing of personal data in that field.[7] The opinion explains how apps collect data and interact with other technologies and different actors. The WP identifies the risks in apps use, including the lack of transparency toward end users, the lack of "free and informed consent," poor security, and a disregard for the purpose limitation principle.[8]

The opinion outlines the different actors and provides examples as to when they would qualify as a data controller. The use of consent is identified as the primary legal basis for processing personal data in an app.[9] The opinion emphasizes the importance of the role of consent and the need for end users to provide their specific and informed consent.[10] Once the app is downloaded, the legal basis can change and may include an underlying

3. Only six formal opinions, two working documents, and one explanatory memorandum were published through Dec. 1, 2013. By way of contrast, in 2012, the WP published eight formal opinions (the same number as in 2009, 2010, and 2011), two working documents, and a set of recommendations. *See Opinions and Recommendations*, Eur. Comm'n (Dec. 17, 2013), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (last visited Feb. 14, 2014).

4. *See Other Documents*, Eur. Comm'n (Jan. 30, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm (last visited Feb. 14, 2014). Please note that it is possible that letters and documents (or specific portions of the same) may not be publishable for reasons of business confidentiality, protection of personal data, or other legitimate reasons.

5. For full access to the WP's documentation (including correspondence and opinions), see *Documentation*, Eur. Comm'n (July 17, 2013), http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm (last visited Feb. 14, 2014).

6. *See infra* I(A)(2).

7. *See generally* Opinion 02/2013 on Apps on Smart Devices, Art. 29 Data Prot. Working Party, Feb. 27, 2013, 00461/13/EN; WP 202 (2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf [hereinafter Opinion 02/2013].

8. *Id.* at 5–6.

9. *See* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 291) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [hereinafter Directive].

10. Opinion 02/2013, *supra* note 7, at 14, 15.

contractual agreement or the legitimate business interest of the data controller.[11] When relying on these legal bases, processing is limited to only non-sensitive data and for legitimate business interests (with the balancing of the fundamental rights of the data subject).[12] The opinion notes that all app actors—including app developers, app stores, operating systems, and device managers, as well as third parties—will need to take data security into account based on their respective roles and responsibilities.[13]

Pursuant to the information requirement, notice provided should include, at a minimum, the data controller's identity and contact details, the categories of personal data to be processed, specified purposes of the processing, whether disclosures will be made, and how end users can exercise their rights.[14] Interestingly, the WP discusses how the information will be provided and includes the possibility to provide more detailed information via links to a privacy policy and the ability "to link through to more extensive explanations, for example in the privacy policy, how the app uses personal data, who the controller is and where a user can exercise his rights."[15] The WP encourages creative solutions from app developers to inform users of their rights on mobile devices and recommends testing these methods with consumers to ensure they are effective.[16] It also points out that apps must ensure that users can invoke their individual rights and that data retention periods are set and respected.[17] For underage users, the WP refers to its 2009 opinion[18] and also echoes concerns expressed in the FTC staff report on mobile apps for kids.[19] The opinion concludes with a list of responsibilities for each app actor, including what is expected for data protection compliance.[20]

b. Explanation of the Purpose Limitation Principle

The WP issued an opinion to guide parties in the application of the purpose limitation principle, which is a key component of the provisions on data quality.[21] This principle is decisive to the protection of personal data, as it limits how controllers use individuals' data. The WP also seeks to clarify the principle and any exceptions in advance of the finalization of the proposed General Data Protection Regulation.[22] The principle of pur-

11. Directive, *supra* note 9, art. 7(b), (f).
12. Opinion 02/2013, *supra* note 7, at 16.
13. *Id.* at 18–21.
14. *Id.* at 22.
15. *Id.* at 24.
16. *Id.*
17. *Id.* at 25.
18. *See generally* Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools), Art. 29 Data Prot. Working Party, Feb. 11, 2009, 398/09/EN; WP 160 (2009), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.
19. *Compare* Opinion 02/2013, *supra* note 7, *with* FED. TRADE COMM'N, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf.
20. Opinion 02/2013, *supra* note 7, at 27–30.
21. *See generally* Opinion 03/2013 on Purpose Limitation, Art. 29 Data Prot. Working Party, Apr. 2, 2013, 00569/13/EN; WP 203 (2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [hereinafter Opinion 03/2013]. For the purpose limitation principle, *see* Directive, *supra* note 9, art. 6(1)(b).
22. *See infra* I(A)(2).

pose limitation is made up of the following two elements: (i) purpose specification and (ii) compatible use. Both elements support "transparency, legal certainty and predictability"[23] by placing limitations on the use of data subjects' personal data by data controllers and ensuring that the use is within the expectations of the data subjects.[24] The first element, purpose specification, means that personal data must be collected for "specified, explicit and legitimate" purposes. This requirement is a precondition for other data quality requirements specified under Article 6; specifically, the purposes will set the bar for what data should be collected, how long the data should be retained, and the other applicable safeguards (e.g., information security).[25]

