DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES

This study was prepared as part of the project *«Vie privée et société de l'information: Etude sur les problèmes posés par les nouveaux services en ligne en matière de protection des données et de la vie privée,»* commissioned from ARETE by Directorate General XV of the Commission of the European Communities.

Study Authors:

Joel R. Reidenberg
Professor of Law
Fordham University School of Law

Paul M. Schwartz
Professor of Law
Brooklyn Law School

DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES

Joel R. Reidenberg
Paul M. Schwartz

TABLE OF CONTENTS

1. INTRODUCTION1. INTRODUCTION1. INTRODUCTION1. INTRODUCTION

This Study will address various key legal aspects of data protection and on-line services. The mission for this Study is to identify the implications of the development of on-line services for data protection and to compare the regulatory treatment of critical issues across several member states of the European Union. The comparison will search for the application of the basic principles of data protection enunciated in the European Union's directive[1] and will examine the regulation and doctrine in four Member States. The methodology will identify particular themes and analyse the national results. The Study concludes with a strategic assessment of data protection regulation in the on-line environment that will draw out the convergences and divergences of the application of existing national laws, address the capabilities of law to resolve data protection issues and recommend various regulatory options to preserve European data protection norms within a framework of robust developing on-line services.

1.1 Study mission1.1 Study mission1.1 Study mission1.1 Study mission

The earlier reports to the Commission on the evolution and development of on-line services[2] as well as the specific information flows[3] associated with particular services raise important risks and opportunities for the rules of data protection. As seen in these earlier reports, the on-line environment has a broad

---

[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 the processing of personal data and on the free movement of such data, O.J. L281 (23nov. 1995) [hereinafter «European Directive».]

[2] ARETE, Les services en ligne et la protection des données et de la vie privée: Rapport no. 1--Situation Globale (Etude ETD/96/B5-3000/142 pour la Commission des Communautés Européennes, DGXV)(Juin 1997) [Hereinafter «Part I».]

[3] ARETE, Les services en ligne et la protection des données et de la vie privée: Rapport no. 2-- Etudes de Cas (Etude ETD/96/B5-3000/142 pour la Commission des Communautés Européennes, DGXV)(Dec. 1997)[Hereinafter «Part II»].

variety of actors, an extraordinarily rapid pace of change, a significant decentralization of information processing activity and a lack of reverence for territorial boundaries. A single session on the Internet may involve web sites located in different Member States of the European Union as well as sites found in third party states. Moreover, even the visit to a single web site can result in global transmissions of data. The architecture of on-line services on the Internet is intercontinental.[4] Search engines[5], «cookies,»[6] on-line shopping,[7] payments,[8] webcasting[9], log analysis,[10] games,[11] and medical diagnoses-[12] to identify just a few of the activities and infrastructure elements- each highlight the increasing tendancy, capability and commercial pressure to collect and use personal information on-line. The information flows illustrated in case studies reported earlier to the Commission reflect an ever critical need to apply basic principles to on-line services. These case studies show an enormous positive need exists for reliable personal information and that the commercial value creates a strong pressure for massive citizen surveillance. Data protection is a necessity if trust and confidence are to exist for on-line services.[13] Yet, the characteristics of the market and

---

[4] For example, the Marché de France, which sells French gastronomic products on the world wide web, contracts in France with those companies whose merchandise it offers for sale, maintains its website in Hong Kong where it is registered to do business, and manages the site and orders through an American server located in Arizona. *See* Part I, Section II.1.1.

[5] *See* Part I, Section I.4.1.

[6] *See* Part I, Section I.3.2

[7] *See* Part I, Section II.1

[8] *See* Part I, Section II.1.3.

[9] *See* Part I, Section I.4.3.

[10] *See* Part I, Section I.3.1.

[11] Part I, Section II.2.4.

[12] Part I, Section II.2.2.

[13] *See* European Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A European Initiative in

information flows pose a fundamental challenge to European data protection law. The implementation of fair information practice principles becomes exceedingly complex in the fluid context of the Internet.

At the same time that the technical and commercial development of on-line services pose substantial risks to privacy, technologies also offer new opportunities for the protection of personal information. Communications, for example, can be encrypted to preserve the confidentiality as well as the anonymity of the participants.[14] Electronic payments can be structured anonymously to minimize or eliminate the collection of personal data. Privacy preferences can be incorporated into Internet browser technologies which, combined with labelling and filtering of web site information practices, can assure respect for data protection.[15] The key questions, thus, revolve around the extent to which infrastructure arrangements create data protection problems and the extent to which data protection can be built within the architecture of on-line services.

In light of these new risks and opportunities, the objective of this comparative regulatory analysis is first to examine the current and likely future responses of European Union Member States to critical issues. The identification of any differences in the treatment by Member States of on-line services will be a prime focus. This identification will allow an evaluation of the potential for data protection to create obstacles to the free movement of on-line services within the Community. Finally, the comparison will be used to develop options for convergent treatment of data protection in an on-line environment.

1.2 Basic Principles of European Data Protection1.2 Basic Principles of European Data Protection1.2 Basic Principles of European Data Protection1.2 Basic Principles of European Data Protection

---

Electronic Commerce, 13, 18 (COM(97) 157)(Apr. 15, 1997), available at <http://www.ispo.cec.be/Ecommerce>.

[14] *See* Information and Privacy Protection Commission of Ontario and Dutch Data Protection Commissions, Privacy Enhancing Technologies: The Path to Anonymity (1995); International Working Group on Data Protection in Telecommunications, Data Protection on the Internet Report and Guidance,_ IIIe, (Budapest Draft)(May 21, 1996); Resolution of the Conference of Data Protection Commissioners of the Federation and theLaender on key points for the regulation in matters of data protection of online services, _ 1 (Apr. 29, 1996).

[15] *See* Minutes of the 21st Meeting of the International Working Group on Data Protection in Telecommunications (Paris: April 3, 1997)(Presentation of Joel RReidenberg on «Internet Labeling: Adapting PICS for Data Protection).

On-line services raise regulatory issues under the basic set of existing principles for European data protection. These core principles have been established within a number of international documents and within the national law of Member States. The critical international documents include the European Directive on Data Protection, the Council of Europe's Convention No. 108, and the OECD's privacy guidelines. Other international documents seek to express these principles within specific sectors of data use. An example of such a sectoral international measure is the Council of Europe's Committee of Ministers Recommendation on regulations for automated medical data banks.

For purposes of this analysis, the critical elements of European data protection law will be divided into four main groups. These are: (1) the establishment of obligations and responsibilities for those who process personal information; (2) the maintenance of transparent processing of personal information; (3) the creation of special protection for sensitive data; and (4) the establishment of enforcement rights and effective oversight of the treatment of personal data.[16] These elements create the comprehensive European approach to the protection of personal information. This section will briefly describe each traditional principle of European data protection law and follow each description with an indication of how on-line services challenge existing regulatory ideas.[17]

1.2.1 The Establishment of Obligations and Responsibilities for the Treatment of Personal Information1.2.1 The Establishment of Obligations and Responsibilities for the Treatment of Personal Information1.2.1 The Establishment of Obligations and Responsibilities for the Treatment of Personal Information1.2.1 The Establishment of Obligations and Responsibilities for the Treatment of Personal Information

---

[16] These groupings were first identified in a prior report to the European Commisison, Directorate General XIII comparing U.S. data protection law and practice to European norms. See Paul Schwartz & Joel R. Reidenberg, Data Privacy Law: A Study of U.S. Data Protection (Michie: 1996).

[17] These descriptions draw directly from the prior study for the Commission. *See id.*

The first element of the European principles is the creation of a series of fair information practices that define obligations and responsibilities with respect to the processing of personal information. The threshold component of this element is that personal information should only be collected legitimately for specific purposes.[18] This requirement is the most basic element of fairness for the use of personal information.

The Internet, however, challenges the establishment of obligations and responsibilities with respect to the processing of personal information. Under current practices, the basic principle of a "purpose limitation" for personal information has become the exception rather than the rule in the on-line environment. Where paper records themselves had provided a physicial barrier of sorts to any further use, information generated by individuals on the Internet is digital from the start and available for any number of further kinds of sharing and combination. Once on-line, the individual generates enormous amount of personal data and further use has not been limited to compatible purposes. As an earlier report to the Commission has noted, for example, a large amount of transactional information is collected by service providers who make various kinds of further use of these data.

As a corollary to the specification of the purpose for collection, another basic element of the European data protection framework is that personal information may only be used in a manner compatible with the purpose of collection. This second component requires the placing of limitations on secondary uses and restricting incompatible uses. The European Directive expresses both the need for specific purpose use and for limits on incompatible uses as one of its chief principles related to data quality. It requires that personal data be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with these purposes.[19] The open structure of the Internet, however, challenges this concept. The network was built around the idea of accessibility and multiple uses of information.

The third component in the basic structure of fair information practices precludes the collection of unnecessary personal information. While this component does not offer specific guidance for determining whether particular information is necessary for an identified collection purpose, collectors of personal

---

[18] Directive 95/46/EC, at Art. 6(1)(a) and Art. 6(1)(b).

[19] Directive 95/46/EC, at Art. 6(1)(b).

information within Europe do not have unfettered discretion to determine whether information is necessary. Rather than trying to maximize their collection of personal information, organizations must try to minimize their data gathering and collect only the least amount of personal information consistent with the intended goals. As the European Directive states, personal data are to be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[20]

Yet, the on-line environment also threatens the requirements that unnecessary personal information not be collected. Here, current technical standards generally permit the maximization of the quantity of personal information that is collected. An example of such maximization is the collection of the clickstream information generated as an individual goes from web site to web site. This collected data can even extend to how long an individual has looked at a given page on a particular web site.

The basic structure of data protection also imposes obligations on the treatment of personal information once collected. A critical component places limits on the duration of storage of personal information. Any collection of personal information will lose accuracy and relevancy with time; as a result, organizations are not permitted to warehouse personal data for unlimited periods. European data protection principles require that personal information not be stored any longer than necessary to accomplish the purpose for collection.[21] In the network environment, restrictions on data storage are necessary because a computer may not "forget" any information that is stored on it. Thus, the Internet, as any digital medium, requires that both collection and storage restrictions be created through technical measures. Restrictions on data storage may sometimes be created, however, due to concerns other than data protection. Thus, to the extent that an on-line service views older information as less relevant for its commercial purposes, it may limit the storage of personal information. As an illustration of this kind of storage limitation, some web sites have placed an expiration date on the cookies that they place on hard drives.

In addition, under the basic principles of data protection, individuals must have a right to access their personal information and to correct inaccurate data.[22]

---

[20] Directive 95/46EC, at Art. 6(1)(c).

[21] Directive 95/46/EC, at Art. 6(1)(e).

[22] Directive 95/46/EC, at Art. 12.

These rights contribute to securing accuracy of personal information. With respect to these access rights, the Internet has great potential for increasing data protection. On-line services technically have the capacity to permit inexpensive access of individuals to personal data that are generated in interactions with these services. Such access is not provided, however, as a general matter. Finally, the basic set of rights and obligations provides that measures must be taken to assure the integrity of personal information.[23] These measures are necessary to protect personal information against destruction or unauthorized alteration. Not surprisingly, the security of information on the Internet is a matter of some controversy. Without special measures of data security, Internet communications are as a general matter insecure. This lack of security follows from the basic structure of the Internet. Information sent through the Internet travels over nondedicated lines in packets to its destination, and such data are capable of interception at numerous points. Moreover, the architecture of client-server systems can raise critical security issues. Thus, the spoofing of web sites and servers provides a significant threat to the security of personal data on-line. Nevertheless, commercial on-line services have a considerable economic incentive to increase data security on the Internet. Continuing electronic commercial transactions will depend on consumer confidence in this medium. One of the most important ways to increase this confidence is through use of encryption. But, the law enforcement community has raised serious objections to encryption because of the potential for criminals to mask effectively their illegal activities from prosecuting or investigatory authorities. The kinds of encryption that will be allowed is currently a matter of considerable international debate; this Study will examine this subject in section 2.5 below

1.2.2 The Maintenance of Transparent Processing of Personal Data1.2.2 The Maintenance of Transparent Processing of Personal Data1.2.2 The Maintenance of Transparent Processing of Personal Data1.2.2 The Maintenance of Transparent Processing of Personal Data

The second key element in the European principles of data protection is the

---

[23] Directive 95/46/EC, at Art. 17.

maintenance of transparent processing systems for personal information.[24] This essential norm requires that processing activities be structured in a manner that will be open and understandable. European consensus finds that individuals must be able to comprehend the treatment of their personal information to participate in social and political life. Secretive processing of personal information risks the suppression of an individual's free choice. Thus, the first component of this element is to require notice to individuals of the collection of personal information.[25] In some cases, a second component further provides that consent from individuals must be obtained for certain kinds of processing and uses of personal information.

Growth in on-line services has not been accompanied by an increase in the kinds of information about data use that is provided to individuals who use these services. Thus, in the age of the Internet, the transparency standard is being challenged.

