Bloomberg Law Reports® Technology Law

Social Media, Cloud Computing and European Philosophy: An Examination of Proposed Amendments to Directive 95/46/EC and Their Possible Effects on U.S. Multinational Corporations

James A. Sherer, Redgrave LLP

On November 4, 2010, the European Commission released a proposal for "a comprehensive approach on personal data protection in the European Union" (the "Proposal") which would modify current Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 ("Directive 95/46").[1] The Commission's Proposal sought to modernize the EU legal system for the protection of personal data, and carried with it a mandate to present legislative proposals in 2011.[2] The Proposal was shared with interested parties and debated throughout the first-half of 2011. The language of the Proposal, as well as the outcomes of those subsequent debates, highlighted the EU's concerns about the current practice of data privacy in a variety of arenas, including international business.

While the most direct effects of the Proposal would fall on the operation of the European Union's Member States, some of the Proposal's language and subsequent debate necessarily impacts multinational corporations, including those based in the United States. The most significant areas touched upon include:

- Member State Autonomy in the Evaluation of Safe Data Practices
- Sensitive Data stored in Cloud Computing Systems
- Information shared on U.S.-based Social Networks
- The Philosophy of EU Privacy and European Personal Data

This article explores the historical (and current) operation of Directive 95/46, and examines the impact that this new Proposal might have on U.S. multinational corporations, both from the Proposal's written language and the political discussions which surround it.

The History of Directive 95/46/EC

At least facially, Directive 95/46 had a straightforward aim: to "protect the fundamental rights and freedoms of natural persons, and in particular, their right to privacy with respect to the processing of personal data."[3] To be clear, in practice "natural persons" likely meant European citizens. And, before the enactment of Directive 95/46 and its subsequent implementation in Europe's Member States, each Member State had to square its own aims – and policies – with the idea of protecting *all* of Europe's citizens, not just one Member State's citizens.

This was an extraordinary political exercise, and the Parliament certainly understood that from the onset. Thus, the second aim of the Directive: to prohibit Member States from restricting or prohibiting "the free flow of personal data *between* Member States connected with the protection afforded under [Directive 95/46]."[4] Due to the tension of protecting each Member State's individual prerogatives while still harmonizing a European legislative environment, it took a number of years before the Directive was enacted in each Member State,[5] with a moratorium on enforcement that was extended until July, 2001.[6]

A third aim, or perhaps more accurately, a concern of the Directive, dealt with the sharing or transmission of personal information to "countries found to be lacking in data protection measures."[7] For the United States, this EU concern led specifically to an agreement between the EU and the United States Dept. of Commerce ("DOC") in 2000[8] that met the moratorium's July 2011 extension. Through that agreement, the European Commission (the "Commission") approved and subsequently ratified the DOC's package of proposed Safe Harbor Privacy materials, comprised of the Safe Harbor Privacy Principles and a set of Frequently Asked Questions ("FAQs") supplementing the Principles.[9]

Under the DOC's Safe Harbor program, companies in the United States were referred to the DOC's website, where they were reminded that any "U.S. organization that is subject to the jurisdiction of the Federal Trade Commission ("FTC") or U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation ("DOT") may participate in the Safe Harbor."[10] Here, U.S. organizations for which the Safe Harbor was available were able to "publicly commit to adherence with seven safe harbor principles aligned with the Directive's privacy principles."[11] Although as of May 12, 2003 there were only "328 companies . . . listed on the US Department of Commerce's Safe Harbor website as currently complying with Safe Harbor Principles,"[12] it is clear that U.S. organizations recognized the benefits of marching to the EU's drum and access to European markets. That participation number grew steadily to the 2,689 organizations listed as of summer, 2011.[13] Finally, if U.S. organizations were ineligible for the DOC's Safe Harbor, they still had the ability to utilize Commission-approved, standard contractual clauses for data transfers to non-EU countries.

