Federal Trade Commission
Protecting America's Consumers

Appendix B

THE EUROPEAN UNION DIRECTIVE ON THE PROTECTION OF PERSONAL DATA

On the first day of the Workshop, panelists discussed the implications of the European Union Directive on the Protection of Personal Dat online marketplace in the United States.(1) The Directive was designed to harmonize European Union member states' laws governing th treatment of personal information. It will become effective in 1998. As Workshop participants noted, the Directive is forcing scrutiny of da protection policies in both the public sector and private industry in this country.(2)

The Directive comprises a general framework(3) of individual rights and information practices respecting the "processing"(4) of "persona which the Directive defines as "any information relating to an identified or identifiable natural person."(5) The Directive establishes a floo which member states may build enhanced information privacy protections.(6) It requires that member states enact national legislation im its provisions.(7)

The Directive includes fair information practices developed in many countries, including the United States, since the 1970's.(8) It provide processing of personal data be "transparent," i.e., that data subjects be given notice of the processing of their personal information and a opportunity to make decisions about how their personal information is used.(9)

The Directive requires generally that, subject to limited exceptions, personal data may be processed only "if the data subject has unamb given his consent."(10) It requires that, when personal data is to be collected from an individual, he or she must be informed of the identi "controller" of the data,(11) the purposes for which processing of the data is intended, and any other information that guarantees "fair pro of the data.(12) Similar protections apply where personal information about a data subject is not obtained directly from him or her.(13)

The Directive gives individuals a right of access to personal data that is subject to processing by the controller of that data, as well as the correct inaccuracies or to erase or block personal data that is processed in a manner inconsistent with the Directive's standards.(14) Und Directive, the data subject has the right to object to the processing of personal data about him.(15) Finally, the Directive requires membe provide individuals with judicial remedies and a right to compensation for violations of their rights under the Directive.(16)

For the United States and other countries doing business with European Union member states, the critical provision of the Directive is Ar which governs the transfer of personal data to countries outside the European Union. Article 25 requires member states to permit the "tra third country of personal data which are undergoing processing or are intended for processing after transfer . . . only if . . . the third coun question ensures an adequate level of protection."(17) This prohibition is subject to exceptions enumerated in Article 26, including an ex where the controller of the data demonstrates "adequate safeguards," such as appropriate contractual provisions, for protecting the priva fundamental rights of individuals.(18)

Under Article 25, the "adequacy" of non-member states' privacy protections is to be assessed in light of the particulars of a proposed tra data (including the nature of the data, the purpose and duration of the proposed processing of that data, the country in which the data or and the country to which it would finally be transferred) and "the rules of law, both general and sectoral, in force in the third country in qu the professional rules and security measures which are complied with in that country."(19) Where, with respect to a particular proposed t transfer, a country is found not to have an "adequate" level of data protection, the Directive requires member states to prevent any transf same type of data to the country in question.(20) The Directive provides only general guidance regarding the assessment of the "adequa non-member states' privacy protections.

The task of further refining the definition of "adequacy" and developing a methodology for assessing "adequacy" has fallen to the Comm Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, created by the Directive to, among other render an opinion on the level of data privacy protections in non-member states.(21) "Adequacy" standards are currently being hotly deb the European data protection commissioners serving as members of the Working Party.(22) The unsettled nature of the "adequacy" stan reflected in the divergent views of workshop participants regarding the impact the Directive may have on online data collection in, and in transfers of personal information to, the United States.

Participants offered varying perspectives on the question of whether existing data privacy protections in the United States satisfy the Dir "adequacy" standard. One participant argued that U.S. privacy law is not "adequate," within the meaning of the Directive.(23) In this part view, the absence of an overarching federal privacy statute will cause European Union member states to examine individual companies' information practices to measure compliance with the adequacy standard;(24) trade association guidelines will not, in and of themselves indicia of "adequacy."(25) According to this panelist, three aspects of U.S. data protection will likely be problematic from a European pers the lack of "transparency" of information practices, i.e., the difficulty that citizens face in trying to ascertain how their personal information used; the degree to which secondary uses of personal information are incompatible with the purposes for which the information was initia collected; and the piecemeal nature of oversight and enforcement of information practices.(26)

Privacy advocates agreed that current information practices on the Internet would not meet the Directive's adequacy standard, because entities give individuals notice of their information practices or an opportunity to consent.(27) Industry representatives expressed the con the current mix in the United States of sector-specific statutory privacy protections and market-driven self-regulatory approaches satisfie Directive's adequacy standard.(28) According to these participants, the United States Government has the duty to convince European U member states that this is so.(29) One panelist opined that, at least with respect to protecting individuals from misuse of their personal ir by the government, U.S. privacy law is more protective than the Directive.(30)

Participants discussed the merits of adopting the Directive's requirements in toto in this country. The Directive requires that member stat national "supervisory authorities" with investigatory powers to monitor compliance with national legislation implementing the Directive.(3 Controllers of data are required to notify the supervisory authority before any automatic processing of data.(32) Several participants expr reservations about this registration requirement, on first amendment grounds.(33)

Panelists disagreed about the need for an independent data protection agency in the United States. One participant argued that a centra protection office is needed, not only to centralize data protection policy at the federal level but also to give European Union member stat entity with which to negotiate on data protection matters.(34) In the absence of such an entity, the burden falls upon individual U.S. busir demonstrate to member states that their information practices comply with the Directive.(35) Other participants questioned the need for a independent regulatory agency devoted to data protection, particularly in light of the uncertainties surrounding the European Union's inte of the adequacy standard.(36)

---

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to th processing of personal data and on the free movement of such data, Eur. O.J. L281/31 (Nov. 23, 1995) [hereinafter "Directive"]. A copy o Directive is included in this Appendix.