Transparency remains of critical importance, however, for a number of reasons. To begin with, in its absence, an individual's consent to the data processing practices of on-line services cannot be considered to be valid. Transparency issues are also raised in the context of consent by the issue of whether relevant information will be provided only in English, the most popular language on the World Wide Web, or also in the national language.

Another reason for the importance of transparency as a fair information practice is that its absence will cause a systematic underrepresentation of the desire for data protection of consumers who use on-line services. Without knowledge of how their personal data are being used, individuals will not be able to create a robust market for privacy.

While transparency is now being challenged by the Internet, this digital medium does have the potential for increasing individual knowledge of the different kinds of processing of personal data. Thus, as an earlier report to the Commission has noted, one world wide web site permits individuals to test in real time the information that a server can collect about the visit. (<http://www.anonymiser.com>). Other sites may also have a link offering a description about their data processing practices.

---

[24] See, e.g., Directive 95/46/EC, at Art. 18 (notification to a central registry of data processing systems required).

[25] Directive 95/46/EC, at Art. 10.

More recently, industry coalitions have begun to prepare technical infrastructures that would provide greater transparency to individuals. The «Platform for Privacy Preferences» («P3P»)under development by the World Wide Web Consortium and the Open Profile Standard («OPS») being promoted by a number of on-line services companies are two examples. P3P would enable the rating and filtering of Internet sites based on their privacy practices.[26] OPS would encourage the collection by web browsers of personal information and the disclosure of that personal information to web sites after individuals selected options for the use of particular bits of personal information. These examples significantly demonstrate that technical means can easily be furnished to provide access and correction rights. Nevertheless, at the moment, these access and corrections rights are not generally provided on the Internet.

1.2.3 The Creation of Special Protection for Sensitive Data1.2.3 The Creation of Special Protection for Sensitive Data1.2.3 The Creation of Special Protection for Sensitive Data1.2.3 The Creation of Special Protection for Sensitive Data

The third element of the European principles requires the creation of special protection for sensitive data.[27] This principle consists of the establishment of greater scrutiny and protection for certain types of information, specifically those dealing with race, religion, health or political beliefs. Yet, the creation of special protection is also understood as requiring attention not only to whether information identifies particular aspects of a person's life that are sensitive, but how data will actually be used. The ability of information technology to combine and share data makes impossible any abstract, noncontextual evaluation of the impact of disclosing a given piece of personal information. The impact of bureaucratic use of personal information, whether merely personal or highly sensitive, depends on the means of processing, the kinds of databases linked together, and the ends to which information will be used.

---

[26] See Joel R. Reidenberg, *The Use of Technology to Assure Internet Privacy: Adapting Labels and Filters for Data Protection*, Lex Electronica, Vol. 3, No. 2 (Fall 1997) <www.lex-electronica.org>(analyzing the benefits and hurdles to the use of labelling and filtering for privacy).

[27] Directive 95/46/EC, at Art. 8.

At present, a great deal of sensitive information is available on-line. Alone the popularity of different kinds of pornographic web sites has led to the creation of highly sensitive on-line data-- specifically information about personal sexual preferences and interests. In addition, web sites and on-line chat groups exist that are devoted to race, religion, health and political beliefs. Visitors to these web sites and participants in these chat groups will generate considerable traces of sensitive information.

Due to the lack of transparency regarding on-line processing practices, individuals are generally unaware of any further use made of the personal data that on-line activities may generate. Indeed, there may also be a lack of knowledge regarding the extent to which these on-line activities create sensitive information.

1.2.4. The Establishment of Enforcement Rights and Effective Oversight of the Treatment of Personal Information1.2.4. The Establishment of Enforcement Rights and Effective Oversight of the Treatment of Personal Information1.2.4. The Establishment of Enforcement Rights and Effective Oversight of the Treatment of Personal Information1.2.4. The Establishment of Enforcement Rights and Effective Oversight of the Treatment of Personal Information

The final element of European fair information practices is the establishment of enforcement rights and effective oversight of the treatment of personal information.[28] This element is recognized in Europe as a critical part of the implementation of fair information practices. The basic component of this norm is that a remedy must exist for individuals in the event that rights, obligations or responsibilities with respect to personal information are abridged. In Europe, damage awards are possible under certain circumstances.

Moreover, this element requires effective external oversight of fair information practices. The European Directive requires creation of an independent governmental body to carry out this oversight.[29] These authorities monitor the development and implementation of national data protection law as well as

---

[28] Directive 95/46/EC, at Art. 22 -24.

[29] Directive 95/46/EC, at Art. 28(1).

international measures that affect global information transfers. Such agencies must be able to act with independance in carrying out their assigned functions.

In the global environment of the Internet, any enforcement rights provided under national law face challenges from international data flows. In a similar fashion, the effectiveness of any national oversight body will be made considerably more difficult. The development of on-line services poses the question of how effective any national regulation can be in a period of global communication services.

1.3 Identification of target countries1.3 Identification of target countries1.3 Identification of target countries1.3 Identification of target countries

The regulatory responses to on-line services will be studied within four Member States.[30] Three large Member States, where the market for on-line services is more economically significant, and which have well established laws in the field of data protection, have been chosen: France, Germany and the United Kingdom. One smaller Member State, Belgium, has been chosen because it has existing data protection law and already significant development of on-line servics. These four countries also present an interesting cross-section of legal systems represented in the European Union.

1.3.1 Belgium1.3.1 Belgium1.3.1 Belgium1.3.1 Belgium

The legal system of Belgium is based on the civil law. The country has a constitutional monarchy and is organized as a federal state consisting of «Communities» and «Regions.»[31] The «Communities» consist of three groups based on language and cultural identity: (1) the Wallons or French Community, (2) the Flemings or Flemish Community and (3) the German-speaking Community. There are also three «Regions» that are geographically defined areas: the Flemish Region, the Brussels-Capital Region and the Walloon Region. The power to issue laws and regulations is shared among the federal government, federal parliament as

---

[30] The study considersregulations, laws and decisions through December 1997.

[31] Belgium was redefined as a «federal» state by constitutional amendment in 1994. Modification à la Constitution du 31janvier 1994 (Moniteur belge du 12 février 1994).

well as the different Communities and Regions. Foreign affairs, defense, justice, finances, social security, public health and domestic affairs are each matters of federal power. The Regions and Communities, however, have power to conduct foreign relations independently in those areas where they have competence such as language and education. The resulting legal structure and its institutions are multilayered. At the federal level, legal authority vests in a House of Representatives, Senate, and government ministers nominated by the King. At the community level, there are Flemish, French, and German Community Councils as well as a Joint Commission. On the Regional and Community levels, each Region and each Community has a governing body.

The Belgian constitution requires that law respect privacy and family life.[32] Data protection in Belgium is within federal competence and assured by federal statute and Royal Decree. In 1992, Belgian enacted a data protection law[33] that was largely inspired by French law. The Belgian statute progressively entered into force and became fully effective on June 1, 1996. The law applies to computer processed personal data as well as manual files organized for retrieval. The law establishes rights and obligations associated with the use of personal data, delegates authority for Royal Decrees, creates a declaration system as a precondition to the processing of personal information, and establishes the *Commission de la protection de la vie privée* (hereinafter «CPVP») as a semi-independent supervisory authority.[34] Decisions of the Commission are public, but have not been published an any one collection. Nevertheless, in late 1997, the Commission released a series of annual reports covering its first five years of existence. In addition, statutory measures may offer sectoral data protection provisions such as those dealing with consumer credit,[35] telephone wire tapping,[36]

---

[32] Belgian Constition, Art. 22(2).

[33] Loi du 8 décembre 1992 relative à la protection de la vieprivée à l'égard des traitements de données à caractère personnel.

[34] See infra 2.2.1 (discussion of 'independence' of the CPVP)

[35] Loi du 12 juin 1991 relative au crédit à la consommation.

[36] Loi du 30 juin 1994 relative à la protection de la vieprivée contre les écoutes, la prise de connaissance et l'enregistrement de communications et detélécommunications privées, M.B., 24 janvier 1994, pp. 1542 et seq.

the social security system,[37] the national register,[38] driver's license records[39]

1.3.2 France1.3.2 France1.3.2 France1.3.2 France

France is a constitutional democracy with a legal tradition anchored in civil law. Under the French Constitution of 1958, laws are promulgated by the President of the Republic after being voted jointly by the National Assembly and the Senate.[40] Under the Constitution of 1958, the Parliament has the sole and exclusive power to establish rules for particular subject areas.[41] Other areas not reserved for statutory enactment may be regulated by government decree after consultation with the Conseil d'État.[42] This regulatory power is confered upon the Prime Minister who directs the government.[43]

The French Constitution provides for respect of human rights and requires that legislation elaborate civil rights and the fundamental constitutional guarantees granted to citizens for the exercise of their public liberties.[44] In 1978, France enacted one of the first national laws to regulate fair information practices.[45] More

---

[37] Loi du 15 janvier 1990 modifiant la loi relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, M.B. 22 février 1990, pp. 3295 et seq.

[38] Loi du 8 août 1983 organisant un registre national des personnes physiques, M.B. 21 avril 1984, pp. 5247 et seq.

[39] Loi du 18 juillet 1990 modifiant la loi relative à la police de la circulation routière, coordonnée le 16 mars 1968 et la loi du 21 juin 1985 relative aux conditions techniques auxquelles doivent répondre tout véhicle de transport par terre, ses éléments, ainsi que les accessoires de sécurité, M.B. 8 novembre 1990, pp. 21184 et seq.

[40] See Constitution du 4 octobre 1958, Arts. 10, 24, 34, 45.

[41] Constitution du 4 octobre 1958, Art. 34 (2). These areas include the protection of civil rights and fundamental rights of citizens, nationality, civil status, inheritance, the definition of criminal acts and penalties, taxation, electoral rules and procedures.

[42] Constitution du 4 octobre 1958, Art. 37.

[43] Constitution du 4 octobre 1958, Art. 21.

[44] Constitution du 4 octobre 1958, Art. 34 (2).

[45] Loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

recently, in the context of a case on videosurveillance, the Conseil Constitutionnel[46] decided that the protection of privacy was part of the group of basic freedoms guaranteed by the constitution.[47] As a result, data protection must be derived exclusively from statute in France.

The existing 1978 data protection law is a comprehensive law of general application that offers wide-ranging protections to citizens. The law applies to the public and private sectors, and imposes obligations and responsibilities on those processing personal information. The law imposes civil as well as criminal penalties for violations. The statute establishes a large independent regulatory commission, the *Commission nationale de l'informatique et des libertés* (the CNIL), that supervises the registration of data processing in the public as well as private sectors and supervises regulatory compliance for both the public and private sectors. The CNIL publishes an annual report as well as its decisions and guidance notes.

1.3.3 Germany1.3.3 Germany1.3.3 Germany1.3.3 Germany

Germany is a federal republic that consists of sixteen states (*Laender*). Legislative power in Germany may be exercised at the state or federal level (exclusive), or, in some cases, concurrent and framework legislation may also be possible. At the federal level, the *Bundestag*, the federal parliament, enacts legislation with the states participating in the legislative process through the *Bundesrat*.

Data protection in Germany has both constitutional and statutory roots. In its "Census" decision in 1983, the German Constitutional Court identified a "right of informational self-determination" based on the first two articles of the Basic Law (*Grundgesetz*), the German constitution.[48] These articles of the Basic Law compel the State to take positive action to protect both human dignity (Article 1)

---

[46] If required, as in the case of certain organic laws, or if requested in conformity with consitutional procedures, theConseil Constitutionnel decides on the constitutionality of laws prior to their taking effect.Consitution du 4octobre 1958, Art. 61. Any law judged unconstitutional may not be promulgated and may not be applied. Id.

[47] Décision 94-352 du Conseil Constitutionnel du 18janvier 1995

[48] 65 Bundesverfassungsgericht 1 (1983).

and the development of human personality (Article 2).[49] The Constitutional Court found that these two provisions, which form the basis of a "right of personality," protect the individual from borderless collection, storage, application, transmission of personal data. The «Census» decision also establishes an obligation that the state create legislation that authorizes and regulates the collection and processing of personal data.[50] The right of informational self-determination prevents any processing of personal data that would lead to an inspection of or an influence on a person that is capable of destroying an individual capacity for self-governance.[51]

In addition to the right of informational self-determination, the Basic Law contains other provisions that can protect data privacy. In this context, the most important of these measures is its Article 10, which protects the privacy of communications.[52] Due to Article 10, the ongoing German debate about encryption has an added constitutional dimension.

Beyond these constitutional elements, German data protection contains significant statutory elements at both the state and federal level. In 1970, the state legislature in Hesse enacted the world's first data protection law.[53] All sixteen German states now have their own data protection laws. In 1977, the *Bundestag*, the German federal parliament, enacted a federal data protection law, which has since been subject to amendment.[54] In addition to the federal omnibus statutes and

---

[49] Art 1(1), Basic Law: "The dignity of man shall be inviolable. To respect and protect it shall be the duty of all state authority." Article 2(1), Basic Law: "Everyone shall have the right to free development of his personality in so far as he does not violate the rights of others or offend against the constitutional order or the moral code." Id.