Second, compatible use signifies that data is not further processed in a way incompatible with those purposes. The opinion clarifies that compatibility does not focus on the originally specified purpose and then subsequently defined purposes; it distinguishes between the first processing operation (i.e., collection) and the subsequent processing operations (i.e., storage and further processing).[26] Therefore, any processing activities after collection are considered further processing and must meet the compatible use requirement. This assessment can be accomplished by the controller in either a formal or substantive assessment.[27] A formal assessment is accomplished by comparing the originally specified purposes (together with any other formal uses) to determine if the further processing activities are covered. Second, a substantive assessment reaches "beyond formal statements to identify the new and the original purposes," to include the way the purposes are understood in fact (i.e., taking into account the surrounding circumstances).[28]

c. Binding Corporate Rules (BCRs) for Processors

Further developing the field of BCRs, the WP published an explanatory document on BCRs for processors. This follows its 2012 working document for requirements in processor BCRs[29] and its recommendation on the standardization of the BCR approval form.[30] The explanatory document aims to provide guidance to both companies and DPAs on how to practically implement this new possibility and how it will work in practice (e.g., contractually, under existing national law and data protection framework).

23. Opinion 03/2013, *supra* note 21, at 11.

24. *Id.*

25. *Id.* at 11–12.

26. *Id.* at 12–13.

27. *Id.*

28. *Id.* at 21.

29. *See generally* Working Document 02/2012 Setting Up a Table with the Elements and Principles to be Found in *Processor* Binding Corporate Rules, Art. 29 Data Prot. Working Party, Apr. 2, 2013, 00930/12/EN; WP 195 (2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf.

30. *See generally* Recommendation 1/2012 on the Standard Application Form for Approval of Binding Corporate Rules for the Transfer of Personal Data *for Processing Activities*, Art. 29 Data Prot. Working Party, Sept. 17, 2012, WP 195a (2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195a_application_form_en.doc.

d. Open Data and Public Sector Information (PSI) Reuse

The EU adopted Directive 2013/37/EU amending Directive 2003/98/EC on the re-use of public sector information (PSI Directive) on June 26, 2013.[31] In response to the new changes, the WP issued an opinion clarifying the role of data protection in this new framework.[32] The amended directive aimed to harmonize the principle that all public information would be "reusable for both commercial and non-commercial purposes."[33] It does so by requiring public bodies to permit the reuse of all public information in their possession. Personal information is not obliged to be disclosed; it is only mandated if it is already publicly available under national law and if the reuse does not violate applicable data protection provisions.[34]

PSI reuse initiatives typically involve (i) making entire databases available (ii) in standardized electronic format (iii) to any applicant without any screening process, (iv) free of charge (or subject to limited fees), and (v) for any commercial or non-commercial purposes without conditions (or under non-restrictive conditions through a license, where appropriate).[35]

The opinion notes that reuse of PSI does not come without risks and the public sector should use a balanced approach and follow data protection rules in order to make a selection of which personal data can be made available for reuse and what safeguards are put in place.[36] The WP states that statistical data taken from personal data will often times be the preferable data for reuse.[37] In cases where personal data can be considered for reuse, there must be a strong legal basis, and the principles related to data quality (proportionality and purpose limitation) should be taken into account in addition to technical and organizational measures to secure the personal data.[38] Furthermore, the public body should always carry out a privacy impact assessment prior to the publication of any PSI with personal data included.[39] Moreover, licensing terms should always include a data protection clause whenever personal data is processed and, in certain circumstances when personal data is anonymized, when re-identification of the individuals and subsequent reuse is prohibited.[40]

31. *See generally* Directive 2013/37/EU, of the European Parliament and of the Council of 26 June 2013 Amending Directive 2003/98/EC on the Re-Use of Public Sector Information, 2013 O.J. (L 175) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:175:0001:0008:EN:PDF.

32. *See generally* Opinion 06/2013 on Open Data and Public Sector Information ('PSI') Reuse, Art. 29 Data Prot. Working Party, June 5, 2013, 1021/00/EN; WP 207 (2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf.

33. *Id.* at 2.

34. *Id.*

35. *Id.* at 3.

36. *Id.* at 6–9.

37. *Id.* at 15.

38. *Id.* at 19–20.

39. *Id.* at 19–21, 23, 27.

