Freedom of Information and the EU Data Protection Directive

James R. Maxeiner(1)

Introduction

Protection of privacy is an important issue in information policy making. Sometimes lost sight of, however, in the zeal to protect privacy on the information superhighway, is that securing one person's privacy may infringe on another person's freedom of information. Freedom of information, in the narrow sense used in the United States, generally refers to free access to government information, but, in a wider sense, freedom of information is an essential part of freedom of expression.

Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms explicitly recognizes that the right to freedom of expression includes the freedom to "receive and impart informa tion or ideas.(1) Because Article 8 recognizes a right to protection of private

life,(2) the Convention itself poses a dilemma: whether to protect privacy or freedom of information. As the United Kingdom Data Protection Registrar recently noted, "[A] balance has to be struck between Articles 8 and 10 of the European Convention on Human Rights . . . the right to private life and freedom of expression.(3)

Common business transactions can raise this very issue. In business, the public interest calls for an open and free flow of information. Positive duties to disclose pertinent information frequently apply.(4) American securities laws are examples of laws that impose obligations to disclose. Even where no legal disclosure requirements apply, parties have a natural and understandable desire to want to know something about one another prior to entering into business relations. Before investing in a business, an investor may wish to know what success that business has experienced. The investor may also wish to know what success the principal of the business has experienced. The potential investor may find it relevant that the business has only recently emerged from bankruptcy or that the owner had other businesses that went bankrupt. Should the privacy interests of the business or its principal permit either one to keep that information confidential?

According to Professor Reidenberg, "the American legal system responds incoherently and incompletely to the privacy issues raised by existing information processing activities in the business community.(5) To state the same conclusion more positively, one might say that the United States has demonstrated a strong preference for freedom of information. In the United States there is skepticism about restrictions on the free flow of information. That skepticism is apparent in one of the earliest U.S. privacy cases, *Roberson v. Rochester Folding Box Co.(6)* In *Roberson*, the New York Court of Appeals rejected the claim that unauthorized use of a per son's likeness on a flour package supported a claim to damages. The court found the claim too great a restriction on third-party comment about neighbors' activities:

The so-called "right of privacy" is, as the phrase suggests, founded upon the claim that a man has the right to pass through this world, if he wills, without having his picture published, his business enterprises discussed, his successful experiments written up for the benefit of others, or his eccentricities commented upon either in handbills, circulars, catalogues, periodicals, or newspa pers; and, necessarily, that the things which may not be written and published of him must not be spoken of him by his neigh bors, whether the comment be favorable or otherwise.(7)

Perhaps because of this skepticism, there are no generally applicable data protection laws in the United States. The privacy laws that exist are sector specific, such as the Fair Credit Reporting Act.(8)

I.The EU Data Protection Directive

In Europe, data protection laws of general applicability have been common for two decades.(9) On February 3, 1995, the Council of Ministers of the European Union adopted a Common Position on a data protection directive.(10) The Common Position went back to proposals first made in 1990(11) and, in particular, to a proposed directive of the European Commission dated October 15, 1992.(12) After the European Parliament made only minor changes in the Common Position, the European Union adopted the Directive on July 24, 1995.(13) A directive, as those familiar with EU law know, is not directly applicable law; it is a direction to Member States to enact law.(14) A directive, even when adopted, is thus not the last word on a subject, particularly if the directive so provides. The Data Protection Directive balances competing interests both directly, by mandating certain rules, and indirectly, by permitting Member States to legislate accordingly. Article 5 recognizes this explicitly when it states: "Member States shall . . . determine more precisely the conditions under which the processing of personal data is lawful.(15)

The Directive identifies two principal objects: protection of the right of privacy and prevention of obstacles to the free flow of information within the European Union. Both are named in the Directive's title: *On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. Article 1(1) states that the object of the Directive is to "protect the fundamental rights and freedoms of natural persons, and in particular their right of privacy, with respect to the processing of personal data.(16) Article 1(2) states, "Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.(17) In acknowledging privacy, the Directive follows the Convention for the Protection of Individuals with Regard to Automatic Data Processing of Personal Data of the Council of Europe(18) and departs from the United Kingdom's Data Protection Act of 1984.(19) The protection that the Directive provides for the free flow of information is not protection of freedom of information but protection of commerce in information.(20)

What is significant in judging the Directive's balancing of the interests of privacy and of freedom of information is what the Directive does *not* do. The Directive does not establish a general right of property in information. It is concerned with processing of information and not with ownership of information. It gives data subjects certain limited rights and, more generally, imposes on data controllers obligations in their conduct of data processing. It does not create intellectual property rights in informa tion.