[50] 65 Bundesverfassungsgerichtentscheidungen 1, at 41-52.

[51] Id.

[52] Article 10(1), Basic Law: "Privacy of correspondence, posts, and telecommunications is inviolable." Article 10(2) adds, "Restrictions may only be ordered pursuant to a law."

[53] This statute has since been amended, see Hessisches Datenschutzgesetz, vom 11. November 1986 in der Fassung des Gesetzes zur Änderung des Hessischen Datenschutzgesetzes vom 21. Dezember 1988.

[54] The most significant of these amendments took place in 1990. BDSG vom 20. Dezember 1990, BGBl. I S.2954 zuletzt geändert durch das Postneuordnunggesetz v. 14.9.1994, BGBl. I, S. 2325, 2385.

these state laws, numerous sectoral and subsectoral data protection laws have been enacted in Germany. These laws include the privacy provisions of the German Social Welfare Code's Book V, which concern personal medical information, and of the Social Welfare Code's Book X, which concern social welfare information.

Finally, data protection oversight agencies have been created at both the federal and state levels in Germany. The federal data protection law (BDSG) assigns to the federal commissioner of data protection an oversight role for federal agencies.[55] German law assigns a parallel oversight role over state agencies to state data protection commissioners.[56] The federal data protection commissioner is also to advise the federal government (*Bundesregierung*) and the *Bundestag* on data protection.[57] Finally, the commissioner is to keep a register of the public sector's automated data files.[58]

As to the private sector, the federal data protection law assigns governmental oversight over it to the so-called "Supervisory Authorities."[59] It requires each state government to appoint its own Supervisory Authority. In some instances, states have assigned this oversight role to existing state data protection commissioners, who, as noted above, also have power over state agencies; other states have assigned these duties to a different governmental body. Like the federal and the state commissioners, the Supervisory Authorities have oversight authority.[60] In addition, the Supervisory Authority keeps a register of entities that store personal data for business purposes.[61] Finally, the Federal Data Protection Law requires companies in the private sector that regularly employ at least five full time employees for the purpose of processing personal data to appoint an internal

---

[55] BDSG, §§ 22-26.

[56] See, e.g., Hessisches Datenschutzgesetz, §§ 21-31.

[57] BDSG, § 26.

[58] BDSG, § 24.

[59] BDSG, § 38.

[60] BDSG, § 38.

[61] BDSG, §(2).

data protection officer.[62]

For on-line services, Germany has a new and comprehensive statutory regulation of on-line services in the Information and Communication Services Act (*Informations- und Kommunikationsdienste-Gesetz* ("IuKDG").[63] This law contains three new acts: (1) the Teleservices Law; (2) the Teleservices Data Protection Law, and (3) the Digital Signature Law. It also carries out amendments to several existing statutes, such as the Penal Code and the Copyright Act.[64]

The IuKDG has generally been welcomed as a successful data protection law. The Federal Data Protection Commissioner, Dr. Joachim Jacob, has greeted this law as one that "does not fix regulation within the status quo, but that

---

[62] BDSG, §§ 36-37.

[63] The German Parliament passed this Bill on June 13, 1997 and it entered into force on August 1, 1997.The text of this statute can be found at http://www.iid.de. The English text cited in this Study is the official translation found at this web site.

[64] With the enactment of theIuKDG, Germany has assumed a pioneer role for the legal regulation of on-line services. AsJürgen Rüttgers, the German Minister of Education, Science, Research and Technology has stated, theIuKDG "creates the preconditions for our transition from an industrial society to an knowledge society."Rede von Dr.Juergen Ruetters MdB, 2. und 3. Lesung des IUKDG im Deutschen Bundestag am 13. Juni 1997 in Bonn, http://www.iid.de/rahmen/rede130697.html. As this quotation indicates, one primary justification for this statutory regulation of on-line services is on economic grounds. TheIuKDG states that its purpose "is to establish uniform economic conditions for the various applications of electronic information and communication services." IuKDG, Article 1, §1.

The notion of "uniform economic conditions" was explained in more detail by the Bundestag's Committee for Education, Science, Research, Technology and the Assessment of Results of Technology. In introducing theIuKDG, this Committee pointed to the need for "removal of obstructions to the free development of market forces in the sector of new information and communication services and the guarantee of a uniform economic framework for the offer and the utilization of these services." Beschlußempfehlung und Bericht des Ausschusses für Bildung, Wissenshaft, Forschung, Technologie und Technikfolgenabschätzung (19. Ausschuß), Bericht der Abgeordneten Dr. Mayer, Tauss, Kiper, Dr. Laermann und Bierstadt 24 (1997) [hereinafter cited as Committee Report]. TheIuKDG regulates on-line services to create the necessary preconditions for successful economic development of this area.

The IuKDG also contains strong data protection provisions. In addition to pointing to economic justifications for theIuKDG, the Bundestag Committee stressed the need for effective data protection measures. Id. Data protection in the on-line world was seen as absolutely essential for creating the confidence necessary for widespread use of this medium.

meaningfully encourages further development.[65] In the words of Hans-Jürgen Garstka, the Data Protection Commissioner of Berlin, this law's promulgation "dramatically improves the legal position of the individual user of multimedia services."[66]

The IuKDG explicitly applies to on-line services, which fall under this law's definition of "teleservices." The law defines "teleservices" as "all electronic information and communication services which are designed for the individual use of combinable data such as characters, images or sounds and are based on transmission by means of telecommunication."[67] As this definition makes clear, this law does not concern telecommunications per se, which are regulated by other statutes, but a certain kind of use of telecommunications, namely the "individual use of combinable data."[68] The Federal Government spoke of the law as regulating the "autonomous and self-determined utilization ... of digitalized data of different representation forms (for example text, graphics, languages, pictures, the succession of pictures, etc)."[69] In a similar fashion, in introducing the law, members of the responsible legislative committee stated that it regulated "new services that are individually utilized by the user through the path of new information and communication services."[70]

---

[65] Der Bundesbeauftragte für den Datenschutz, 16. Tätigkeitsbericht 1995-1996 143 (1997) [hereinafter cited as Federal Data Protection Commissioner, 16th Activity Report].

[66] Berliner Datenschutzbeauftragter, Informationzum Datenschutz, Bereich Recht II, 711.141.2 (August 1, 1997).

[67] IuKDG, Article 1, § 2(1).

[68] Id.

[69] Drucksache 13/7385 (pg 17).

[70] Id. at p. 25.

The Teleservices Law, which is the first part of the IuKDG, also provides explicit examples of the kinds of services to which it applies. This statutory list of the on-line services within the law's jurisdiction is not intended to be exclusive. The Teleservices Law states that the relevant services "include in particular" five general groups. These are:

> "1. services offered in the field of individual communication (e.g, telebanking, data exchange),
>
> "2. services offered for information or communication unless the emphasis is on editorial arrangement to form public opinion (data services providing e.g. traffic, weather, environ- mental and stock exchange data, the dissemination of

The Teleservices Law does *not* apply, however, to so-called "media services." These are regulated by the Media Services Interstate Agreement, which entered into force on the same day as the IuKDG.[71] The Media Services Interstate Agreement is a treaty that is based on the *Länder*'s jurisdiction over the mass media. This agreement between the individual German states regulates such new media as electronic press information, television text, and teleshopping to choose television events (pay per view).[72] In contrast to the IuKDG, the Media Services Interstate Agreement concerns itself with electronic mass media that does not require the user to manipulate and combine information.[73] The Media Services Interstate Agreement also contains data protection provisions, which intentionally seek to track those of the IuKDG in order to provide a uniform level of privacy protection irrespective of a categorization as a "teleservice" or "media service."[74] In one area, namely that of provisions for independent data protection audits, however, the Media Services Interstate Agreement contains an important additional data privacy measure beyond that in the IuKDG.[75]

1.3.4 United Kingdom1.3.4 United Kingdom1.3.4 United Kingdom1.3.4 United Kingdom

The United Kingdom is a constitutional monarchy and a parliamentary democracy. The country's head of government is the prime minister, who leads the

---

information on goods and services),

"3. services providing access to the Internet or other networks,

"4. services offering access totelegames,

"5. goods and services offered and listed in electronically accessible data bases with interactive access and the possibility for direct order."

On-line services are covered by the law whether or not one pays for them or receives them for free.

[71] Staatsvertrag über Mediendienste, Drucksache 12/1954 [hereinafter cited as Media Services Multistate Agreement].

[72] Media Services Interstate Agreement, § 2. The sixteen German states continue to have regulatory authority over traditional media. For a discussion of these jurisdiction issues in German federalism in the age of the Internet, see Ralf Roeger, Internet und Verfassungsrecht, 1997 Zeitschrift für Rechtspolitik 203.

[73] Media Services Interstate Agreement, § 2(2).

[74] Media Services Interstate Agreement, §§12-17.

[75] Media Services Interstate Agreement, § 17.

political party that commands a majority in the House of Commons. Political power is concentrated in the prime minister and the Cabinet. The prime minister chooses members of the Cabinet from members of his political party in the Parliament.

Data protection in the UK is regulated by the Data Protection Act of 1984.[76] Data protection supervision is carried out in the UK through the Data Protection Registrar, who has power through the registration process and through her ability to seek prosecution for violations of the Data Privacy Act.[77] Through the registration process, the Data Protection Registrar can serve an Enforcement Notice that directs a registered person to take specific steps to comply with the Data Privacy Act, and, in particular, with the data protection principles.[78] The Registrar's powers also permit the issuance of a De-registration Notice that cancels the whole or part of any registration entry from the Register. Finally, the Registrar can issue a Transfer Prohibition Notice that prevents the transfer of personal data overseas.[79] If the Registrar issues any of these notices, the data user may appeal the enforcement action to the independent Data Protection Tribunal.[80]

The Registrar may also seek prosecution of violators of the Data Privacy Act. Where the Registrar has reasonable grounds for suspecting a criminal offense, or a breach of a principle, she may apply for a search warrant to enter and search any premises.[81] Prosecutions can also be made for failure to register.[82] In the most recent year for which data are available, the Registrar secured fifty-two

---

[76] Data Protection Act 1984, enacted 12th July 1984.

[77] Data Protection Act 1984, Part II, 4-20.

[78] Id. at 10.

[79] Id. at 10-12.

[80] Id. at 13-14. The Data Protectional Tribunal consists of a chairman, deputy chairmen, and members to represent the interests of data users and data subjects. Id. at Part I, 3. The Tribunal can overturn the Registrar's decision and substitute its own decision. Id. at Part II, 14. For a discussion, see Data Protection Registrar, The Guidelines Third Series 10 (1994).

[81] Id. at 16 & Schedule 4.

[82] Id. at 19.

convictions against unregistered data users.[83] In 1996, the Data Protection Registrar brought the first prosecution for the unlawful procuring and selling of data, which led to a conviction and a fining of the plaintiff, who was a part-time private investigator.[84]

1.4 Methodology1.4 Methodology1.4 Methodology1.4 Methodology

The methodology for the comparative analysis of these countries will follow the «functional» approach.[85] The analysis will search to find regulatory treatment in national law that responds to a set of themes identified from the earlier phases of this Report. These themes address critical problems for the regulatory treatment of on-line services.

For each country, the comparative analysis relies on published reports from the national data protection authority, published regulatory decisions, interviews with members of the relevant data protection commission, as well as contacts with other national experts and various European and international studies.[86]

Since national responses to on-line services appear on the whole to be only first emerging, this Study, in keeping with the functional approach, also examines other existing data protection rules that may give guidance for the treatment of on-line services. In addition, to the extent that specific data protection rules for on-line services are under development in any of the countries, the analysis of the country seeks to examine these emerging regulatory actions. In the absence of specific regulatory initiatives or actions, the views of data protection authorities, government administrators and other experts have also been explored to present conclusions on the current expectations for the treatment of on-line services under existing legal rules.

---

[83] Data Protection Registrar, The Thirteenth Annual Report 45 (1997).

[84] News Release, http://www.open.gov.uk/dpr/news.htm

[85] *See* Paul Schwartz & Joel R. Reidenberg, Data Privacy Law: A Study of U.S. Data Protection, 24-25 (Michie: 1996).

[86] Joel Reidenberg had primary responsibility for the analysis of Belgium and France, while Paul Schwartz had primary responsibility for Germany and the United Kingdom.

2. EUROPEAN REGULATORY RESPONSES2. EUROPEAN REGULATORY RESPONSES2. EUROPEAN REGULATORY RESPONSES2. EUROPEAN REGULATORY RESPONSES

This section will focus on a current assessment of European regulatory responses to data protection for on-line services. The assessment is organized around a set of fundamental, recurring issues for the application of data protection principles to on-line services. The first two sub-sections treat jurisdictional questions. The analysis first looks to the basic scope of data protection law as a form of subject matter competence over the disaggregated data flows associated with many on-line services. For example, to the extent that on-line service activities might avoid the use or creation of «personal data» through anonymity, data protection regulations may be wholly inapplicable.