40. *Id.* at 19, 25–26.

e. Clarification of Obtaining Consent for Cookies

On October 2, 2013, the WP published a working document providing guidance on obtaining consent for cookies.[41] This document was likely a response to the overwhelming divergence of the practical implementation of the new cookie rule from Article 5(3) of the ePrivacy Directive, which has been marked by frustration from both companies and users.[42] The working document reiterates consent requirements (drawing from its previous opinions on cookies, consent, and online behavioral advertising) and clarifies that valid consent must consist of specific information, be given prior to processing, be unambiguous (data subject's active choice that leaves no doubt as to his or her intention), and be freely given (that the data subject has an actual choice).[43]

In terms of active choices, the WP notes that tools such as banners, splash screens, modal windows, and browser settings may be used. For browser settings, the WP states that when "the website operator can be confident that the user has been fully informed and actively configured their browser or other application," then these configurations would indicate active behavior.[44] This does not unequivocally specify in which circumstances this would be the case, but it appears to refer to "do not track" preferences (or custom browser setting where users select the automatic rejection of third party cookies). Of course, these preference settings would only inform the website operator that he or she does not consent to tracking cookies, leaving the issue of other cookies unresolved.

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

a. Delay in Adoption of New EU Laws on Data Protection

In January 2012, the European Commission outlined its proposals for a radical overhaul of data protection rules in the European Union. Included in these proposals was the draft text of a proposed, new General Data Protection Regulation (Regulation).[45] The aim of the Regulation is to increase compliance obligations of all companies targeting customers

41. *See generally* Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies, Art. 29 Data Prot. Working Party, Oct. 2, 2013, 1676/13/EN; WP 208 (2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf [hereinafter Working Document 02/2013].

42. For examples of the expression of such frustrations see, e.g., Mike Butcher, *Stupid EU Cookie Law Will Hand the Advantage to the US, Kill Our Startups Stone Dead*, TECH CRUNCH (Mar. 9, 2011), http://techcrunch.com/2011/03/09/stupid-eu-cookie-law-will-hand-the-advantage-to-the-us-kill-our-startups-stone-dead/; *see also* Struan Robertson, *Consent Will Be Required for Cookies in Europe*, OUT-LAW (Nov. 9, 2009), http://www.out-law.com/page-10510; *see also* Zack Whittaker, *Sweet Irony: EU Imposes Cookie Law, Ignores Own Rules*, ZDNET.COM (May 29, 2012, 4:58 PM), http://www.zdnet.com/blog/london/sweet-irony-eu-imposes-cookie-law-ignores-own-rules/4975; *see also* Rupert Jones, *Internet Security: Cookie Monster Unleashed Following EU Ruling*, THE GUARDIAN (May 27, 2011), at Money, 3, *available at* http://www.theguardian.com/money/2011/may/28/internet-security-cookie-eu-ruling; *see also* Peter Kirwan, *EU Cookie Law: Stop Whining and Just Get On With It*, WIRED (May 24, 2012), http://www.wired.co.uk/news/archive/2012-05/24/eu-cookie-law-moaning.

43. *See* Working Document 02/2013, *supra* note 41, at 3.

44. *Id.* at 4–5.

45. *See, e.g.*, *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. 1, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. For an earlier discussion of the Regulation, see W. Gregory Voss et al., *supra* note 1, at 102–04.

in the European Union. Among the new key initiatives that attracted immediate attention was the possibility of fines of up to 2 percent of global turnover for certain breaches[46] and a new breach notification regime.[47] The draft Regulation was anticipated as being the most significant development in European data protection law for twenty years. While the draft did not progress to adoption in 2013, some slow progress did occur during the year.

The Regulation has been championed principally by the Vice President of the European Commission (Commission) and Commissioner for Justice, Fundamental Rights, and Citizenship, Viviane Reding. But despite her extensive efforts and those of the Commission, the adoption process for the Regulation has been subject to protracted delays, reflecting the fact that the Regulation requires the approval of the European Parliament (Parliament) and the Council of the European Union (Council) under the co-decision process before it can become law. Below are set out the key developments during 2013 and their impact on the Regulation's progress.

b. The Regulation's Progress within the LIBE Committee

Within the Parliament, the Regulation falls under the auspices of its Committee on Civil Liberties, Justice, and Home Affairs (LIBE Committee) and its *rapporteur*, Jan Philipp Abrecht, who produced a draft report on the Regulation for the LIBE Committee in January (the Report).[48] Observers noted at the time that rather than rowing back on some of the newly expanded data subject rights contained in the Regulation, the Report in fact sought to further strengthen individual rights, notably the data subject's right of access.

Over the course of the year, the LIBE Committee received non-binding opinions from other stakeholders within the Parliament, including the Employment and Social Affairs Committee[49] and the Legal Affairs Committee.[50]

46. *Id.* art. 79(6).

47. *Id.* arts. 31–32.

48. *See, e.g.*, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 0011 (Jan. 16, 2013), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-501.927%2b04%2bDOC%2bPDF%2bV0%2f%2fEN [hereinafter Draft Report]. For a discussion of the Draft Report, see W. Gregory Voss, *One Year and Loads of Data Later, Where Are We? An Update on the Proposed European Union General Data Protection Regulation*, 16 J. INTERNET L. 1, 18–21 (2013).