The Directive also does *not* follow the path taken by some European countries of establishing a right of "informational self-determination.(21) In 1983, the German Constitutional Court recognized a quasi-constitutional right to "informational self-determination.(22) Today, in Germany, while the federal constitution has yet to include an explicit right of privacy, some state constitutions do.(23) For example, the newly adopted constitution of Thuringia in former East Germany includes a detailed right of privacy which provides:

Everyone has the right to consideration and protection of his personality and of his private life. Everyone is entitled to protection of his personal data. He is entitled to determine the disclosure and use of such data for himself. These rights may be limited only by a statute. [W]ithin the terms of statutory law, everyone has a right to be told what information concerning him is contained in files and databases and to view those files and databases that concern him.(24)

The Data Protection Commissioner for the German state of Baden- Württemberg was quoted as saying that, "[d]ata protection . . . is the right of every individual to decide fundamentally for himself, who may know what about him and when.(25)

II.Data Protection in the Directive

The Directive mandates a comprehensive control of processing of information. This system includes:

· requirements of data quality (*e.g*., accuracy, but also limitations as to purpose and time of retention)(26)

· restrictions on permissible grounds for processing(27)

· prohibitions on processing sensitive data (*e.g*., race, ethnic origin, etc.)(28)

· required notification to the data subject(29)

· limitations on disclosures to others(30)

· rights of the data subject to access to the data(31)

· rights of the data subject to object to certain processing(32)

· requirements of levels of security(33)

· obligation to notify the supervisory authority of processing(34)

·private and public liability(35) and

· limitations on third-country transmission of personal data.(36)

The Directive applies its rules to government and private processing alike. Where it applies, it requires positive authorization to process information. Article 7 establishes, as a basic rule of prohibition, that "Member States shall provide that personal data may be processed `*only if*'" one of six conditions is met.(37) Most private party processing of personal data, unless otherwise exempted, would be permissible only if either Article 7(a), 7(b), or 7(f) is satisfied. Article 7(a) permits processing where the information subject "has unambiguously given his consent.(38) Article 7(b) permits processing "necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.(39) Article 7(f) permits processing if "necessary for the purposes of the legitimate interests of the controller or by the third party or parties to whom the data are dis closed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject . . . .(40) While the operative legal concepts of Article 7(a) (collection with consent) and Article 7(b) (in preparation or performance of a contract) are fairly definite, those of Article 7(f) are considerably more indefinite. The Directive offers scant guidance in determining what interests are legitimate under Article 7(f) and when they might be overridden by the interests of the data subject.(41)

III.Balancing Privacy and Freedom of Information

The Directive balances competing interests in privacy protection and freedom of information in three principal ways: (1) it exempts particular activities from its application; (2) it authorizes Member States in their own legislation to do the same in certain instances; and (3) it ameliorates otherwise applicable requirements.

A. Directive-Imposed Exemptions

1. Personal Data

One of the most important ways the Directive balances competing interests of privacy and freedom of information is to limit its application to "personal data.(42) The Directive has no application to other informa tion. Article 2(a) defines personal data to mean "any information relating to an identified or identifiable natural person (data subject).(43) This means that everyone may freely collect, process, and report information about corporate bodies and groups of individuals where the individuals cannot be identified.(44)

2. Private and Personal Processing

Article 3(2) provides that the Directive shall not apply "to the processing of personal data . . . by a natural person in the course of a purely personal or household activity.(45) In the minutes accompanying the Common Position, the Council and the Commission emphasized that "the expression ?purely personal or household activity' must not make it possible to exclude from the scope of the Directive the processing of personal data by a natural person, where such data are disclosed not to one or more persons but to an indeterminate number of persons.(46) Since the exemption also does not apply to the activities of corporate businesses, it may have little effect in the protection of freedom of information.