Next the jurisdictional inquiry turns to the territorial applicability of data protection rights, obligations and supervision. This subsection will try to determine how data protection regulators react to the simultaneous foreign, yet local, activities on the Internet as seen through registration and supervision practices.

The third subsection analyzes transparency issues such as notice and consent as well as data subject access and correction of erroneous data. In particular, this section seeks to understand how the four different countries implement these rules in the face of decentralized, diverse and complex information use on the Internet.

The next subsection examines profiling and sensitive data. This inquiry looks to determine how issues such as finality, consent, and data storage are treated in the four countries.

Finally, the last subsection turns to security issues. With the vital importance of cryptography to electronic commerce and the vigorous debate over law enforcement access to network data, an analysis of the data protection framework on these questions is crucial.

2.1 Jurisdiction: Scope of «Personal data» and Clickstream Information2.1 Jurisdiction Scope of «Personal data» and Clickstream Information2.1 Jurisdiction Scope of «Personal data» and Clickstream Information2.1 Jurisdiction Scope of «Personal data» and Clickstream Information

As a threshold issue of statutory competence, data protection regulation only applies to the processing of «personal data.» The European Directive defines «personal data» as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more psychological factors specific to his physical, physiological, mental, economic, cultural or social identity.[87]

For on-line services, the determination of whether particular information relates to an «identifiable person» is unlikely to be straightforward. For example, a dynamic Internet Protocol address is a numeric routing number uniquely associated with a particular session on the Internet and a particular computer being used for that session. An Internet service provider can associate the numeric address with a specific subscriber. However, the sites that are being visited by the user can only associate the numeric address with the Internet service provider. In the absence of other information obtained either by disclosures from the user[88] or from the Internet service provider, the host cannot specifically identify the user. In contrast, a fixed IP address will always identify the same specific computer for every session on the Internet and the identity of the owner will customarily be publicly available.[89]

The recitals in the European Directive recommend that «account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.»[90] The recitals also advise that the data protection rules should not be applicable to «data rendered anonymous in such a way that the data subject is no longer identifiable.»[91] Both interpretive

---

87 Directive 95/46/EC, Art. 2(a).

88 Such disclosures, however, may be made without the user's knowledge. For example, an e-mail address stored in the user's browser may be transmitted to a visited site.

89 The domain name registries and routing tables can be used like a reverse directory to identify the owner of the computer with a fixed IP address.

90 Directive 95/46/EC, Preamble # 26.

91 Directive 95/46/EC, Preamble # 26.

guidance provisions indicate that the definition of the scope of «personal data» represents a critical issue for the treatment of on-line services. The European Commission is, for example, looking to anonymization as a means for protecting privacy in electronic commerce and Member States are also considering «identity protectors.»[92] Yet, for data protection regulation, the means of anonymizing data or hiding the original user's identity may be subject to different national interpretations and, thus, impose varying obligations.

In addition to the definitional threshold, the jurisdictional competence of national data protection law over clickstream data poses a second critical question. The European Directive sets out a basic choice of law provision.[93] However, the allocation of responsibility for clickstream data may be difficult to discern. The clickstream data generated by on-line activities is initially processed by an Internet access or service provider. The bits and bytes are then shared with a myriad of parties to on-line service transactions. The localization of relevant processing activities may be quite variable. Consequently, the determination by various Member States of their authority to apply national law to all or parts of the clickstream will have a significant impact on the development of on-line services.

2.1.1 Belgium2.1.1 Belgium2.1.1 Belgium2.1.1 Belgium

Belgium does not have any data protection legislation that specifically targets on-line services. The general data protection law, the Law of December 8, 1992,[94] will nevertheless apply to information used in connection with on-line services. This law has contradictory tendencies for the scope of personal information covered by the data protection rules. Under the general data protection law, personal information must satisfy two criteria to fall within the scope of protection. First, the information must be of a «personal character» and

---

92 *See* John Borking, *Back to Anonymity-- Privacy Enhancing Technologies* in Proceedings of the 17th International Conference of Data Protection Commissioners (Copenhagen: 1996)

93 Directive 95/46/EC, Art. 4.

94 Loi du 8 décembre 1992 relative à la protection de la vieprivée à l'égard des traitements de données à caractère personnel, M.B., 18 mars 1993, pp. 5801-5614 [hereinafter, Loi du 8 décembre 1992].

relate to an «identified or identifiable natural person.»[95] Second, this qualifying information must be in a «file» defined as having been collected or stored with a logical organization that permits systematic consultation.[96] This concept of «file» distinguishes innocuously stored information from personal information subject to data protection principles.[97] Information stored only for occasional consultation will not qualify for protection.[98] Incidental processing of personally identifiable information also does not come within the statute.[99] The various sectoral data protection provisions contained in other laws such as the consumer credit statute[100] do not contain any rules specific to on-line services with respect to the definition of «personal information» or the treatment of clickstream data.

Unlike other countries' data protection laws, the Belgian statute contains a series of exclusions from substantive coverage whether or not «personal character» information is implicated. These exclusions, in effect, remove specific types of information from the scope of regulated personal information. Specifically, the data protection law does not apply to the following categories of information:

- those used exclusively for private, family or household purposes;
- those published in compliance with legislative or regulatory

---

[95] Loi du 8 décembre 1992, art. 1er, _ 5. The CPVP notes that the legal definition implies three elements: (1) data; (2) relating to a natural person; and, (3) the natural person be identified or identifiable. CPVP, Rapport d'activité 1992-1993, p. 24 (1997).

[96] Commission de la protection de la vie privée, Protection des données à caractère personnel en Belgique: Quelle Commission? Pour quelle vie privée? p. 2 (3 mai 1993).

[97] See, e.g., CPVP, Rapport d'activité 1994-1995, p. 13 (1997); CPVP, Rapport d'activité 1996, pp. 28-29 (1997).

[98] A recent decision of the Cour de Cassation declined to apply the data protection law to a job candidate's file. Cour de Cassation du 16 mai 1997. See also CPVP, Revue de Presse Septembre 1997, p. 8 (excerpting Alain Heyrendt, Un dossier de candidature n'est pas un ficier, La libre Belgique and reprinting the decision).

[99] See Cour d'appel d'Anvers, 1ère Chambre, 27 septembre 1995 *cited in* CPVP, Rapport d'activité 1996, pp. 28-29 (1997)

[100] Loi du 12 juin 1991 relative au crédit à la consommation.

obligation.

- those published or assured publication by the person concerned, provided that the processing respects the purposes for the publication;

- those processed in compliance with the law concerning public statistics.[101]

The exclusion for information made public by the person concerned is likely to be significant for on-line services. This exemption effectively removes certain «public data» from the scope of «personal information.»[102] While the exemption is limited by the finality of the public purpose,[103] participating on open networks such as the Internet often publishes otherwise personal information. For example, a message posting to a discussion group publicly associates the individual's identity with the content of the message and the topic of the discussion group. On-line services will, thus, shift debate to the finality of publication rather than the identifiable aspects of the information in order to determine if the law applies to the data.

The extent to which the Belgian law will regulate the treatment of critical information related to online services, such as an IP address and clickstream data, is ambiguous. There is no clear guidance from the statutory provisions, Royal Decrees, or the *Commission de protection de la vie privée* («CPVP») regarding the identifiable nature of online services data. The rules for caller identification would ordinarily provide useful guidance on the interpretation of the jurisdictional scope of «personal information.» Yet, these services are just being introduced within Belgium. The CPVP has, for the moment, chosen not to issue any public policy with respect to caller identification. For example, the CPVP's Annual Report for 1996 seeks to advance anonymity as a basic principle for telephone communications and notes that anyone should be able to place a call without

---

[101] Loi du 8 décembre 1992, art. 3, _ 2.

[102] CPVP, Recommandation No. 02/93 du 7 septembre 1993 (applying the law to the commercial sale of address lists by BELGACOM as a breach of the finality of the original publication of those addresses.)

[103] CPVP, Rapport d'activité 1994-1995, p. 48 (1997).

communicating his own number.[104] The CPVP then merely indicates that no regulation currently covers this problem. The CPVP is, however, in consultation with Belgacom, the national telephone company, to develop notices that explain the available services for telephone subscribers.

In addition, the scope of the Belgian law seems to encompass even the treatment of anonymous data. Although the data protection law does exclude the treatment of personal information «rendered anonymous for the exclusive purpose of disseminating anonymous statistics,»[105] the exclusion applies only to the law's provisions on notice, access and correction.[106] The exclusion does *not* apply to other obligations under the data protection law such as the declaration requirement.[107] This suggests that anonymity will not suffice to bring the processing of information completely outside the scope of the data protection principles and thereby allows the data protection law to regulate what is otherwise considered to be anonymous data. Moreover, by the terms of the statute, the purpose of anonymity is critical for the exemption; the anonymity must be for a statistical dissemination purpose. For example, an anonymous payment transaction made over the Internet would not be for a statistical purpose and would, therefore, be unlikely to meet the conditions for the exemption. Nevertheless, the CPVP recognizes that the data protection law should not apply to anonymous data.[108] The CPVP has noted, however, that data cannot be considered truly anonymous unless the choice of criteria (e.g. location, age, etc.) prevents the person responsible for the treatment from re-identifying the person concerned without special effort.[109] The CPVP has not elaborated specifically on the scope of 'special effort.' The CPVP has, however, said that, in making a determination of true

---

104 CPVP, Rapport d'activité 1996, p. 61 (1997).

105 Loi du 8 décembre 1992, art. 11.

106 Loi du 8 décembre 1992, art. 11.

107 See infra 2.2.2.

108 CPVP, Recommandation No. 01/96 du 23 septembre 1996 à propos de l'analyse de la consommation de médicaments en Belgique basée sur des informations issues des prescriptions médicales, p. 5

109 Id.

anonymity, it will look to the availability to the person responsible for the processing of any other information from external sources.[110] Thus, if any external information is available that might lead to the re-identification of the individual, the data cannot be considered anonymous. As a consequence of this strict interpretation of anonymity, the electronic traces left behind on-line services may preclude them from being structured in a sufficiently anonymous way. An IP address, for example, will generally allow tracing back to the individual.

In contrast to the narrow limitation for anonymous information, the concept of «file» may prove to exclude significant data processing for online services from the scope of the data protection principles. As noted in the previous parts to this Study, information related to individuals on-line is highly decentralized and flexible in terms of the structure of information processing arrangements. These technical characteristics run counter to the definition of information stored for systematic consultation with a logical organization; dynamic databases may, in fact, have no true «organization» and consultation may be ad hoc rather than systematic in the sense of the statute. For example, the use of any of the many search engines, such as Lycos, Hotbot, or Excite, available on the World Wide Web entails an ad hoc consultation of information stored in diverse sites with no organization particularly relevant to the search criteria. As a result, the substantive reach of the data protection law has some ambiguity for on-line services. This lack of clarity means, for example, that dynamic databases might escape the Belgian rules for data protection.

2.1.2 France2.1.2 France2.1.2 France2.1.2 France

The comprehensive French regime of data protection law has neither a statutory provision specific to the Internet nor a statutory definition explicitly setting out the scope of «personal data» in connection with on-line services. The general data protection law, Law No. 78-17 of January 6, 1978, takes a broad view of the type of data that qualifies for treatment as personal information, and both the CNIL and the Conseil d'État[111] have made a number of important decisions that confirm the expansive scope of the statute. This doctrine supports a

---

[110] Id.

[111] The Conseil d'état is the highest court of administrative appeal in France. Appeals from decisions of the CNIL may be brought to the Conseil d'état.

conclusion that an extremely wide range of processing activities for on-line services will be subject to the rights and obligations of the French data protection law. As a result, French data protection law may apply to a larger range of information flows on the Internet than other European data protection laws, especially the British law.[112] This poses an inherent problem for European harmonization.

Yet, at the same time, the trend for data protection and on-line services in France seems to open the way for narrowing the coverage of French data protection law. The emerging Internet policy of the CNIL seeks to promote anonymity as a means to protect the individual's control over personal information, and this anonymity may be used to differentiate electronic commerce activities that implicate basic rights and those that fall outside the scope of data protection concerns.

Law No. 78-17 defines information as «nominative» if in any way it directly or indirectly permits the identification of a natural person.[113] In the context of on-line services, the traceability of any information back to an individual can classify that information as «nominative,» even if the entity processing that information did not actually know the identity of the data subject. For information that indirectly identifies an individual, the French law makes no distinction between information that can easily be linked to an individual and information that can only be linked with extraordinary means or with the cooperation of third parties. In contrast, the European Directive's policy restricts the scope of «indirectly» identifiable information to that which can reasonably be linked to an identified person.[114] In effect, under the French legal standard, if information *can* be identified with an individual, then the law says information will be considered nominative data; the data protection law will apply to anyone processing such indirectly identifiable data.