49. *See, e.g.*, *Opinion of the Committee on Employment and Social Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the 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) 0011 final (Mar. 4, 2013), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-498.045%2b02%2bDOC%2bPDF%2bV0%2f%2fEN.

50. *See, e.g.*, Press Release, Eur. Parl., Safeguarding Personal Data While Boosting Competition for Business (Mar. 19, 2013), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20130318IPR06658%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN.

In March 2013, the LIBE Committee, taking into account the Report and submissions of other committees of the Parliament, began deliberating the Regulation. In all, over 3,000 proposed amendments to the Regulation were considered.[51]

c. The Regulation's Progress within the Council

Progress in relation to the Regulation was to be a key priority of the Irish Presidency of the Council.[52] Reding acknowledged as much in March 2013 when she noted (notwithstanding the wide ranging changes being discussed by the LIBE Committee in the Parliament) that "all the elements are falling into place" to "make decisive political progress on this critical dossier under the Irish Presidency [of the Council]."[53] On March 1, 2013, the Irish Presidency published a note regarding its progress on the Regulation,[54] which addressed the most common critique—that it was too prescriptive in nature (the Regulation was designed to harmonize data protection law by replacing Directive 95/46/EC (the Directive) which is a largely "principles based" piece of legislation). The note suggested amendments to the Regulation, notably by introducing a greater emphasis on the "risk-based approach," a shift away from the perceived prescriptiveness of the Regulation.

On May 31, 2013, the Justice and Home Affairs (JHA) Committee of the Council released a compromise draft of the Regulation to begin debating the instrument at Council level. This draft was prepared in tandem with the debates that were taking place simultaneously in the LIBE Committee of the Parliament and will ultimately form the basis of the Council's position. The draft text echoed the note discussed above from the Irish Presidency—seeking to row back on some of the more prescriptive aspects of the Regulation and narrow its focus.[55]

At the same time that the Council produced a draft compromise text, debates took place as to the form it should take. The Commission had chosen a regulation that would be directly applicable across all twenty-eight Member States of the European Union.[56] This is consistent with the key goal of the Commission—harmonization of European data protection law—addressing a frequently quoted criticism that the Directive was implemented with important variances in its application and enforcement across the Member States and that it had a negative effect on multinational corporations. It was noted, however, that not all Member States were in favor of proceeding this way. In a note produced with the

51. *See Subject Files: Data Protection*, EUR. PARLIAMENT, http://www.europarl.europa.eu/committees/en/libe/subject-files.html?id=20120514CDT45071#menuzone (last visited Feb. 10, 2014).

52. *See* IRISH PRESIDENCY OF THE COUNCIL OF THE EUR. UNION, PROGRAMME OF THE IRISH PRESIDENCY OF THE COUNCIL OF THE EU: FOR STABILITY, JOBS AND GROWTH (2013), *available at* http://www.eu2013.ie/media/eupresidency/content/documents/EU-Pres_Prog_A4.pdf.

53. Viviane Reding, Vice-President of the Eur. Comm'n, Justice Comm'r, Intervention in the Justice Council (Mar. 8, 2013), *available at* http://europa.eu/rapid/press-release_SPEECH-13-209_en.htm.

54. *Note from the Presidency to the Council on the '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)*, 6607/1/13; REV 1 (Mar. 1, 2013), *available at* http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%206607%202013%20REV%201&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F13%2Fst06%2Fst06607-re01.en13.pdf.

55. *Note from the Presidency to the Council on the '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)*, 10227/13 (May 31, 2013), *available at* https://www.huntonprivacyblog.com/wp-content/uploads/2013/06/st10227.en13.pdf.

56. Croatia became the twenty-eighth EU Member State on July 1, 2013.

Council's compromise text, it was noted that some eight Member States (Belgium, the Czech Republic, Denmark, Estonia, Hungary, Sweden, Slovenia, and the United Kingdom) expressed a preference for a directive that would allow Member States a certain amount of latitude in transposing it into national law.[57]

d. The Parliament's Compromise Text

On October 21, 2013, after many months of committee hearings and debate, the Parliament, through the LIBE Committee, approved its own compromise text of the Regulation.[58] Some features of the Parliament's compromise text are worth highlighting:

- a new definition of "pseudonymous" data was proposed;
- the "legitimate interests" basis for processing data without consent in limited circumstances was proposed in a way that is similar to its current incarnation under the Directive;
- new data subject rights were introduced, and, in particular, it was proposed that a data controller would have to provide notice to data subjects where their personal data was provided to public authorities in the previous twelve months (this proposal was undoubtedly influenced by the "PRISM" and related governmental surveillance controversies that also played out during the course of 2013);
- the data protection officer's role would be reinforced with a proposal that the minimum term be extended from the two years in the Commission's draft to four years; and
- the proposed twenty-four hour breach notification deadline was removed and replaced with a requirement that data breaches be reported "without undue delay."[59]

e. Prospects for the Regulation's Future

The position of the European Commission is clear and has been since the Commission's proposal of the Regulation in January 2012. The position of the Parliament was made clear as of October 2013, with their approval of a draft compromise text led by the LIBE Committee. The last body that needs to formally adopt a position is the Council. The most recent significant development in that body came on October 25, 2013, with its adoption of a set of "conclusions" regarding the Regulation.[60] One such conclusion is that the passing of a robust data protection reform package is "essential for the completion of the Digital Single Market by 2015." This was widely interpreted as meaning that any

57. Hunton & Williams LLP, *Council of the European Union Releases Draft Compromise Text on the Proposed EU Data Protection Regulation*, PRIVACY AND INFO. SECURITY L. BLOG (June 4, 2013), https://www.huntonprivacyblog.com/2013/06/articles/council-of-the-european-union-releases-draft-compromise-text-on-the-proposed-eu-data-protection-regulation/.

58. Eur. Parl., *Civil Liberties MEPs Pave the Way for Stronger Data Protection in the EU*, EUR. PARLIAMENT (Oct. 21, 2013, 8:37 PM), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20131021IPR22706%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN.

59. *WSGR Alert: European Parliament Adopts Compromise Amendments on Data Protection Regulation*, WILSON SONSINI GOODRICH & ROSATI (Oct. 23, 2013), http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-compromise-amendments.htm.

60. Council of the Eur. Union, Draft Conclusions No. 12398/13 of Oct. 23, 2013, CO EUR-PREP 38, *available at* http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2012398%202013%20INIT.

formal Council position on the Regulation is being postponed until after the Parliament elections in May 2014. If this proves to be the case (although perhaps too much is being read into the referenced conclusion), it will push back the introduction of the Regulation until at least 2016. The Commission and the Parliament will likely continue to put pressure on the Council to expedite its deliberations. In any case, there is quite a lot of further work still to be done, so we remain far from being able to accurately predict if and when the Regulation will be adopted.

3. *Action of DPAs with Respect to Privacy Policies*

France's DPA (*Commission Nationale de l'Informatique et des Libertés*) (CNIL) announced on September 27, 2013,[61] that it is initiating a formal procedure that may lead to sanctions against Google Inc. for breaches of paragraph II of Article 32 of France's data protection legislation (French DP Law)[62]

The French order and enforcement actions of other DPAs relate to Google's global privacy policy that was introduced in 2012 (and last modified on June 24, 2013).[63] Google's Privacy Policy, which replaced individual privacy policies for the various Google services, was the subject of correspondence between Google and the WP, of which the CNIL is a member. The WP claimed that the Privacy Policy did not comply with EU data protection law, especially in connection with information requirements regarding the purpose of data collection and the use of such data, which were then bundled together in one privacy policy although the purpose and use of data collection might differ from service to service.[64] The CNIL was given the lead role to discuss with Google.[65]

Late in 2012, the WP set out recommendations with which Google was asked to comply within four months to upgrade its privacy policy practices.[66] After such period, without implementation by Google of "any significant compliance measures," six DPAs announced on April 2, 2013, that they had launched enforcement actions against Google.[67]

---

61. *Google: Failure to Comply Before Deadline Set in the Enforcement Notice*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (Sept. 27, 2013), http://www.cnil.fr/english/news-and-events/news/article/google-failure-to-comply-before-deadline-set-in-the-enforcement-notice/.

62. Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of Jan. 6, 1978 on Information Technology, Data Files, and Civil Liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 7, 1978, pg. 227 (Fr.), *available at* http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (English translation).

63. *Privacy Policy*, GOOGLE (Dec. 20, 2013), https://www.google.com/intl/en/policies/privacy/.

64. *See, e.g.*, Letter from Isabelle Falque-Pierrotin et. al, Commission Nationale de l'Informatique et des Libertés, to Larry Page, CEO, Google Inc., (Feb. 27, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf.

65. *See* Letter from Jennifer Stoddart et. al, Privacy Comm'r, Can., to Larry Page, CEO, Google Inc. (Feb. 2, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130618_letter_to_google_glass_en.pdf.

66. Letter from Article 29 Data Protection Working Party, Eur. Comm'n, to Larry Page, CEO, Google Inc. (Oct. 16, 2012), Appendix, 5–9, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_google_privacy_policy_recommendations_cnil_en.pdf.

67. *Google Privacy Policy: Six European Data Protection Authorities to Launch Coordinated and Simultaneous Enforcement Actions*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (Apr. 2, 2013), http://www.cnil.fr/english/news-and-events/news/article/google-privacy-policy-six-european-data-protection-authorities-to-launch-coordinated-and-simultaneo/.