3. Filing Systems, Not Files

An entry in the minutes that accompanied the Common Position states, "The Council and Commission recognize that: —in line with the current definition in Article 2(c), the Directive covers only filing systems, not to files.(47) This statement creates confusion, because it is not at all clear that the Directive is to apply only to filing systems and not to files. Article 3(1) provides, "This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a file or are intended to form part of a filing system.(48) The preamble likewise suggests that it is only with respect to manual (for example, noncomputerized) systems that the Directive applies—only to filing systems and not to files.(49)

Limiting the Directive to filing systems of personal data and not applying it to files generally that contain personal data would reduce the burdens that the Directive imposes on freedom of information.(50) This limitation means that the Directive would regulate only organized activities of data processing directed to particular individuals; organized activities that only incidentally affect individuals would remain unregulated. Thus, a database on companies could incidentally include information on the principal officers of the company without falling under the strictures of the Directive. However, assuming that the Directive is to apply to "filing systems" and not to "files" generally, technological developments may overtake that limitation. If a database is searchable by an individual's name, one might argue that it is a filing system where there is easy access to personal data.

B. Directive-Authorized Exemptions

1. Journalism

Article 9 provides that:

Member States shall provide for exemptions or derogations from the provisions of this Chapter [general rules], Chapter IV [third country transfer of data] and Chapter VI [supervisory authority] for the processing of personal data carried out solely for journalistic purposes or for the purpose of artistic or literary creation only if they are necessary to reconcile the right of privacy with the rules governing freedom of expression.(51)

This direction to the Member States to create exemptions for journalism is the clearest example in the Directive of an attempt to balance protection of privacy and freedom of information.(52) The Directive itself, however, gives no clear direction as to what the nature and the scope of these exemptions ought to be.

The language limiting the authority of Member States to provide exemptions "only if they are necessary" to reconcile the right to privacy and freedom of expression was inserted after the U.K. Data Protection Registrar had expressed her concern that the balance drawn should not fall too much in favor of the media.(53) She had commented that "getting the balance right does not mean simply exempting the media from all data protection controls" and had proposed language similar to that adopted as a substitute for the more liberal language of the Common Position, which had permitted Member States to make such exemptions as "prove necessary.(54)

Getting the balance right is not an easy task. While the interest of free expression is particularly strong in the case of journalism, so too is the individual's interest in privacy. Because of the opportunities for broad dissemination, it is especially likely that in the case of journalism, individuals would be interested in, for example, a right to correction. On the other hand, limiting exemptions to journalism leaves many activities that should fall under freedom of information protection uncovered. The usual definition of journalism is limited to print and broadcast media,(55) but freedom of expression is not a monopoly of journalism. The informa tion highway that has led to the felt need for data protection laws has created new opportunities for communication which share aspects of traditional journalism—or simply traditional free speech. For example, is there a basis for treating on-demand, on-line information providers differ ently than the publications some of them carry?

2. General Exemptions to Particular Obligations

Article 13(1) authorizes Member States in certain instances to adopt legislative measures to restrict the scope of certain obligations and rights; namely, the obligations of data quality (Article 6(1)), the disclosure obligations (Articles 10 and 11), the obligations to publicize data collection (Article 21), and the right of access to data (Article 12).(56) While most of the instances in which Article 13 authorizes Member States to make exemptions relate to public interests such as national security, it might be used to support exemptions for freedom of information.(57) Subparagraph (g) allows exemption for "the protection of the data subject or of the rights and freedoms of others.(58) There is little indication how, or if, Member States will make use of Article 13 to protect freedom of information.

C. Modified Rules

1. Sensitive Data

Article 8 is an instance where the Directive takes a generally applicable rule and suspends or limits its operation and, thus, intentionally or unintentionally promotes the interest of freedom of information. Article 8(1) requires that Member States prohibit processing of certain special categories of data, such as those containing racial or ethnic information, political or religious beliefs, and so forth.(59) Article 8(2) then requires Member States to permit that processing in five specified instances.(60) Article 8(2)(e)—one of the five enumerated instances where processing is to be permitted—permits processing when "the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.(61)

2. Disclosure Not Required in Certain Instances

Article 11(2) provides that Article 11(1), which requires disclosure to the data subject that personal data has been processed, shall not apply where "the provision of information proves impossible or involves a disproportionate effort or if recording or disclosure is expressly laid down by law.(62) Article 11(2) gives statistical purposes and historical and scientific research as examples of such instances but does not limit its exception to these cases. How the Member States implement this exception is important from a business perspective. A business that routinely disseminates personal data might choose to locate its processing operations in a Member State that exempts its operations from that prior notification requirement rather than settle in a Member State where notification is de manded in every case. Such a result, of course, runs counter to the Common Position's goal of achieving a single European market.