The CNIL interpretations confirm an expansive definition and application of French law. In a publication dedicated to summarizing its first decade of

---

[112] See infra 2.1.3.

[113] Loi No. 78-17 du 6 janvier, 1978, article 4 («sont réputées nominatives au sens de la présente loi les information qui permettent, sous quelques forme que ce soit, directement ou non l'identification des personnes physiques auxquelles elles s'appliquent»)

[114] Directive 95/46/EC, Recital # 26.

experience with the data protection law, the CNIL expressly stated that it «gives a very broad interpretation to the term 'nominative information.'»[115] The CNIL, for example, has even indicated that a telephone number and the place of pick-up for a taxi reservation are indirectly nominative information without questioning whether the telephone number relates to the name of the person making the reservation or whether the pick-up address can be related to a specific individual.[116]

A set of decisions in 1997 illustrates that the CNIL intends to continue the expansive philosophy for on-line services. Under its authority to review public sector data processing,[117] the CNIL examined a series of three applications by government offices seeking permission to establish Internet web sites and Internet connections.[118] In three of these decisions, the CNIL addressed the log files that were needed for security purposes and emphasized that they would only contain each visitor's IP address, each visitor's domain name, the web page requested by the visitor and the date and time of the page request.[119] While the visitor's Internet

---

[115] CNIL, Dix ans d'informatique et libertés, p. 42 (1988).

[116] See Délibération No. 90-93 du 10 juillet 1990 portant adoption d'une recommandation concernant les traitements automatisés mis en oeuvre par les sociétés de taxis, *reprinted in* J.O. Informatiques et Libertés No. 1473 (1991). Under the terms of this Recommandation, the CNIL would appear to consider a pick-up address on the Champs Elysées and a restaurant's phone number to be nominative information for the person making the reservation, even though neither can be linked to an individual in the absence of further information.

[117] Loi No. 78-17 du 6 janvier, 1978, article 15 (requires the advice of the CNIL prior to the implementation of government data processing).

[118] See Délibération No. 97-051 du 30 juin 1997 concernant une demande d'avis présenté par la Mairie de Paris relative à un traitement d'informations nominatives mis en oeuvre dans le cadre du site Internet de la Ville de Paris; Délibération No. 97-050 du 24 juin 1997 relative à une demande d'avis présenté par France Télécom concernant un traitement automatisé d'informations nominatives dénommé «Minitelnet;» Délibération No. 97-32 du 6 mai 1997 relative à la demand d'avis présenté par le premier ministre concernant un modèle-type de traitements d'informations nominatives opérés dans le cadre d'un site Internet ministériel; Déliberation No. 97-009 du 4 fevrier 1997 relative à la demande d'avis du Service d'information du Gouvernement concernant le traitement d'informations nominatives opéré dans le cadre du site Internet du Premier Ministre et du Gouvernement.

[119] See Délibération No. 97-051 du 30 juin 1997 concernant une demande d'avis présenté par la Mairie de Paris relative à un traitement d'informations nominatives mis en oeuvre dans le cadre du site Internet de la Ville de Paris; Délibération No. 97-32 du 6 mai 1997 relative à la demand d'avis présenté par le premier ministre concernant un modèle-type de traitements

service provider might be able to determine the identity of the particular user from this information, the web sites themselves would *not* have access to that identity information. Nevertheless, the CNIL noted with approval that these log files would be deleted after fifteen days.[120] By examining the purpose for the existence of the log files and by accepting their deletion within a short time period, the CNIL may be implicitly treating the data as nominative information subject to the storage limitation in the data protection law. Such a conclusion follows the logic for treating telephone reservations for taxis as personal information. Together, these decisions suggest that the CNIL may regard any IP address, whether fixed or dynamic, and all clickstream data as nominative information for the recipients or holders of that information.

Similarly, representatives of the CNIL view «cookies»[121] information as nominative because web servers place this information on the personal computers of visitors in order to identify those visitors when they return to the site. «Cookies,» however, do not independently identify any particular user; the data pertains to use of a particular computer rather than use by a particular person. Instead, to be able to identify a particular user, the information in the file must be linked with other data such as a registration entry at the web site.[122] Although the CNIL has no decision explicitly addressing «cookies,» the CNIL's authorization for government web sites does not grant authority for these sites to place «cookies» on visitors' hard drives.[123]

---

d'informations nominatives opérés dans le cadre d'un site Internet ministériel; Déliberation No. 97-009 du 4 fevrier 1997 relative à la demande d'avis du Service d'information du Gouvernement concernant le traitement d'informations nominatives opéré dans le cadre du site Internet du Premier Ministre et du Gouvernement.

120 Id.

121 See Part I, _ I.3.2 (complete description of «cookies» protocol.)

122 This is increasingly a typical practice for web sites. See Part II, New York Times case study.

123 See Délibération No. 97-051 du 30 juin 1997 concernant une demande d'avis présenté par la Mairie de Paris relative à un traitement d'informations nominatives mis en oeuvre dans le cadre du site Internet de la Ville de Paris; Délibération No. 97-32 du 6 mai 1997 relative à la demand d'avis présenté par le premier ministre concernant un modèle-type de traitements d'informations nominatives opérés dans le cadre d'un site Internet ministériel; Déliberation No. 97-009 du 4 fevrier 1997 relative à la demande d'avis du Service d'information du Gouvernement concernant le traitement d'informations nominatives opéré dans le cadre du site Internet du Premier Ministre et du Gouvernement..

The CNIL also has well articulated views on anonymity that are highly relevant for the application of data protection principles to electronic commerce. For electronic traces associated with a group of individuals, the information will not be considered anonymous if the aggregation is too small. The CNIL rejected, for example, a proposed intelligent transport system in part because of the reliance on collecting and tracking data matched by license plate number.[124] The CNIL's position emphasized the right of citizens to travel anonymously on public roads. Yet, license plate numbers are only indirectly linked to drivers; the license plate number merely identifies the owner of the car and not the actual person driving the car. The significance of treating the license plate number as personal data for the actual driver of the car is that information linked to a small group of people (possible drivers of a particular car) cannot be treated as anonymous, but rather will be considered «nominative.»

Along the same lines, the CNIL has interpreted the scope of nominative information for statistical research. The earliest decisions treated aggregations of census data to be sufficiently anonymous if the aggregation pertained to more than 5,000 people.[125] More recently, the CNIL has authorized the release of census data for an academic research project aggregating information for only 150 people in a relatively homogenous grouping.[126] This approach suggests that the CNIL

---

[124] Délibération no. 96-069 du 10 septembre 1996 relative à la demande d'avis portant création à titre expérimental d'un traitement automatisé d'informations nominatives ayant pour finalité pincipale la lecture automatique des plaques d'immatriculation des véhicules en mouvement par la société des autoroutes Paris-Rhin-Rhône (SAPR).

[125] See CNIL, 16e Rapport d'activité, p. 378-382 (1996). The particular prohibition on disclosing census data for aggregations of less than 5,000 people was, however, successfully challenged before the Conseil d'état for flaws in administrative procedures. See Arrêt du Conseil d'état du 26 juillet, 1996; CNIL, 17e Rapport d'activité, at 33-34 (1997). Another decision in connection with the release of census data allows smaller aggregations in tabular form with specified data fields for particular uses where re-identification, though possible, was precluded by a 'use agreement.' Délibération No. 93-092 du 12 octobre 1993 portant avis sur la demande présentée par l'INSEE, relative à la diffusiondes données aggrégées issues de l'exploitation du rencensement général de la poplulation de 1990, in CNIL, 14e Rapport d'activité, 212-215 (1994). Earlier decisions in the context ofepidemological studies treated aggregations that could not lead to the identification of groups less than 5 people would be treated as anonymous information. See CNIL, Dix ans d'informatique et liberté, p. 49 (1988).

[126] CNIL, 17e Rapport d'activité, at 33-34 (1997).

may eventually view dynamic IP addresses differently than fixed IP address in the future. A dynamic IP address is much like a statistical aggregation for any recipient other than the Internet service provider since the address may pertain to anyone of millions of subscribers to the Internet service provider. A dynamic IP address masks the identity of the individual subscriber behind the mass of all subscribers to the service provider.

In contrast to these decisions, the CNIL rulings on caller identification suggest that French data protection law may treat all IP addresses as nominative information. The CNIL initially refused to allow France Telecom, a national telephone company, to reveal the full detail of calls to subscribers in order to protect information that might relate to others in the household.[127] Subsequently, the CNIL granted authorization for the release of such information only for the purpose of the subscriber's account. While the billing information relates to the subscriber, since the subscriber must pay the charge, the billing information does not implicitly indicate who placed the call. Additional information must be ascertained by the subscriber to indirectly link the transaction to an individual within the household who may have placed the call. In many ways, the caller identification information resembles a dynamic IP address. An Internet service provider assigns a temporary number to its subscriber and anyone receiving that number, such as visited web sites, will only know that it belongs to the Internet service provider. Only the Internet service provider with additional information can link the address to an individual subscriber.

In short, the French data protection law and the CNIL's doctrine leave little room to differentiate information flows on the Internet between anonymous information outside the scope of data protection concerns and identifiable information subject to the full array of rights and obligations. Because clickstream data is ultimately capable of being traced back to an individual, each element of this data appears to be «personal information» anywhere it flows. The practical difficulties and incentives inhibiting actual traces of clickstream data back to

---

[127] Initially, the CNIL authorized the disclosure of called numbers on a subscriber's bills only if the numbers were truncated to anonymize the identity of the call recipient. Déliberation No. 82-104 du 6 juillet, 1982. More recently, the CNIL rescinded the obligation to truncate numbers provided that the subscriber requested the full numbers and certified that the only use would be for managing telephone use. Délibération No. 95-005 relative à la demande de modification de traitement présenté par France Télécom concernant la facturation détaillée; CNIL, 16e Rapport d'activité, at 402-403 (1996).

particular individuals do not appear to have relevance.

Nevertheless, France appears to face a contradiction with the expansive definition of personal information and the recent French trend providing encouragement for anonymous on-line services. The CNIL appears strongly to support anonymity as a possible solution to data protection in the network environment. For example, the CNIL recently criticized an Internet discussion group maintained by a financial services organization because it did not offer users the opportunity to make anonymous message postings.[128] Moreover, the European Directive suggests that data rendered anonymous is no longer subject to the substantive rights and obligations embodied in the European Directive.[129] Yet, anonymity in a network environment is not necessarily absolute. The mapping functions that render data anonymous are not always irreversible. In a set of 1994 cases, the CNIL noted that coded identities for pay-per-view customers still constituted indirectly nominative information.[130] For example, reversal may be accomplished through exceedingly difficult and onerous means such as cracking an algorithm that randomizes information records. More recently, the CNIL addressed anonymity for on-line transactions and praised a proposed electronic payment service that masked the identity of on-line product and service purchasers from merchants by assigning codes to buyers.[131] Although the buyer's information was anonymous with respect to the merchant, the information was «nominative» with respect to the payment service provider. The CNIL did not address whether the merchants could nevertheless treat the information acquired from the electronic payment service as outside the scope of the data protection law.

To the extent that information related to an individual appears incidental to an electronic commerce activity, French law seems to place such information outside the scope of the data protection law. In an early decision, for example, the

---

[128] CNIL, 17e Rapport d'activité, p. 91 (1997)(stating that the Caisse nationale de prévoyance should have structured its discussion group to allow anonymous posts, though recognizing that sophisticated users have the technical means to «borrow a third party's identity in order to participate in the discussion.»)

[129] See Directive 95/46/EC, Recital # 26.

[130] See CNIL, 15e Rapport d'activité, pp. 62-63 (1995).

[131] CNIL, 17e Rapport d'activité, pp. 92-93 (1997)(describing Kléline's system for electronic payments.)

CNIL found that the processing by a business of account data that might reference individuals did not by itself involve nominative data.[132] More recently, the Conseil d'État found that the data protection law did not apply to protect celebrities who were to be the subject of national opinion polls.[133] The Conseil d'État ruled that the reference to celebrities was incidental to the purpose of the poll-- measuring public opinion-- and, consequently, the poll results could not be considered personal information with respect to the celebrities.

The CNIL has also indicated that pseudonyms might be outside the scope of personal information. However, recent decisions seem to include a number of contradictory elements. In its authorization of a web site for the Paris Mayor's office, the CNIL appears to treat all e-mail addresses as 'nominative' information whether or not the e-mail address uses a pseudonym or an anonymous re-mailer; the CNIL's authorization seeks to encourage pseudonymous and anonymous communications with the Mayor's Office, but makes no distinction for the treatment of such communications by the site.[134] In another case, the CNIL granted permission to France Telecom to proceed with an e-mail service, Minitelnet, linking the Minitel to the Internet.[135] In this authorization as well, all e-mail addresses are considered nominative. While these decisions were clearly directed at the majority of cases where an e-mail address identifies an individual, they do not give direct encouragement to the use of anonymous or pseudonymous e-mail-- anonymous and pseudonymous e-mail messages will still be treated as nominative.