The Proposed Amendments to Directive 95/46

On November 4, 2010, the Commission released its Proposal for "a comprehensive approach on personal data protection in the European Union" with a view to modernizing the EU legal system for the protection of personal data and with a mandate of presenting legislative proposals in 2011.[14] This proposal acknowledged that, while Directive 95/46 was still valid,[15] changes in technology and globalization required refinements to the Directive. This echoed concerns that had long resounded in the United States, as wryly noted in the IACIS[16] observation that, "the environment fostered by the rapid increase in Internet based activities raises issues that might not have been foreseen in 1995, when Directive language was being finalized and the Internet was in its early stages of commercialization. The end-result is a law that does not fully recognize the competitive environment in which U.S. businesses find themselves."[17] The Commission certainly acknowledged that concern, and turned its attention to the specifics of where Directive 95/46 needed to mature. Here, the Commission focused on several key points: the activities of Member States acting independently; some rapidly-evolving technologies (*e.g.*, Cloud Computing and Social Media); and the European philosophy that underlay the recognition of data privacy as a personal (perhaps European) "right" that needed protection.

— Member State Autonomy in the Evaluation of Safe Data Practices

Under the direction of Directive 95/46, EU Member States have the affirmative obligation to determine

if safe data practices are in place for those parties it does business or exchanges information with. But, because of the EU's use of a directive, to some degree each Member State defines *what* safe data practices are. Because there is no international or EU standard for this definition, it stands to reason that Member States' evaluations of one non-EU state's data practices might differ between Member States. The Proposal specifically noted a concern with these types of international practices, highlighted in the Proposal's § 2.4. - *The global dimension of data protection*[18] and expressed its concerns regarding the autonomy Member States currently enjoy.

The Proposal's evaluation of the potential results of autonomous practice was also voiced by so-called stakeholders, "particularly multinational companies," of the "lack of sufficient harmonisation between Member States' legislation on data protection, in spite of a common EU legal framework"[19] where the multinationals could not rely on advice from one Member State as being sufficient for subsequent interactions with a different Member State. The Commission agreed, and its Proposal's evaluation focused on the current corporate practice where multinationals negotiate agreements with individual Member States, indicating that (and as noted by the commenting multinationals) this self-directed process has the ability to create agreements that both the signing party and Member State are comfortable with, but that the whole of the EU might not agree to. This concern might also implicate those multinationals who availed themselves of Commission-approved, standard contractual clauses for data transfers to non-EU countries outside of the U.S. Department of Commerce's Safe Harbor Provisions.

Commenters actively involved in the Proposal's subsequent debate agreed. In his March 29, 2011 Draft Report "on a comprehensive approach on personal data protection in the European Union," Parliament Rapporteur Axel Voss[20] highlighted the need for a "strong European and international data protection regime" for "the flow of personal data across borders," but stated that "current differences in data protection legislation and enforcement are affecting the global economy and the single European market."[21] Mr. Voss also focused on "further clarification of the rules on applicable law with a view to delivering the same degree of protection for individuals irrespective of the geographical location of the data controller."[22]

Further, Mr. Voss named one brief section of concerns "Strengthening the global dimension of data protection" and called on the commission to "define core EU data protection aspects to be used for all types of international agreement." Mr. Voss also asked that the Commission better specify "the criteria and requirements for assessing the level of data protection in a third country or an international organisation."[23] Here, Mr. Voss added certainty to the direction the Commission will take with its proposed modifications: the current practice of Member State autonomy is not working for stakeholders to the process, and further clarification is needed for what proper, EU standards should be.

— Improving International Data Transfers with a Focus on Cloud Computing and Social Media

Another Proposal bullet point was dedicated to "[a]ddressing globalisation and improving international data transfers."[24] Here, the Commission indicated that the concern was twofold: processing EU information outside the EU clouded the issue of which law applied to that processing, and attempts to clarify that issue only succeeded in further hindering international commerce:

> [T]he increased outsourcing of processing, very often outside the EU, raises several problems in relation to the law applicable to the processing and the allocation of associated responsibility. As to international data transfers, many organisations considered that the current schemes are not entirely satisfactory and need to be

> reviewed and streamlined so as to make transfers simpler and less burdensome.[25]

The Proposal also addressed the application of data protection principles to new technologies (*e.g.*, Cloud Computing)[26] and new services (*e.g.*, Social Media sites).[27] This paints targets firmly on those multinational corporations storing European data in the "cloud," or accreting European data through Social Media customer or client interaction. These are, of course, not new issues. The effect of Directive 95/46 had already caused concerns for multinational corporations, with commentators noting that, "the extraterritorial effect of [Directive 95/46] is to create problems for US and other nations' companies that deal with personal data from EU nations, making these firms subject to the adequate protection provisions of the Directive."[28]