Conclusion

The Directive makes attempts to balance protection of privacy and freedom of information. In many instances, it does this by authorizing Member States to provide exemptions and derogations in their individual legislation. The question remains as to how the Member States of the European Union will balance the competing interests of protection of privacy and freedom of information. In drafting that legislation and in amending existing legislation, Member States should accept that the need to protect privacy in an Information Age should not lead to measures that lose sight of the equally compelling need to encourage free exchange of information, even when that information is classified as "personal data." The actions of Member States should be of interest to the United States as it formulates its own information policy.

(1)* J.D., LL.M., Dr. Jur. (Munich); Vice-President and Associate General Counsel, Dun &

Bradstreet, Inc. The views expressed are the Author's and not necessarily those of Dun & Bradstreet. Translations without attribution are the Author's.

(1)"1. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4,

1950, art. 10, para. 1, 213 U.N.T.S. 221, 230.

(2)2. *Id*. at art. 8, para. 1, 213 U.N.T.S. at 230.

(3)" . United Kingdom Data Protection Registrar, Draft European Union General

Directive on Data Protection Common Position of the Council of Ministers Briefing Note § 4.2 (Mar. 17, 1995) [hereinafter Briefing Note] (copy on file with the *Federal Communications Law Journal*).

(4). *See generally* Nicola W. Palmieri, *Good Faith Disclosures Required During*

Precontractual Negotiations, 24 Seton Hall L. Rev. 70 (1993) (discussing such requirements under U.S., Italian, and German law).

(5)" . Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for*

Individual Rights?, 44 Fed. Comm. L.J. 195, 199 (1992).

(6). *Roberson*, 64 N.E. 442 (N.Y. 1902).

(7). *Id*. at 443. The decision in *Roberson* led the New York state legislature to adopt a

limited, statutory right of privacy. The current version of that statute is N.Y. Civ. Rights Law §§ 50-51 (McKinney 1992).

(8). 15 U.S.C. §§ 1681, 1681a-1681t (1988).

(9). In 1970, the German state of Hesse adopted what is generally considered to be the

world's first data protection law. *See* Hessisches Datenschutzgesetz as amended Dec. 11, 1988, *reprinted with translation* in 1 *Datenschutz in der Europäischen Union—Gesetzes sammlung/Data Protection in the European Union —The Statutory Provisions* (Nomos Verlagsgesellschaft, Baden-Baden) (Supp. 2, 01) (Apr. 1994).

(10). Common Position (EC) Adopted by the Council on 3 Feb. 1995, with a View to

Adopting Directive 94/ /EC 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. [hereinafter Common Position] (copy on file with the *Federal Communications Law Journal*).

(11). Commission Communication on the Protection of Individuals in Relation to the

Processing of Personal Data in the Community and Information Security; Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data; Draft Resolution of the Representatives of the Governments of the Member States of the European Communities Meeting within the Council; Commission Declaration on the Application to the Institutions and Other Bodies of the European Communities of the Principles Contained in the Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data; Proposal for a Council Directive Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommuni cations Networks, in Particular the Integrated Services Digital Network (ISDN) and Public

Digital Mobile Networks; Recommendation for a Council Decision on the Opening of Negotiations with Regard to the Automatic Processing of Personal Data; Proposal for a Council Decision in the Field of Information Security, COM(90)314 final. *See also* Briefing Note, *supra* note 3, § 1.

(12). Amended Proposal for a Council Directive on the Protection of Individuals with

Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM(92)422 final. For a discussion of the 1992 Commission, see James R. Maxeiner, *Business Information and "Personal Data": Some Common-Law Observations About the EU Data Protection Directive*, 80 Iowa L. Rev. 619 (1995).

(13). Council Directive of 24 July 1995 on the Protection of Individuals with Regard to

the Processing of Personal Data and on the Free Movement of Such Data. [hereinafter Council Directive] (copy on file with the *Federal Communications Law Journal*).

(14). "A directive shall be binding in its entirety, as to the result to be achieved, upon

each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods." Treaty Establishing the European Economic Community, art. 189, 298 U.N.T.S. 11, 78-79.

(15)" . Council Directive, *supra* note 13, at art. 5.

(16)" . *Id.* at art. 1, para. 1.

(17)" . *Id*. at art. 1, para. 2.

(18). "The purpose of this convention is to secure in the territory of each Party for every

individual, whatever his nationality or residence, respect for his rights and fundamental

freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (? data protection')." Convention for the Protection of Individuals with Regard to Automatic Data Processing of Personal Data, Jan. 28, 1981, art. 1, Europ. T.S. 108.

(19). Briefing Note, *supra* note 3, § 3. The U.K. Registrar welcomed this development.