2.1.3. Germany2.1.3. Germany2.1.3. Germany2.1.3. Germany

---

132 CNIL, Dix ans d'informatique et libertés, 97 (1988).

133 Conseil d'état, Décision No. 148975 relative à la Chambre Syndicale Syntec Conseil du 9 juillet 1997.

134 Délibération No. 97-051 du 30 juin 1997 concernant une demande d'avis présenté par la Mairie de Paris relative à un traitement d'informations nominatives mis en oeuvre dans le cadre du site Internet de la Ville de Paris.

135 Délibération No. 97-050 du 24 juin 1997 relative à une demande d'avis présenté par France Télécom concernant un traitement automatisé d'informations nominatives dénommé «Minitelnet.»

In the age of the Internet, new kinds of information are generated and issues therefore arise as to which of these new data will be considered as "personal" data in the sense of German data protection law. The concept of "personal information" has traditionally been critical for deciding the applicability of data protection statutes, and German law follows this approach. Thus, the Federal Data Protection Act (BDSG) seeks "to protect the individual against interference with his personality rights resulting from the handling of his personal data (*personenbezogen Daten*)."[136] The Information and Communication Services Act (*Informations- und Kommunikationsdienste-Gesetz*, or "IuKDG") states that it is to "apply to the protection of personal data used in teleservices."[137] While the IuKDG incorporates the BDSG's definition of «personal data,» the law also reduces the significance of this term by providing explicit protection for information that may or may not be «personal» under all circumstances. Such information includes utilization data (*Nutzungsdaten*) and information about pseudonyms. Moreover, the IuKDG identifies the first obligation of the provider of teleservices as making anonymity in cyberspace possible.[138] Only when anonymity is not possible can personal data be created.

At the same time as the IuKDG applies to "personal data," this Law itself does *not* define "personal data." Due to the relationship between the IuKDG and the Federal Data Protection Act's (BDSG), this lack of definition obligates one to refer to the BDSG. The IuKDG explicitly indicates that the BDSG continues to apply to data processing unless specific language in the IuKDG speaks to the situation in question.[139] Thus, the IuKDG Law does not abolish the BDSG, but

---

[136] BDSG, §1(1).

[137] IuKDG, Article 2, § 1(1).

[138] IuKDG, Article 2, § 4 (1).

[139] IuKDG, Art. 2, § 1(2). As one of the drafters of the IuKDG explains, "The Teleservices Data Protection Act concerns itself with the special conditions for the processing of data in Teleservices. Only in circumstances where the Teleservices Data Protection Law contains a special regulation does this regulation have priority over the general Federal Data Protection Law. If the Teleservices Data Protection Law contains no applicable statement, the Federal Data Protection Law is valid." Stefan Engel-Flechsig, Die datenschutzrechtlichen Vorschriften im neuen Informations- und Kommunikationsdienste-Gesetz, Recht der Datenverarbeitung 59, 61 (2/1997)

replaces it only to the extent that this new law contains a specific, applicable regulation.

In light of the IuKDG's definitional silence regarding "personal data," one is obligated to turn to the BDSG to determine the scope of "personal data" and whether IP addresses fall under this rubric. The term "personal data" is itself a critical one for the BDSG; as one treatise has noted, "personal data" is this law's "most important and most frequently utilized concept."[140] In this context, BDSG, § 3 is the relevant section; it states, "'Personal data' means information (*Angabe*) concerning the personal or material circumstances of an identified or identifiable individual (data subject)."[141]

Under German law, legal treatises have traditionally been accorded an important role in deciding the meaning of law. Thus, it is natural to turn to treatises for help in deciding the meaning of "personal data." According to the data protection treatise by Spiros Simitis et al., an identifiable individual exists in the sense of BDSG, § 3 when the information in question "relate to this person and only to him."[142] In this treatise, Ulrich Dammann uses encrypted personal information as an example of when information is identifiable and when it is not.[143] Parties who receive encrypted information, but who do *not* have access to the necessary code to break the encryption will *not* have personal information in their possession; once the code becomes accessible to them, however, the previously anonymous data will become identifiable and thus personal data. Deciding whether or not information is "identifiable," therefore, requires a determination of "the objective identifiability of the concerned party in the concrete case."[144]

A different German data protection treatise speaks of "identifiability" as relating to the "knowledge, means and possibilities of the data processing body."[145]

---

[140] Ulrich Dammann, in Simitis et al, Kommentar zum BDSG, § 3, page 4.

[141] BDSG, § 3(1).

[142] Spiros Simitis, Ulrich Dammann et al, Kommentar zum Bundesdatenschutzgesetz, § 3, 11.

[143] Ulrich Dammann, in Simitis et al, Kommentar zum BDSG, § 3, 14.

[144] Id. at 14 (emphasis removed).

[145] Peter Gola, Rudolf Schomerus, Hans-Joachim Ordemann, Bundesdatenschutzgesetz § 3 (2.8, pg. 90) (6th ed. 1997).

This work makes reference to "one's practical experience" regarding "that kind of possibility [of identifiability] that can be expected with a certain level of probability."[146] Even when the use of additional information allows the individual to be "identifiable," the initial data in question becomes "personal data" for purposes of the BDSG only when the additional information are actually available and are likely to be used to make the information identifiable.

This analysis is also supported by looking at a concept that is the opposite of identifiability-- namely, anonymity. The BDSG, § 3(7) defines anonymization (*Anonymisieren*) as "the alteration of personal data in such a way that specific information on the personal or material circumstances of an identified or identifiable natural person can no longer be attributable to him or only with a disproportionately great expenditure of time, money, and labor."[147] This definition supports the idea that "identifiability" depends on a likelihood that a reasonable effort can lead to personal data that refer to only one person.

This analysis indicates that under German law: (1) when the use of IP addresses and other kinds of information (such as clickstream data) can be combined with other data to identify an individual, and (2) these data are likely to be used to make this identification, (3) initial information will be "identifiable" and, therefore, "personal data" under the IuKDG. The IuKDG supports this interpretation by explicitly providing specific protection for utilization data (*Nutzungsdaten*), accounting data (*Abrechnungsdaten*), contractual data (*Bestandsdaten*), and even pseudonyms. For example, utilization data, which are defined as information that enable the user to utilize teleservices,[148] are to be erased as soon as possible and are not to be transmitted to other providers or third parties.[149] It must also be stressed that, as will be discussed below, the IuKDG requires the provider of teleservices to make anonymous or pseudonymous use of its services possible. Thus, the first obligation for a provider under German data protection law is, «to the extent technically feasible and reasonable,» to prevent

---

[146] Id.

[147] BDSG, § 3(7).

[148] Id. at Article 2, § 6(1)(1).

[149] Id. at Article 2, §6(2) & (3).

personal information from ever being generated.[150]

The IuKDG also indicates that IP addresses and clickstream data might sometimes be regarded as personal data by moving away from the BDSG's requirements regarding "data files."[151] Under the Federal Data Protection Law, certain requirements apply only to information in data files. In contrast, the IuKDG states, "Unless otherwise provided in this Act, the relevant provisions concerning the protection of personal data shall be applicable even if the data are not processed or used in data files."[152] This provision indicates that the IuKDG's data protection requirements will *not* hinge upon whether collections of personal information fulfill the BDSG's notion of "data files."

Turning from the issue of IP addresses as personal data in Germany, this study will now consider anonymization and pseudonyms. The IuKDG contains strong and explicit provisions to make anonymity possible in the on-line world. The Law requires service providers "to offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable."[153] It also explicitly requires providers to inform users of these options.[154] Moreover, a user has a right of access not only to the provider's stored data regarding his person but also to stored data about his pseudonym.[155]

Pseudonyms also play an important role in the Law's regulation of profiling. The IuKDG generally restricts user profiles to circumstances under which pseudonyms are used. Such anonymous profiles are *not* to be linked to identifiable data.[156] As the Law states, "Profiles retrievable under pseudonyms

---

[150] Id., at Article 2, §4(1). See Article 2, §3(4)(«The design and selection of technical devices to be used forteleservices shall be oriented toward the goal of collecting, processing and using either no personal data at all or as few data as possible.»).

[151] See BDSG, § 3(2), § 14(1), § 20(2), § 27(1).

[152] IuKDG, Article 2, §1(2).

[153] IuKDG, Article 2, § 4.

[154] Id.

[155] IuKDG, Article 2, § 7.

[156] IuKDG, Article 2, § 4(4).

shall not be combined with data related to the bearer of the pseudonym."[157] The issue of profiling will be explored in more detail below.

It is important to note one important limitation on a certain kind of use of pseudonyms. As the section on cryptography discusses below, German law permits publicly certified digital signatures to be utilized on a pseudonymous basis,[158] but requires the certification authority to know the individual's identity. Under certain circumstances, the certification authority must share that information with law enforcement authorities.

Anonymity also plays an important role in limiting the use that providers may make of utilization and accounting data. The initial service provider may not transmit to other providers whose on-line services have been used any data other than accounting data and "anonymised utilization data for the purposes of their market research."[159] In addition to these provisions regarding anonymization and pseudonyms, the IuKDG requires the provider to take technical and organizational precautions to ensure that "the user is protected against third parties obtaining knowledge of his use of teleservices."[160] These are extremely high standards that appear to prohibit the sharing of such data as "http" information about web sites visited with outside parties.

One German on-line service provider is already following the requirements of the IuKDG. T-Online is the on-line service of Deutsche Telekom, which is the newly privatized former German state telecommunications service. Deutsche Telekom generally assigns e-mail addresses that consist only of numbers. It then allows each T-Online member to choose his own email name and terms the resulting email address, the "email Alias."[161] By first starting out with an email address that is numerical and terming any transformation of this number into letters the "email Alias," T-Online emphasizes the customer's freedom to choose a pseudonym.

---

[157] Id.

[158] See section 2.5.3.

[159] IuKDG, Article 2, § 6(3).

[160] IuKDG, Article 2, § 4(2)(3).

[161] T-Online: Macht alles fuer jeden so einfach 22 (5/97).

2.1.4 United Kingdom2.1.4 United Kingdom2.1.4 United Kingdom2.1.4 United Kingdom

The British data protection regime has no statutory provision specific to the Internet. No law speaks explicitly to the scope of information constituting "personal data" in connection with on-line services. The general data protection law, the Data Protection Act of 1984, defines "personal data" as "data consisting of information which relates to a living individual who can be identified from the information (or from that and other information in the possession of the data user)...."[162] This definition clearly suggests that an IP address will be viewed as identifiable data when additional information allow it to be used identify the data user, but not when such additional information is unavailable. The Data Protection Registrar and the Home Office have both advocated such an interpretation of the law.

The Registrar specifically addressed the issue of whether an email address is personal data in an official paper, "Data Protection and the Internet." In this document, the Registrar states:

> The answer [whether an IP address is personal data] will depend on a number of facts: whether the address is issued to a particular individual; what is the context in which it is held; whether it itself identifies an individual; etc. If the address can be related to an identifiable individual either from itself or from itself and other information in the possession of the data user, it is personal data.[163]

In this view, an e-mail address is personal data under British data protection law only when it can be related to an identifiable person.

The Home Office has taken a similar approach in its paper regarding the Government's proposals for implementing the European Directive.[164] In this

---

[162] Data Protection Act 1984, 1(3).

[163] http://www.open.gov.uk/dpr/internet.htm

[164] Data Protection: The Government's Proposals (July 1997). <http://www.homeoffice.gov.uk/ datap1.htm>

paper, which was issued in July 1997, the Home Office states that it interprets the term "'personal data' as excluding anonymous information to which identifiers are unlikely to be capable of being attached."[165] The Home Office provides the following example, "[W]here a person holds data which are to him anonymous and does not hold complementary information which might help to identify the people concerned, the mere existence of such information elsewhere should not make the data personal within the meaning of the Directive. There must be a reasonable likelihood of the two pieces of information being brought together."[166]

This analysis is analogous to established British data protection law regarding telephone numbers.[167] Generally, telephone numbers are viewed as personal information in the United Kingdom when they refer to an individual subscriber. As for work telephone numbers, these can become personal information depending on the circumstances. For example, when a telephone number is assigned to a specific person, or when telephone calls are logged and attributed to a specific person, an extension number will become a personal number.

The Data Protection Act does not itself explicitly include anonymity as one of its core seven data protection principles. Anonymity does clearly relate, however, to several of these principles; perhaps the two most relevant principles are "fairness" and to collect only personal information that is "adequate, relevant and not excessive."[168]

The Data Protection Registrar has emphasized the importance of anonymity in the on-line world. One of the most important such references to anonymity came in the Data Protection Registrar's response to "government.direct," which is an important British initiative for the on-line delivery of government services. The "government.direct" Green Paper pointed to strategies for the electronic delivery of such services as "providing information, collecting taxes, granting licenses, administering regulation, paying grants and

---

[165] Id. at 2.3.

[166] Id.

[167] This analysis is based on a personal communication from a member of the staff of the Data Protection Registrar.