These concerns were taken up by the EU Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data (the "Article 29 Working Party"). The Article 29 Working Party is an "independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC"[29] that sought to specifically determine the continued validity of Directive 95/46, but also bring its principles up to modern effect. On November 19, 2010, the Article 29 Working Party brought its influence to bear and called for a "strict general privacy agreement with [the] United States."[30] This followed what the Article 29 Working Party called the "unsatisfactory result – from a data protection point of view – of the negotiations on the TFTP[31] II Agreement [that allowed] the United States to obtain access to information on international bank transfers."[32] It also followed a concern where the Article 29 Working Party asked for "very strict rules for the onward transfer of EU-originating data to other countries or non-law enforcement agencies within the US."[33]

The March 16, 2011 meeting of the "European Privacy Platform" group of the European Parliament also gave indications as to where the Proposal might go after consideration and debate. Specifically, Commissioner Viviane Reding[34] highlighted the idea of European data *protection*, regardless of data *location*, indicating that EU law should apply irrespective of the location of and means by which data is processed. In her statements, Ms. Reding continued on the Proposal's Social Media theme, and focused further on online services targeting EU consumers. Ms. Reding stated that those services, including "U.S.-based social networks," should be compelled to comply with EU laws concerning data privacy.

Mr. Voss[35] agreed with Ms. Reding, "that EU law should apply wherever the data of EU citizens are processed" and then criticized the presently-constituted EU-U.S. Safe Harbor agreement. Mr. Voss's criticisms of international protections were not limited to the United States; his concerns about data privacy abroad were further pronounced in questions and remarks about Cloud Computing, where Mr. Voss stated that the "processing of sensitive data generally should not be allowed in [C]loud [C]omputing systems, or only if the relevant servers are located in the EU."[36] Ms. Reding then further "reiterated her point that EU law should apply when EU data are processed anywhere in the world."[37]

— The Philosophy of the Commission's Proposal

The Commission's aims did not stop with its concrete concerns about international or non-EU evaluations. Instead, the Commission's sights were set much higher - presenting an international standard on data privacy that focused nearly exclusively on European data privacy ideals. The Commission's statement on this point was anything but subtle:

> The EU legal framework for data protection has often served as a benchmark for third countries when regulating data protection. Its effect and impact, within and outside the Union, have been of the utmost

> importance. The European Union must therefore remain a driving force behind the development and promotion of international legal and technical standards for the protection of personal data, based on relevant EU and other European instruments on data protection. This is particularly important in the framework of the EU's enlargement policy.[38]

It may be true that an enlightened Europe must lead the way to proper data privacy practices. Or, at the very least, the EU may succeed in dragging the United States along as the EU further modifies its data privacy rules. Perhaps an "enlightened data privacy" view in modern computing simply demonstrates one of the EU's fundamental, philosophic points. Or perhaps, as some articles have noted, this sentiment is more recent in origin and the EU's data privacy views "were strengthened after repressive regimes such as the Third Reich used personal information in a way that fueled the later development of modern data privacy laws throughout the 70's, 80's and 90's by many European states."[39] But regardless of the philosophy's origins, as others have observed, when it comes to the attitudes of citizens of the EU and United States, there is a true "difference [between] basic values. Outside the core physical space of the home, Americans do not care particularly about privacy."[40] Perhaps the United States' ambivalence towards privacy will ensure European success when developing an international right to privacy standard, or specifically, the arguably philosophic points raised in the Proposal: of the "principle of data minimization," the "rights of access, rectification, erasure or blocking of data," the "so-called right to be forgotten," and the guarantee of "data portability."[41]

This philosophic shift in practice, if not belief, may come sooner rather than later. In a press release dated April 20, 2011, Mr. Voss stated that the EU and the United States were "ready to reach agreements ... on data protection issues right across the board."[42] However, at that time, Mr. Voss acknowledged that a key concern was a continued firm standing on the EU's "core values."[43] Mr. Voss also acknowledged that, at least with regards to the passenger name record ("PNR") agreement between the EU and the United States, the European Commission was "actually conducting the negotiations."[44] Here, Mr. Voss reiterated the European concern with privacy ideals and provided an accurate contrast – that of the United States' concerns with garnering travel data to fight terrorism. This contrast brings a focus back to what United States citizens, at least as a whole, consider truly important: safety first, business success second – and *maybe* privacy – if it is offered – and does not cost too much money.