The CNIL's June 20, 2013, order to comply with French law was part of this larger set of enforcement actions taken simultaneously in six EU countries (France, Spain, United Kingdom, Germany, the Netherlands, and Italy). In the CNIL's order, Google was to, within three months:

- Define specified and explicit purposes to allow users to understand practically the processing of their personal data;
- Inform users . . . with regard to the purposes pursued by the controller of the processing implemented;
- Define retention periods for the personal data processed that do not exceed the period necessary for the purposes for which they are collected;
- Not proceed, without legal basis, with the potentially unlimited combination of users' data;
- Fairly collect and process passive users' data, in particular with regard to data collected using the "Doubleclick" and "Analytics" cookies, "+1" buttons or any other Google service available on the visited page;
- Inform users and then obtain their consent in particular before storing cookies in their terminal.[68]

The CNIL summarized the DPAs' bases for enforcement actions as insufficient information, undefined or insufficiently defined data retention periods, and unlimited combination of data.[69]

The procedure initiated on September 27, 2013, may lead to sanctions under French DP Law Article 45, the imposition of a financial penalty under Article 47[70] (€150,000 maximum in case of a first breach and up to €300,000 "where similar previous offences have been committed"[71]), and an injunction to cease the processing.[72] The CNIL may make the sanctions, if any, public and order their publication in the journals, newspapers, or "other media" it designates, at Google's expense.[73]

Although it is not now known whether Google will be sanctioned and, if so, how much the penalty will be, it should be noted that the CNIL imposed a €100,000 fine on Google in 2011 for violation of the French DP Law.[74]

In related proceedings in the Netherlands, the Dutch DPA issued its report of definitive findings of its investigation on November 28, 2013, in which it found Google to be in breach of the Dutch data protection act regarding the combining of personal information, since the introduction of Google's new Privacy Policy. The Dutch DPA has invited

68. *See CNIL Orders Google To Comply with the French Data Protection Act, Within Three Months*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (June 20, 2013), http://www.cnil.fr/linstitution/actualite/article/article/cnil-orders-google-to-comply-with-the-french-data-protection-act-within-three-months/.

69. *See* Letter from Isabelle Falque-Pierrotin et. al, *supra* note 64.

70. Law 78-17 of Jan. 6, 1978, art. 47 (Fr.).

71. *See Role and Responsibilities*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (2013), http://www.cnil.fr/english/the-cnil/role-and-responsabilities/.

72. Law 78-17 of Jan. 6, 1978, art. 45 (Fr.).

73. *Id.* art. 46.

74. *See* W. Gregory Voss et al., *Privacy, E-Commerce, and Data Security*, 46 INT'L LAW 97, 102–103, I(B)(2)(b) (2012). In that case, publication of the decision was made on the website of the CNIL and on http://legifrance.gouv.fr, an official French Government legal site.

Google to attend a hearing, after which it will decide whether it will take enforcement measures against Google.[75]

II. Developments in the United States

With respect to the United States, this article is divided into (1) federal developments and (2) a state development in California.

A. Federal Developments

In April 2013, the U.S. Supreme Court declined to hear a case that tested the extent to which personal emails are protected by federal law.[76] The appeal sought to have the Supreme Court resolve two conflicting opinions, one from South Carolina[77] and one from California,[78] as to whether both unread and read emails are considered "in electronic storage" and would thus be entitled to protection and considered private under the Federal Stored Communications Act (FSCA).[79] Under current law, communications falling under the FSCA, such as postal mail, are entitled to a higher level of protection, and a probable cause warrant issued by a judge must be obtained in order for the government to legally access them. If emails are not considered to fall within the scope of the FSCA, however, the government may request access to them via a subpoena, which does not require judicial oversight. No Supreme Court decision has yet decided whether emails, opened or unopened, are entitled to the higher level of protection required by the FSCA, and the Supreme Court did not issue an explanation for their refusal to hear the case.

In November 2013, the Supreme Court also declined to hear a case that challenged the legality of the National Security Agency's (NSA) bulk collection and storage of telephone metadata from any citizen.[80] The case questioned whether the order issued by the Foreign Intelligence Surveillance Court (FISC) in April 2013, requiring cellular provider Verizon to turn over information, including cellular phone calls and internet exchanges made entirely within the United States, exceeded the court's statutory authority to authorize foreign surveillance.[81] Currently, this type of government surveillance remains legal, despite domestic and international criticism as to whether it violates privacy rights. The case may still be brought through the lower courts in the United States, however, and cases regarding the FISC's actions are currently pending in several district courts.

---

75. Press Release, Dutch Data Prot. Auth., Dutch DPA: Privacy Policy Google in Breach of Data Protection Law (Nov. 28, 2013), *available at* http://www.dutchdpa.nl/Pages/pb_20131128-google-privacypolicy.aspx.