[168] Data Protection Act 1984, Schedule 1, Part I.

benefits, collecting and analysing statistics, and procuring goods and services.[169] "government.direct" seeks to utilize information technology to bring government closer to the individual, make public services more accessible, and give citizens and businesses more control over their dealing with the government.[170]

In response to this initiative, the Data Protection Registrar stressed the importance of anonymity. The Registrar observed, "Where services are to be delivered electronically, service or benefit providers do not necessarily need to know at all times the precise identify of an individual."[171] Technology is to be made available that will provide individuals with a secure method of authorizing and authenticating transactions electronically while also "minimising the need for actual identification whenever possible."[172] This minimalization of identification of data users will be made possible through the incorporation of privacy enhancing technologies.

It is likely that anonymity and the use of pseudonyms will play an increasing important role in British data protection. The most likely trend in an on-line environment is for anonymity and the use of pseudonyms to be interpreted as key elements of the core data protection principles.

2.2 Jurisdiction: Registration and Supervision by Data Protection Authorities2.2 Jurisdiction Registration and Supervision by Data Protection Authorities2.2 Jurisdiction Registration and Supervision by Data Protection Authorities2.2 Jurisdiction Registration and Supervision by Data Protection Authorities

The international nature of on-line services raises a second set of jurisdictional issues regarding the territorial applications of substantive data protection rules. The European Directive instructs each member state to apply its national provisions when: (a) the processing is carried out by a data controller in

---

[169] <http://www.open.gov.uk/citu/gdirect/greenpaper/chap1.htm>

[170] <http://www.open.gov.uk/citu/gdirect/greenpaper/foreword.htm>

[171] Response to Government.Direct Including a Paper on Privacy Enhancing Technology, Appendix 11, 13 Activities Report, 103.

[172] Id.

the member state, including situations in which a controller may be processing personal data in several member states, (b) the national law applies by virture of international public law even though the controller may not be established in that member state, or (c) the controller is outside the Community, but makes use of equipment within the Community for purposes of processing the information.[173] In effect, multiple national laws may apply to on-line services.

Registration requirements with data protection authorities and supervision by these officials offer a good glimpse of the scope of data protection regulation for on-line services and a practical set of conflicting issues that might arise. The European Directive requires notification to Member State data protection authorities prior to the processing of personal data.[174] Existing laws in European nations already require that a data user who holds personal information register all nonexempt data with the national oversight authority. For example, the United Kingdom's Data Protection Registrar has summarized its national requirements in this fashion, "every data user who holds personal data must be registered, unless all the data are exempt.»[175]

With the Internet, however, any information that is on-line may be transferred to any Internet user anywhere in the world. On-line services and web browsing often involve the collection of information by a server located in a country other than the user's state. For example, a French Internet user may fill in a form found while searching the World Wide Web to request product information. The form may reside on a server in Montreal, but the server may send the collected personal data for processing in Frankfurt/Main. As a result, the various sites and foreign data users may have an obligation to register with one or more given European data protection authorities. Examination of the obligation to register is a shorthand way of assessing the applicability of the full set of data protections to remote, global activities.

On-line services challenge the effectiveness of data protection officials' supervision of data processing practices. Article 28 of the European Directive requires the creation of such independent authorities who will be "responsible for monitoring the application within its territory of the provisions adopted by the

---

173 Directive 95/46/EC, Art. 4. See also *id*., at Recitals 18-20.

174 Directive 95/46/EC, Art. 18.

175 Data Protection Registrar, The Guidelines, p.6 (Third Series, Nov. 1994).

Member States." The European Directive also requires each national data protection authority to pay attention to data processing *outside* national boundaries through its provisions regarding international data transfers. Such extraterritorial oversight will be far from easy to carry out. As a further element of difficulty, in Germany, where federal and state data protection commissioners have different kinds of oversight authority, the question of who has responsibility for oversight of international on-line services will arise. This sub-section will seek to analyze how the Member States interpret the applicability of their national laws to global activities on the Internet.

2.2.1 Belgium2.2.1 Belgium2.2.1 Belgium2.2.1 Belgium

Belgium requires the filing of a declaration to the CPVP prior to the commencement of any processing of personal information.[176] While no special rules apply to online services, the general data protection law will require the declaration of processing for such services. The law seeks to assure the disclosure of data processing activities. The declaration must indicate: (a) the date of application or the date of the law, decree, ordinance, or regulatory action that authorized the processing; (b) the name and address of the person responsible for processing the information; (c) the name and address of the person managing the processing; (d) the purpose for the processing; (e) the types of information being processed, specifically identifying any forms of sensitive information; (f) the persons authorized to obtain the personal information; (g) the guarantees for medical data; (h) the means by which individuals are given notice of the processing, the office where the right of access may be exercised, and the measures taken to facilitate such right; (i) the maximum duration of storage, use and dissemination.[177] For public sector data processing, a statute or Royal Decree must authorize the processing of personal information prior to the filing of the declaration. Like many of its counterparts in other countries, the CPVP has an important advisory role in the preparation of such statutes and decrees.[178]

As a reflection of the extremely broad territorial scope of the Belgian data

---

[176] Loi du 8 décembre 1992, art. 17, _ 1er.

[177] Loi du 8 décembre 1992, art. 17, _ 3.

[178] CPVP, Rapport d'activité 1992-1993, p. 11-12 (1997).

protection law, this declaration requirement applies to «any automatic treatment even if all or part of the processing takes place abroad in the event that such processing is directly accessible in Belgium by means that are specific to the processing.»[179] In effect, this creates a substantive choice of law rule that makes Belgian standards the applicable law for the treatment of personal information.[180] When no human intervention is needed and the processing abroad is accessible in Belgium, then Belgian law will apply. This principle establishes that if a user of personal information is in Belgium, the location of actual processing is irrelevant for the application of Belgian law to the user of the personal information and the processing must be declared to the CPVP.[181] The converse may also apply: if the user of personal information is located outside of Belgium, but obtains access to information in Belgium, then the Belgian rules might apply to the use of the personal information. The law, however, is ambiguous in this situation.[182] According to the CPVP, the law does not apply to processing not «directly accessible» outside of Belgium.[183] The official examples used for accessibility examine the inbound flow of information (i.e. data held outside of Belgium for use within Belgium under the control of someone within Belgium). But, the statute expressly applies the notice requirements to the collection of information occurring within Belgium for processing outside of Belgium,[184] and the law forbids the collection within Belgium for processing abroad of sensitive data that would otherwise be restricted under the law.[185] If the Belgian law applied fully to

---

[179] Loi du 8 décembre 1992, art. 3, _ 1er.

[180] M-H. Boulanger, C. De Terwangne et Th. Léonard, La protection de la vieprivée à l'égard des traitements de données à caractère personnel-- La Loi du 8 décembre 1992, Journal des Tribunaux, 15 mai 1993, p. 375.

[181] CPVP, Rapport d'activité 1994-1995, p. 17-18 (1997) (explaining the Commission's interpretation of the territorial reach of the Belgian law.)

[182] Id.

[183] Id.

[184] Loi du 8 décembre 1992, art. 4. The CPVP takes the position that this obligation only attaches if the information will be «accessible» in Belgium. CPVP, Rapport d'activité 1994-1995, p. 18 (1997)

[185] Loi du 8 décembre 1992, art. 3, _ 2.

situations in which obtaining data within Belgium sufficed to apply Belgian law to the processing, this special export provision would not be necessary for sensitive data.

In either case, the broad territorial reach is likely to have significant impact for on-line services. Anytime personal information residing on servers outside of Belgium is used within Belgium, multiple laws will apply to the on-line activity; the law of the place where the server is located as well as the law of Belgium. Similarly, if information originates in Belgium, foreign services may still find themselves subject to Belgian law. If they do not, then the difference in territorial application provides a disincentive to locate electronic services in Belgium. In particular, the location of a server outside of Belgium with data being input world-wide, such as through the completion of an on-line subscription form, might avoid the strictures of the Belgian law. The processing would not be «accessed» within Belgium-- rather the data would be obtained within Belgium.

When Belgian law applies, the user or «controller» of the database (the «*maître du fichier*») must have a presence in Belgium, either through an existing legal domicile, through the election of a Belgian domicile, or, for foreign parties, through the designation of a Belgian agent.[186] The status of «controller,» however, is a vague concept in the Belgian law. Article 6 of the data protection law defines the «controller» as the person or entity «competent to decide the purposes of processing or the type of information to be included.»[187] According to the CPVP, the «controller» will be the person ultimately responsible for the information.[188]

Belgium has faced some difficulty assessing an appropriate fee for the declaration of processing. At present, the fees are progressive according to the significance of the data processing as measured by the number of individuals to whom the processing relates and whether the declaration is made on paper or in electronic form.[189]

---

[186] Loi du 8 décembre 1992, art. 1 _ 6.

[187] Loi du 8 décembre 1992, art. 1 _ 6.

[188] CPVP, Rapport d'activité 1994-1995, pp. 15-16 (1997).

[189] Arrêté royal no. 12*bis* du 16 mars 1996 modifiant l'arrêté royal no. 12 du 7 mars relatif à la contribution àverser lors de la déclaration des traitements de données à caractère personnel à la Commission de la protection de la vieprivée, M.B., 15 mars 1996, p. 5801 et seq.

Under the Belgian law, a Royal Decree can exempt categories of processing from the obligation to declaration requirement if the information and the processing obviously do not threaten privacy.[190] This provision was inspired by the French law authorizing the national data protection authority to allow simplified registration for certain types of data processing.[191] In Belgium, a wide range of common data processing activities have been exempted from declaration, particularly those involving:

1. Salary administration
2. Personnel management (excluding health information or sensitive information)
3. Accounting
4. Partner and shareholder administration
5. Client and supplier management
6. Member and donor administration
7. Communications data
8. Visitors' logs
9. Student records
10. Communal registries
11. Public registers
12. Social security
13. Processing pursuant to specific rules.[192]

The treatment of personal information will only qualify for the exemption from declaration, however, if a set of specific conditions exist for the processing: (1) a predetermined finality limits the type of information being processed; (2) restrictions on the source of storage are imposed; (3) restrictions on data use are

---

[190] Loi du 8 décembre 1992, art. 17 _ 8.

[191] Rappor au Roi sur l'Arrêté Royal (No. 13) du 12 mars 1996, M.B., 15 mars 1996, p. 5802 (noting the Belgian transplantation from French law). For a discussion of France, see _ 2.2.2, infra.

[192] Arrêté Royal (No. 13) du 12 mars 1996 portant exemption conditionelle de l'obligation de déclaration pour certaines catégories de traitements automisés de données à caractère personnel qui ne présentent manifestement pas de risque d'atteinte à la vie privée, M.B., 15 mars 1996, p. 5816; CPVP, Rapport d'activité 1996, pp.48-49 (1997).

imposed; (4) the communication to third parties of the information is prohibited; and (5) a limitation on the duration of data storage exists.[193] If these conditions are not met, then the Royal Decree does not grant an exemption from the law's declaration requirement; the processing is permissible subject to satisfaction of the declaration obligation as well as the other data protection principles contained in the law.

Various aspects or functions of online activities may, thus, qualify for the exemption from declaration. However, these exemptions are reasonably specific by comparison to many Internet activities. The exemption for «visitors' logs» would probably not apply, for example, to the log files maintained by many web sites to track usage. The exemption only covers controlled entry logs of visitors to work sites and may only include specific information: name, professional address, identification of the employer, identification of the person's car used for site access, the area and identity of the person being visited and the date and time of the visit.[194] While many parallels exist between these physical site logs and virtual site logs, only the processing *strictly* conforming to the Royal Decree can be exempt from declaration.

For on-line services, a significant gap appears to exist between the legal requirements and actual practices. For example, despite the declaration requirement, none of the major operators of on-line services in Belgium has declared the treatment of personal information to the CPVP.[195] While account management and communications data for switching purposes are exempt from declaration, subscriber profiling and the transmission of subscriber data to third parties such as the transmission of IP addresses and information concerning subscriber's browsers[196] would not be covered by the exemption.

In terms of supervision, the Belgian data protection law disbanded the *Commission consultative de la protection de la vie privée* and created a new, semi-independent supervisory authority-- theCPVP, *Commission de protection de*

---

193 Id.

194 Arrêté Royal (No. 13) du 12 mars 1996, art. 9.

195 A search of the Commission's register for Microsoft Network (MSN), Skynet, CompuServe, Datapak, and Interpac on August 5, 1997 revealed no entries.