Conclusion

The Proposal to modify Directive 95/46 is still under debate and revision, but some clear signposts are emerging to help guide multinationals that must take European concerns seriously. The EU is concerned with varying standards regarding safe data transfer amongst its Member States and will likely restrict the exercise of that prerogative to more clearly-defined rules and regulations. The EU and its representatives are also very concerned with the use of Social Media data collection and Cloud Computing data processing. Here, updates to Directive 95/46 will specifically address these topics, with an eye towards European data privacy ideals. Finally, each of these concerns – and others sure to emerge under the guise of debate and revision – will take on the unique EU gloss of data privacy "philosophy" as discussed above. The Proposal will incorporate data minimization; rights of access, rectification, erasure or blocking of data; the right to be forgotten; and support the portability of EU citizens' data.

What can multinationals do in the meantime? Multinationals can begin with refining the narrative inherent within their existing – and, perhaps more importantly and availably – future processes. While the specifics of the updated EU Privacy Regime are not yet written, or at least not yet set in stone, the

philosophical aims are clear. For existing multinational practices, even audits are expensive,[45] and at this point even if practices that run contrary to the EU's political winds are identified, it may be inappropriate to modify those practices until they are memorialized in rule format. There will most assuredly be a transition period provided. However, for new multinational-*contemplated* practices, an understanding of the Proposal's philosophy will be more valuable in the near-term. The installation of a new Cloud Computing service for global data should take Mr. Voss's concerns to heart, just as recognition of the EU's concerns with Social Media must cause multinationals to reevaluate new customer interaction programs. In fact, forearmed with an understanding of where EU Privacy regulation is going, a savvy multinational can position itself to be the first out of the gate to comply with changing EU regulations – and the first to reap any newly-available rewards in a changing European market.

James A. Sherer is a Partner at Redgrave LLP's Washington, D.C. office.

---

1 Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: *A comprehensive approach on personal data protection in the European Union*, Nov. 4, 2010, *available at* http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (last visited June 30, 2011).

2 *Id*.

3 European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Council Directive 95/46"), *Article 1: Object of the Directive No. 1*, Journal of the European Communities of 23 November 1995 No L. 281 31 (available online in all official languages through www.europa.eu).

4 Council Directive 95/46, *Article 1: Object of the Directive No. 2*. (emphasis added).

5 European Commission Directorate-General for Justice, *Status of Implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data*, *available at* http://ec.europa.eu/justice/policies/privacy/law/implementation_en.htm (last visited June 30, 2011).

6 James E. Weber and Richard Paulson, *The EU'S Data Protection Directive Headed for the Rocks*, IACIS 748, 750 (2003) (citing Harvey, J.A & Verska, K.A. (2001) The Computer and Internet Lawyer, 18(4), 17-20), *available at* http://www.iacis.org/iis/2003_iis/PDFfiles/WeberPaulson.pdf (last visited June 30, 2011).

7 Matt Sorensen, *European Union Data Privacy Directive 95-46-EC - Transfer Mechanisms from the European Union to Non-Union Countries*, ISSA Journal at 18 (February 2011) (citing to Council Directive 95/46, Art. 25, p.18, 1995), *available at* http://www.issa.org/Library/Journals/2011/February/Sorensen-European%20Union%20Data%20Privacy%20Directive.pdf (last visited June 30, 2011).

8 World Privacy Forum, *The US Department of Commerce and International Privacy Activities: Indifference and Neglect*, Nov. 22, 2010, *available at* http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf (last visited June 30, 2011).