76. Jennings v. Jennings, 736 S.E.2d 242 (S.C. 2012), *cert. denied*, 133 S. Ct. 1806, 185 L. Ed. 2d 812 (2013) (cert. denied as Jennings v. Broome).

77. Jennings v. Jennings, 736 S.E.2d 242 (S.C. 2012).

78. Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

79. 18 U.S.C. §§ 2701–12 (2012).

80. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things [etc.], Docket No. 13- 80, Secondary Order (F.I.S.C. Apr. 25, 2013) (Secondary Order), *cert. denied*, 134 S. Ct. 638 (2013) (cert. denied as *In re* Elec. Privacy Info. Ctr.).

81. 50 U.S.C. § 1861 (2006).

At the appellate level, the Ninth Circuit held that Google violated the Federal Wiretap Act[82] by collecting information, such as passwords and emails, from internet users of unencrypted Wi-Fi networks for its Street View photo mapping service.[83] The Ninth Circuit and the District Court rejected Google's argument that the information collected constituted "electronic communication" that was "readily accessible to the general public"[84] and thus was an exception under the Wiretap Act. Judge Jay Bybee stated, "[s]urely Congress did not intend to condone such an intrusive and unwarranted invasion of privacy when it enacted the Wiretap Act."[85] Thus, the Ninth Circuit held that the Federal Wiretap Act protects information transmitted over Wi-Fi networks.

The U.S. District Court for the District of New Jersey ruled that non-public Facebook wall posts are protected under the FSCA.[86] The district court determined that the statutory language protects "(1) electronic communications, (2) that were transmitted via an electronic communication service, (3) that are in electronic storage, and (4) that are not public."[87] The court ruled that Facebook wall posts that are configured to be inaccessible by the general public are protected under the FSCA.[88] But, in this case, because the plaintiff's Facebook wall posts were volunteered to the defendant employer by a fellow employee who had access to the posts, the defendant employer fell within the exception to the FSCA that exempts conduct authorized by a user of an internet service with respect to a communication intended for that user.

The U.S. District Court for the District of Vermont ruled that there can be no expectation of privacy for information shared over peer-to-peer file sharing networks.[89] The defendants were charged with possession of child pornography and argued that the evidence gathered by a peer-to-peer search tool should be suppressed because it was illegally obtained. Judge Christina Reiss denied defendants' motion to suppress, stating that "either intentionally or inadvertently, through the use of peer-to-peer file sharing software, [d]efendants exposed to the public the information they now claim was private."[90] The automated search tool used by the government in this investigation did not open or download any of the files on defendants' computers but did identify files that the defendants had themselves made publicly available for download on the Internet.

B. State Developments: California

The Governor of California approved California Senate Bill 568[91] (the Bill) on September 23, 2013, (Chapter 336, Statutes of 2013) thus adding a Chapter 22.1 on Privacy Rights for California Minors in the Digital World to Division 8 of California's Business

82. 18 U.S.C. § 2511 (2008).
83. Joffe v. Google, Inc., 729 F.3d 1262 (9th Cir. 2013).
84. *Id.* at 1264.
85. *Id.* at 1272.
86. Ehling v. Monmouth-Ocean Hosp. Serv. Corp., No. 2:11 Civ. 03305 (WJM), 2013 WL 4436539 (D.N.J. Aug. 2013).
87. *Id.* at 6.
88. *Id.* at 8.
89. United States v. Thomas, No. 5:12-cv-00037, 2013 U.S. Dist. LEXIS 159914 (D. Vt. Nov. 2013).
90. *Id.* at 47.
91. S. B. 568, 2013–14 Leg. Sess. (Cal. 2013-2014), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

and Professions Code, relating to the Internet. Its operative provisions will come into force on January 1, 2015.[92]

The Bill aims to protect minors, defined as natural persons less than eighteen years of age, who reside in California.[93] The Bill is divided into two principal parts: (1) it prohibits certain advertising and marketing to minors (Section 22580), and (2) it furnishes a digital "eraser" right or "right to be forgotten" for minors (sec. 22581), which will be discussed in order below.

1. *Prohibitions on Certain Advertising and Marketing to Minors*

The Bill prohibits an operator (Operator) of an Internet web site, service or application, or a mobile app (Media) directed to minors from advertising certain products or services on such Media.[94] If an advertising service is used and is informed that the Media are directed at minors, the Operator may benefit from an exception, and the advertising service would be subject to the prohibition.[95] An Operator is also prohibited from directly marketing or advertising such products or services to a minor he knows is using such Media[96]; however, a reasonable good faith actions exception is available.[97] In addition, such an Operator, if his Media are directed to minors or if he has actual knowledge that they are being used by minors, shall not knowingly use, disclose, or compile a minor's personal information or allow another party to do the same (if he has actual knowledge that such prohibited actions are for marketing or advertising certain products to such minor).[98]

The certain products or services may be analyzed as those that are potentially harmful to the minor's physical health (e.g., alcoholic beverages) or safety (e.g., firearms and handguns), or related to certain behavior (e.g., tickets in a lottery game), or irreversible actions (e.g., body branding).[99] The Bill's text should be consulted for details.

