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

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

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

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

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 right to correct inaccuracies or to erase or block personal data that is processed in a manner inconsistent with the Directive's standards. For the United States and other countries doing business with European Union member states, the critical provision of the Directive is Article 25 which governs the transfer of personal data to countries outside the European Union. The Directive requires member states to permit the "third country of personal data which are undergoing processing or are intended for processing after transfer to its provisions.

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

For the United States and other countries doing business with European Union member states, the critical provision of the Directive is Article 25 which governs the transfer of personal data to countries outside the European Union. Article 25 requires member states to permit the "third country of personal data which are undergoing processing or are intended for processing after transfer to its provisions. 文章内容过于冗长，这里可能需要进行一定的删减或归纳。
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 concern that the current mix in the United States of sector-specific statutory privacy protections and market-driven self-regulatory approaches satisfy Directive's adequacy standard.(28) According to these participants, the United States Government has the duty to convince European Union member states that this is so.(29) One panelist opined that, at least with respect to protecting individuals from misuse of their personal information 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 states establish national "supervisory authorities" with investigatory powers to monitor compliance with national legislation implementing the Directive.(31) Controllers of data are required to notify the supervisory authority before any automatic processing of data.(32) Several participants expressed 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 centralized protection office is needed, not only to centralize data protection policy at the federal level but also to give European Union member states a single entity with which to negotiate on data protection matters.(34) In the absence of such an entity, the burden falls upon individual U.S. businesses to demonstrate to member states that their information practices comply with the Directive.(35) Other participants questioned the need for an independent regulatory agency devoted to data protection, particularly in light of the uncertainties surrounding the European Union's interpretation of the adequacy standard.(36)


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 means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Directive, Art. 2(b).


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


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." Directive, Art. 6.

Workshop participants debated the question of whether the Directive was intended to apply only to large, centralized data bases using mainframe computing technology, as was typical of the 1960's and 1970's. The IIA representative asserted that this was indeed the case. Cochetti 223; Hendricks 223; Reidenberg 211-12; Rotenberg 210. One participant argued that the language of the Directive itself demonstrates that the Directive is "neither technology dependent nor system specific." Reidenberg Comment at 1 (Doc. No. 7). Directive states that its protections "must not in effect depend on the techniques used to process personal data." Id. at 2 (citing Directive Explanatory Paragraphs 26-27). According to this panelist, the Directive's focus upon rules governing the "processing" of data and the "adequacy" 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, philosophical beliefs, trade-union membership, health status or sexuality, absent the data subject's "explicit" consent, again subject to certain enumerated exceptions. Id. Art. 8.

11. "Controller" is defined as 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).


15. Directive, Art. 14. This includes the right either to object to the processing of personal data about him for direct marketing purposes c...
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. 26(2). Under Article 26, member states may also permit the transfer of personal data to countries whose level of data protection is not deemed "adequate" where: the data subject has "unambiguously" consented to the proposed transfer; the transfer is necessary for performance of a contract between the controller of the data and the data subject (or of a contract between the controller and a third party benefiting the data subject) or is necessary to protect the data subject's vital interests; the transfer is required to support a legal claim; or the transfer is of data maintained in certain public records. Directive, Art. 26(1).


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 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.


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


27. CDT Comment at 30-31 (Doc. No. 5). CDT stated that the Directive's core notice and consent standards could be satisfied by implementing 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.


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

34. Reidenberg 196-98.

35. Reidenberg 196.

36. Plesser 201; Wellbery 205-06.