9 Sorensen, *supra* note 7, at 18, 21.

10 U.S. Department of Commerce - Export.Gov, http://www.export.gov/safeharbor/.

11 Sorensen, *supra* note 7, at 18, 22 (citing to Council Directive 95/46, Art. 25, p.22, 1995).

12 Paulson, *supra* note 6, at 748, 752.

13 U.S. Department of Commerce - Export.Gov, Safe Harbor List, https://safeharbor.export.gov/list.aspx (last visited June 30, 2011).

14 Communication, *supra* note 1.

15 Hunton & Williams LLP, *European Commission Outlines Strategy for Revision of the Data Protection Directive*, Nov. 4, 2010, *available at* http://www.huntonprivacyblog.com/2010/11/articles/european-union-1/european-commission-outlines-strategy-for-revision-of-the-data-protection-directive/ (last visited June 30, 2011).

16 The "International Association of Computer Investigative Specialists." https://www.iacis.com/.

17 Paulson, *supra* note 6, at 748, 750.

18 Communication, *supra* note 1, at 15.

19 *Id*. at 4.

20 Axel Voss is a "German MEP and member of the EPP parliamentary block who is serving as the Parliament's Rapporteur on the Directive." *See* Hunton and Williams LLP, *European Parliament Meeting Offers Update on Review of EU Data Protection Directive*, Mar. 16, 2011, *available at* http://www.huntonprivacyblog.com/2011/03/articles/european-union-1/european-parliament-meeting-offers-update-on-review-of-eu-data-protection-directive/ (last visited June 30, 2011).

21 Axel Voss - *DRAFT REPORT On a Comprehensive Approach on Personal Data Protection in the European Union*, p. 5, March 29, 2011, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-460.636+01+DOC+PDF+V0//EN&language=EN (last visited June 30, 2011).

22 *Id*.

23 *Id*. at 6.

24 Communication, *supra* note 1, at 5.

25 *Id*.

26 *Id*. at 2, 11.

27 *Id*. at 2.

28 Paulson, *supra* note 6, at 748, 749.

29 Article 29 Data Protection Working Party, *Data Protection Authorities Call for Strict General Privacy Agreement with United States*, p.6, Nov. 19, 2010, *available at* http://epic.org/pr_19_11_10_en.pdf (last visited June 30, 2011).

30 *Id*. at 1.

31 The "Terrorist Finance Tracking Program," *available at* http://ec.europa.eu/commission_2010-2014/malmstrom/archive/TFTP%20II%20Draft%20Agreement%2011%20June%20initialled.pdf (last visited June 30, 2011).

32 *Id*.

33 *Id*.

34 Ms. Reding is the "Vice President of the European Commission and Commissioner for Justice, Fundamental Rights and Citizenship." *See* Hunton and Williams LLP, European Parliament Meeting Offers Update on Review of EU Data Protection Directive, *supra* note 20..

35 Mr. Voss is a "German MEP and member of the EPP parliamentary block who is serving as the Parliament's Rapporteur on the Directive." *See* Hunton and Williams LLP, European Parliament Meeting Offers Update on Review of EU Data Protection Directive, *supra* note 20.

36 *Id.*

37 *Id*.

38 Communication, *supra* note 1, at 16.

39 Paulson, *supra* note 6, at 748, 749 (citing George, B.C, Lynch, P & Marsnik, S.J. (2001). U.S. multinational employers: Navigating through the "safe harbor" principles to comply with the EU data privacy directive. American Business Law Journal, 38(4), 735-783).

40 Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Privacy Network*, Michigan Journal of International Law, Vol. 26:807, 808 (May 5, 2005) (citing Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (2004)) available at http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2271&context=faculty_scholarship&seiredir=1#search=%22%2C%20Transgovernmental%20Networks%20vs.%20Democracy%3A%20Case%20European%20Privacy%20Networ%22 (last visited July 7, 2011).

41 Communication, *supra* note 1, at 8.

42 Axel Voss, MEP and EEP Group, *EU and USA Can Agree on Data Protection Issues*, Apr. 20, 2011, *available at* http://www.eppgroup.eu/press/showpr.asp?prcontroldoctypeid=1&prcontrolid=10295&prcontentid=17421&prcontentlg=en (last visited June 30, 2011).

43 *Id*.

44 *Id*.

45 Paulson, *supra* note 6, at 748, 751.

Disclaimer

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.