2. *A Digital "Eraser" Right or "Right to Be Forgotten" for Minors*

The second part of the Bill furnishes the "eraser" right or "right to be forgotten" for minors. An Operator of a Media directed to minors or with actual knowledge that a minor is using his Media must, *inter alia*, allow a registered user minor to remove or, if preferred by the Operator, to request and obtain removal of content or information he or she posted and must provide notice of such right with clear instructions on how to exercise it.[100]

92. On that date, CA Sen. Bill 568 will be included in the California Law database. *See Frequently Asked Questions*, CAL. LEGIS. INFO., *available at* http://leginfo.legislature.ca.gov/faces/home.xhtml# (follow "FAQ" link, then follow "How can I tell how current a version of the code is?" link) (last visited Feb. 10, 2014).

93. S. B. 568, § 22580(d).

94. *Id.* § 22580(a).

95. *Id.* § 22580(h)(1)–(2).

96. *Id.* § 22580(b)(1). This Section sets out elements to be used in application of an actual knowledge standard.

97. *Id.* § 22580(b)(2).

98. *Id.* § 22580(c).

99. *Id.* § 22580(i).

100. *Id.* § 22581(a).

In certain circumstances, such requirement to erase or eliminate content or information does not apply, thus limiting the interest of the right. For example, where the content or information was posted by a third party, or anonymized by the Operator or where the minor received compensation or consideration for furnishing the content, the requirement does not apply.[101]

Law enforcement officials may continue to be able to obtain content or information from the Operator by court order or under law,[102] and other exceptions may apply.[103]

III. Developments in Africa

A. Cape Verde

On September 17, 2013, the Cape Verdean National Assembly issued Law 42/VIII/2013 (the Law).[104] Though directed to the incorporation of the Cape Verdean Data Protection Agency (CV DPA), the Law aims at finally establishing an effective body that will regulate foreign and local companies involved in personal data transfers, because all data processing issues will be resolved within the scope of the CV DPA. The Law will be fully implemented in January 2014, because it will otherwise adversely impact the Cape Verdean fiscal budget.[105] We describe the CV DPA's core features, scope, composition, and powers.

The CV DPA may investigate and collect any information it deems necessary to fulfill its supervisory functions. It is an influential agency that can order companies to temporarily or permanently cease transferring data or order them to erase the data or prescribe a maintenance time.[106] It has a wide scope. The CV DPA may grant transfer data authorizations, require companies to file notifications to alert the data subject and the CV DPA, and update previous applications when exchanging personal data. It may issue guidelines, compile best practice manuals, and inquire into the lawfulness of data processing, i.e., upholding the purpose limitation principle. The agency will analyze complaints, respond to data subject petitions, and take all necessary steps to satisfy complainants, including levying heavy fines.

Three distinguished individuals elected by the National Assembly on the basis of competence and integrity will make up its board for six year terms, assisted by experienced professionals who may conduct research and issue opinions on complex matters.[107] With broad discovery powers, the CV DPA may collaborate with other agencies and initiate legal proceedings intended to enforce the data protection rules (raising the bar of African jurisdictions).

---

101. *Id.* § 22581(b).

102. *Id.* § 22581(c).

103. *Id.* § 22581(d).

104. Pub. L. No. 42/VIII/2013, de 17 de setembro de 2013, Boletim Oficial [B.O.] Bulletin Official 48 Série I (Cape Verde), *available at* http://www.parlamento.cv/GDiploApro3.aspx?codDiplomasAprovados=207.

105. *Id.* art. 51.

106. *Id.* art. 8.

107. *Id.* arts. 13, 14.

On the same day, the National Assembly issued Law 41/VIII/2013,[108] which modifies Article 22[109] of the General Data Protection Statute, previously empowering a Parliamentary Commission to play the role now performed by the CV DPA. Though not yet active (to the best of our knowledge), a fully operational CV DPA means that notification requirements, mandatory under the current law when personal data is being processed, together with the provisions of the General Data Protection Statute, will be vigorously enforced.

108. *See generally id.*

109. Regime Jurídico Geral De Protecção de Dados Pessoais a Pessoas Singulares [General Legal Regime of Personal Data Protection to Individuals], Lei No. 133/V/2011, de 22 de janeiro de 2001, BOLETIM OFICIAL [B.O.] BULLETIN OFFICIAL, art. 22 (Cape Verde), *available at* http://www.afapdp.org/wp-content/uploads/2012/01/Cap-vert-Lei-n%C2%B0133-V-2001-do-22-janeiro-20011.pdf (stating that the Parliamentary Commission is in charge of providing the necessary oversight to the Data Protection Legislation).