Id. § 6.

(20). This is apparent in the Directive's preamble. For example, the third recital

provides:

Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded.

Council Directive, *supra* note 13, at pmbl. recital 3.

(21)" . *Cf*. Briefing Note, *supra* note 3, § 4.5 (discussing the Common Position, *supra* note

10).

(22)" . Judgment of Dec. 15, 1983, Bundesverfassungsgericht (Fed. Const. Ct.), 65

BVerwGE 1, translated in 5 Hum. Rts. L.J. 94 (1984). *See* H. Prantl, *Der Datenschutz zehn Jahre nach dem Volkszählungsurteil: Unanständiges für unanständige Leute. Der späte Sieg des ehemaligen Innenministers Friedrich Zimmermann*, Süddeutsche Zeitung, Dec. 16, 1993.

(23). *See* Hans-Hermann Schrader, *Datenschutz in den Grundrechtskatalog*, 1994

Computer und Recht 427.

(24). *Id*. at 428 (quoting Verfassung des Freistaats Thüringen [Const. of Thuringia] art.

6).

(25)" . Prantl, *supra* note 22.

(26). Council Directive, *supra* note 13, at art. 6.

(27). *Id.* at art. 7.

(28). *Id.* at art. 8.

(29). *Id.* at arts. 10-11.

(30). *Id.* at art. 12.

(31). *Id.*

(32). *Id.* at arts. 14-15.

(33). *Id.* at arts. 16-17.

(34). *Id.* at arts. 18-21.

(35). *Id.* at arts. 23-24.

(36). *Id.* at arts. 23-26.

(37). *Id.* at art. 7 (emphasis added).

(38)" . *Id.* at art. 7(a).

(39)" . *Id.* at art. 7(b).

(40)" . *Id.* at art. 7(f).

(41). The other provisions are 7(c) (to comply with law), 7(d) (to protect the data

subject), and 7(e) (to perform a task carried out in the public interest exercise of official authority). Council Directive, *supra* note 13, at art. 7.

(42)" . This limitation has been a feature of all EU proposals since the first one in 1990

but is not a necessary feature of a data protection law.

(43)" . Council Directive, *supra* note 13, at art. 2.

(44). The preamble notes that "the principles of protection shall not apply to data

rendered anonymous in such a way that the data subject is no longer identifiable." Council Directive, *supra* note 13, at pmbl. recital 26.

(45)" . Council Directive, *supra* note 13, at art. 3(2).

(46)" . Common Position, Statements for Entry in the Minutes, 4730/95 (quoting Council

Directive, *supra* note 13, at art. 3(2)) (copy on file with the *Federal Communications Law Journal*).

(47)" . *Id.*

(48)" . Council Directive, *supra* note 13, at art. 3(1).

(49). The 27th recital, for example, states, "as regards manual processing, this Directive

covers only filing systems, not unstructured files." *Id.* at pmbl. recital 27. The 15th recital provides:

Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question.

Id. at pmbl. recital 15.

(50). Québec, Canada as a matter of statutory interpretation, seems to have taken this

approach with its data protection law. *See* Maxeiner, *supra* note 12, at 712.

(51). Council Directive, *supra* note 13, at art. 9.

(52). The 37th recital expressly recognizes freedom of information:

Whereas the processing of personal data for purposes of journalism or for purposes of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive insofar as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Id. at pmbl. recital 37. *Cf*. Briefing Note, *supra* note 3, § 2 (calling this the "most distinctive" balancing measure).

(53). Briefing Note, *supra* note 3, § 5.4. The U.K. Data Protection Registrar is

Elizabeth, France.

(54)" . *Id*. § 5.4. The Registrar's view was "[i]f exemptions are to present a proper

balance, they will need to be limited in extent." *Id*. § 4.4. The adopted language was close to that which was proposed in the Briefing Note ("only so far as is necessary"). *Id*. § 5.4.

(55). *Cf*. American Heritage Dictionary of the English Language 707 (1st ed.

1969).

(56). Council Directive, *supra* note 13, at art. 13(1).

(57). *Cf.* Briefing Note, *supra* note 3, § 4.4 (discussing Common Position, *supra* note 10,

at art. 13).

(58)" . Council Directive, *supra* note 13, at art. 13.

(59). *Id*. at art. 8(1).

(60). *Id*. at art. 8(2).

(61)" . *Id.* at art. 8(2)(e).

(62)" . *Id*. at art. 11(2).