2. CDT Comment at 29 (Doc. No. 5); Reidenberg 192.

3. Reidenberg Comment at 1-2 (Doc. No. 7).

4. "Processing" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic me as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemina otherwise making available, alignment or combination, blocking, erasure or destruction." Directive, Art. 2(b).

5. Directive, Art. 2(a).

6. Directive, Art. 5; CDT Comment at 26 (Doc. No. 5).

7. Directive, Arts. 5, 32.

8. CDT Comment at 27 (Doc. No. 5); Reidenberg Comment at 1 (Doc. No. 7).

9. Reidenberg 183-84. The Directive requires that personal data must be: (1) processed "fairly and lawfully;" (2) "collected for specified, legitimate purposes and not further processed in a way incompatible with those purposes;" (3) "adequate, relevant and not excessive in the purposes for which they are collected and/or further processed;" (4) "accurate;" and (5) "kept in a form which permits identification of subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed." Dire 6.

Workshop participants debated the question of whether the Directive was intended to apply only to large, centralized data bases using m computing technology, as was typical of the 1960's and 1970's. The IIA representative asserted that this was indeed the case. Cochetti 2 However, several other participants disagreed. Hendricks 223; Reidenberg 211-12; Rotenberg 210. One participant argued that the langu Directive itself demonstrates that the Directive is "neither technology dependent nor system specific." Reidenberg Comment at 1 (Doc. N Directive states that its protections "must not in effect depend on the techniques used [to process personal data]." Id. at 2 (citing Directiv Explanatory Paragraphs 26-27). According to this panelist, the Directive's focus upon rules governing the "processing" of data and the "c of data, neither of which is defined in terms limited to a specific technology, is further support for this proposition. Id. (citing Directive Arts (d), 6, 7, 10-12, 14).

10. Directive, Art. 7. The Directive prohibits the processing of personal data revealing the data subject's race, ethnicity, political, religious philosophic beliefs, trade-union membership, health status or sexuality, absent the data subject's "explicit" consent, again subject to cert enumerated exceptions. Id, Art. 8.

11. "Controller" is defined as the "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data . . . ." Directive, Art. 2(d).

12. Directive, Art. 10.

13. Directive, Art. 11.

14. Directive, Art. 12.

15. Directive, Art. 14. This includes the right either to object to the processing of personal data about him for direct marketing purposes o

informed before the disclosure of personal data to third parties and to be expressly offered the right to object to such disclosures. Id., Art

16. Directive, Art. 22-23.

17. Directive, Art. 25 (1).

18. Directive, Art. 26(2). Under Article 26, member states may also permit the transfer of personal data to countries whose level of data p is not deemed "adequate" where: the data subject has "unambiguously" consented to the proposed transfer; the transfer is necessary fo performance of a contract between the controller of the data and the data subject (or of a contract between the controller and a third part benefits the data subject) or is necessary to protect the data subject's vital interests; the transfer is required to support a legal claim; or w transfer is of data maintained in certain public records. Directive, Art. 26(1).

19. Directive, Art. 25(2).

20. Directive, Art. 25(4). The Directive empowers the European Commission to enter into negotiations with non-member states whose pr protections have been deemed "inadequate," in order to derive international agreements that satisfy the Directive's data protection stand Directive, Art. 25 (5-6).

21. Directive, Art. 29-30; Reidenberg Comment at 3, 4 n.14 (Doc. No. 7).

22. CDT Comment at 26 n.26 (Doc. No. 5); Reidenberg Comment at 3 (Doc. No. 7). In connection with its efforts to apply the Directive's of rights and responsibilities to specific contexts, the European Union has begun a study of data privacy protection as it relates to online Blatch at 217; Reidenberg Comment at 3 and 4 n.10 (citing Notice 96/C114/11, Eur. O.J. C114/11 (April 19, 1996).

23. Reidenberg 193.

24. Reidenberg 195.

25. Id. Another participant argued that there is nothing inherently new about having to comply with an "adequacy" standard such as the E Union's. Friend 188. American companies doing business internationally can conform their information practices to other countries' requi through (for example) employee training and contractual arrangements that limit the uses of information as required by both U.S. and for This will still be necessary after the Directive is implemented, because each member state's law will govern data flows between that cou the United States. Friend 189-91.

26. Reidenberg 194-95.

27. CDT Comment at 30-31 (Doc. No. 5). CDT stated that the Directive's core notice and consent standards could be satisfied by implen emerging online technologies that make it possible for individuals to express their privacy preferences and for Web sites to disclose their information practices in a uniform format. Id. at 29-30.

28. IIA Comment at 5-6, 13 (Doc. No. 23).

29. Id. at 13.

30. Plesser 199-200.

31. Directive Art. 28.

32. Directive, Art. 18.

33. CDT Comment at 30 (Doc. No. 5); Plesser 202.

34. Reidenberg 196-98.

35. Reidenberg 196.

36. Plesser 201; Wellbery 205-06.

Last Modified: Monday, June 25, 2007