196 This is generally part of the <http> protocol information that is transmitted to remote web sites.

la vie privée.[197] In addition, specific laws may establish a sectoral advisory committee such as the Oversight Committee of the Banque-carrefour de la sécurité sociale.[198] While the members of the CPVP are appointed to serve as independent watchdogs, the CPVP itself depends upon the Ministry of Justice for both its staff and budget.[199] This dependance vitiates complete independent oversight of data protection. The transposition of the European Directive should affect this structure,[200] but the revised draft of the proposed Belgian legislation does not offer any modification to the institutional arrangements.[201]

2.2.2 France2.2.2 France2.2.2 France2.2.2 France

France requires the public disclosure of all data processing of nominative information and assigns the role of supervision to the CNIL. Public sector data processing may not take place without specific statutory authority or a regulation promulgated after approval by the CNIL.[202] If the CNIL refuses to approve the proposed regulation, then the processing may only take place following approval by the Council of State and adoption of a decree.[203] For the private sector, France requires that a declaration be made to the CNIL of any processing of nominative information prior to the commencement of processing.[204] The CNIL must accept

---

197 Loi du 8 décembre 1992, art. 23.

198 See Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, chapitre VI, M.B., 22 février 1990, pp. 3295 et. seq.

199 Id.; CPVP, Rapport d'activité 1996, p. 58 (1997).

200 CPVP, Rapport d'activité 1996, p. 58 (1997) *citing* Avis No. 30/96 du 13 novembre 1996 concerant l'Avant-Projet de loi adaptant la loi du 8 décembre 1992 à la Directive européenne.

201 See Projet de loi adaptant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel à la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protectiondes personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

202 Loi No. 78-18 du 6 janvier 1978, art. 15.

203 Id.

204 Loi No. 78-17 du 6 janvier 1978, art. 16.

any declaration formally complying with the required elements of disclosure.[205] France does not have any particular statutory provision enumerating specific registration requirements for on-line services or for Internet activities. The general obligations apply to on-line services and, for these services, the territorial reach of the law appears to extend beyond French borders.

In terms of supervision, authority rests with the CNIL and with individuals. The CNIL is charged with monitoring respect for the data protection law[206] and may submit cases of illegality to the public prosecutor for enforcement actions.[207] The CNIL has an indirect enforcement power, however, through its investigatory missions, site visits, and notification process.[208] As a 'public order' statute, the data protection law includes criminal sanctions for violations of the requirements including registration. However, under the generally applicable principles of the French criminal code, sanctions may only be imposed if the violation takes place on French territory or if one of the acts contributing to the violation takes place on French territory.[209] This principle will, thus, limit these supervision powers over multinational on-line services to those activities taking place*within* France. For example, the CNIL's powers to compell a party to comply with investigatory requests will not have force if the party is outside of France. Otherwise, individuals may also «supervise» data processing to the extent that the law gives individuals a right of access to their data and a right of correction.[210] French law does not distinguish between residents and non-residents for these rights of access and correction.

Ordinarily, the provisions of French national law apply only to processing

---

[205] See Arrêt du Conseil d'État du 6 janvier 1997 (voiding the implicit rejection by the CNIL of a declaration of processing)*reprinted in* CNIL, 17e Rapport d'activitéé, p. 414 (1997)

[206] Loi No. 78-17 du 6 janvier 1978, art. 6.

[207] Id., art. 11.

[208] Loi No. 78-17 du 6 janvier 1978, art. 21.

[209] Nouveau Code Pénal, Art. 113-2 («La loi pénale française est applicable aux infractions commises sur le territoire de la République. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire.»)

[210] Loi No. 78-17 du 6 janvier 1978, art. 34, 36.

activities in France. This territorial limitation is seen in the CNIL's authority to restrict transborder data flows if foreign processing will contravene French data protection principles.[211] A law designed for extra-territorial application would not have a policy need to block foreign data transfers because it would presumably regulate this processing directly.

In addition, the data protection law's registration requirement itself suggests that information partially obtained in France for purposes of processing abroad, such as the clickstream data generated in France from on-line services for use outside of France, is a data export.[212] But, several recent decisions suggest that France will apply the French standards to anyone accessing data that is located within France.[213] In discussing the arrangements for airline reservation systems, the CNIL established that companies using international airline reservation systems must follow the legal standards of the place where the information was collected.[214] Under this doctrine, any web site collecting nominative information from users located within France will be subject to the registration requirement of French law prior to collecting such information. Specifically, if a French user responded to a form on a foreign site that was used to collect nominative information, the foreign site would be required to register with the CNIL prior to accepting the information from the French user. In essence, access to information localized in France will be assimilated to processing such information in France; registration obligations will attach to the site of collection or to the point of data entry as well as the site of use. Thus, whether different actors must register under French data protection law may depend upon the nature of the contacts with the French forum and not just the situs of the actor.

---

211 Loi No. 78-17 du 6 janvier 1978, art. 24 («la transmission entre le territoire français et l'étranger, sous quelque forme que ce soit, d'informations nominatives faisant l'objet de traitements automatisés régis par l'article 16 ci-dessus [obligation de déclaration] peut être soumise à autorisation préalable ... en vue d'assurer le respect des principes posés par la présente loi.»).

212 Loi No. 78-17 du 6 janvier 1978, art. 19 («la déclaration doit préciser: .... si le traitement est destiné à l'expédition d'informations nominatives entre le territoire français et l'étranger, sous quelque forme que ce soit, y compris lorsqu'il est l'objet d'opérations partiellement effectuées sur le territoire français à partir d'opérations antérieurement réalisées hor de France.»)

213 CNIL, 17e Rapport d'activité 1996, p. 106

214 CNIL, 17e Rapport d'activité 1996, p. 106

For data processing subject to the registration obligation, French law requires the designation of a person within France who controls the processing or, in the absence of a controller in France, the designation of a legal representative in France.[215] This requirement would oblige anyone accessing information on-line that is stored on a server located in France to designate an agent within France. The airline reservation systems decision also made an important point regarding the responsibility of parties in a decentralized network. Under the decision, equipment providers and service providers might be liable for data processing in each country where established.[216] This position has important implications for browsers, search engines and similar technology. To the extent that these technologies create nominative information or search for nominative information on French web sites, they might be subject to French registration requirements and the obligations of the data protection statute. For example, the movement toward a definition of an Open Profiling Standard and the incorporation of such a standard in browser software would result in the retention by browser software of detailed, nominative information. Users would be asked to provide demographic information to the browser for future automatic collection by web sites. The retention and subsequent disclosure by browser software may make the manufacturer of the software responsible for some of the information processing activities.[217] For example, the manner in which the browser software incorporates the Open Profile Standard is significant. A manufacture who requires that all data fields be completed prior to the installation of the browser software on a user's personal computer would be in likely contravention of the notice, opposition and relevancy requirements of the French data protection law.

In essence, French law may result in multiple registrations for any single on-line commerce activity. This result arises from clickstream data passing through many entities on the Internet and the likely broad interpretation of the definition of nominative information to include clickstream information collected by any

---

[215] This requirement derives from the information that is required to be included in the registration declaration. Loi No. 78-17 du 6 janvier 1978, art. 19.

[216] CNIL, 17e Rapport d'activité 1996, p. 106.

[217] Although the data would still be entered into the browser by the user and the data would be tagged by the user for different levels of disclosure, the manufacturer controls the data fields, formats and processing by the software (including security) that would each be subject to the protections of the data protection law.

recipient. For example, an on-line subscription to an electronic journal such as *Le Monde* will require the registration of the subscription and browsing processing by *Le Monde*, the browsing processing by the Internet Service Provider, the payment processing by the financial intermediary, and any profiling by third parties such as DoubleClick.

The CNIL is just beginning to focus on registration issues and compliance by Internet Service Providers. In 1995, the CNIL announced an investigation of various on-line service providers including MSN, AOL and Club-Internet.[218] However, to date the investigations have not been concluded and predictions regarding their impact would be premature. Nevertheless, the CNIL may be heading toward the eventual elaboration of a simplified registration process for Internet sites.[219] This might alleviate the otherwise required lengthy application process for every Internet site collecting such minimal information as log files or IP addresses.

French data protection law already allows the CNIL to accept «simplified declarations» for routine processing that does not threaten privacy or freedom.[220] For public sector sites, the CNIL has already granted permission for a proposed government regulation that would authorize agencies to establish Internet sites conforming to a specific model containing approved types of information, finality and notice.[221] At the moment, however, no simplified registration process for on-line services in the private sector. A number of existing simplified registration categories are relevant for on-line services and electronic commerce, such as account and billing data,[222] client management processing,[223] payment records held

---

[218] See CNIL, 16e Rapport d'activité, p. 86.

[219] Already, the CNIL has taken this approach for some limited public sector Internet sites. See Délibération No. 97-032 du 6 mai 1997 relative à la demande d'avis présenté par le premier ministre concernant un modèle-type de traitements d'informations nominative opérés dans le cadre d'un site Internet ministériel.

[220] Loi No. 78-17 du 6 janvier 1978, art. 17. The CNIL has approved 40 simplified registration declaration forms. CNIL, 17e Rapport d'activité, at p. 13.

[221] Délibération No. 97-032 du 6 mai 1997 relative à la demande d'avis présenté par le premier ministre concernant un modèle-type de traitements d'informations nominative opérés dans le cadre d'un site Internet ministériel.

[222] Norme Simplifiée No. 14, Délibération No. 80-33 du 21 octobre 1980 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des fichiers de

by financial institutions,[224] or mailing list processing if used to send information other than commercial soliciations.[225] However, these simplified declarations are unlikely to apply to many on-line services. To qualify for a simplified declaration, the processing must conform strictly to the requirements established by the CNIL including finality and types of information collected. Yet, on-line services will generally collect types of information, such as an e-mail addresses, encryption codes and log file information, that is not included in the authorization for simplified registration.

France has also taken a special interest in the supervision of processing of data held in the public sector. A series of decisions concerning the use of on-line directories demonstrates particular concern for the territorial application of French law. The CNIL has required public agencies to warn Internet users that directory services supplied by the agency on their sites are subject to the protections of the French law. In one case, the CNIL noted that the site operators planned to put the notice in French as well as English along with the text of the French law in both languages.[226] The fact that the CNIL endorsed an English language notice for the French web site is in itself extraordinary, given the national emphasis on the French language. France seems to be using the host site within France as a pressure point for assuring local standards in the international environment.

2.2.3 Germany2.2.3 Germany2.2.3 Germany2.2.3 Germany

On-line services can pose difficult challenges to a requirement of registration with a data protection authority and raise complicated issues regarding

---

fournisseurs comportant des personnes physiques.

[223] Norme Simplifiée No. 11, Délibération No. 80-21 du 24 juin 1980 concernant les traitements automatisés d'informations nominatives relatifs à la gestion des fichiers de clients.

[224] Norme Simplifiée No. 12, Délibération No. 80-22 du 8 juillet 1980 concernant les traitements automatisés d'informations nominatives relatifs à la tenue des comptes de la clientèle et le traitement des informations s'y rattachant par les établissements bancaires et assimilés.

[225] Norme Simplifiée No. 15, Délibération No. 80-32 du 21 octobre 1980 concernant les traitements automatisés d'informations nominatives relatifs aux listes d'adresses ayant pour objet l'envoi d'informations

[226] See CNIL, 16e Rapport d'activité 84-85 (1996).

the ability of these officials to supervise and oversee data processing. This Study's analysis of these issues in Germany begins with a discussion of German law's traditional decentralized approach to data protection supervision. Data protection oversight agencies have been created at both the federal and state levels in Germany.

The federal data protection law (BDSG) assigns an oversight role for the federal public sector to the Federal Data Protection Commissioner.[227] State data protection laws assign to state data protection commissioners a similar oversight role over state public organizations. As for the private sector, the BDSG assigns governmental oversight over private organizations to the so-called "Supervisory Authority."[228] Some states have assigned this oversight role to existing state data protection commissioners; other states have granted these duties to a different governmental authority. Finally, the BDSG requires companies in the private sector to appoint an internal data protection officer if they have at least five employees involved with processing personal data.[229] These officers are to monitor the proper use of projects involving the processing of personal data.[230]

German data protection commissioners in the public sector and the Supervisory Authorities in the private sector primarily have an advisory role. Although binding legal decisions concerning data processing generally rest elsewhere (exceptions will be discussed below), these data protection authorities can investigate certain data processors. The federal and state data protection commissioners can submit formal complaints to the responsible ministers at the level of the federal government and*Länder*. Moreover, BDSG, § 38(4) allows the Supervisory Authority "to enter the property and office premises of the body during business hours and to conduct examinations and inspections there."[231] The data protection authorities can also issue appeals to the media and to the legislature. Moreover, data protection authorities have a special obligation to help anyone who believes that the processing of her personal data has caused a hardship

---

[227] BDSG, §§ 22-26 .

[228] BDSG, § 38.

[229] BDSG, §§ 36-37.

[230] BDSG, § 37.

[231] BDSG, § 38(4).

to her privacy rights.

Germany does *not* grant its data protection authorities the power to license collections of personal data. In addition, except in a limited range of circumstances, data protection authorities cannot order governmental or private bodies that process information to take certain actions or desist from other behavior. Thus, the BDSG requires the Federal Data Protection Commissioner to lodge complaints with other authorities should he "discover any violation of the provisions of this Act or of other provisions on data protection or some other irregularities in the processing or use of personal data."[232] State data protection commissioners also have a similar power (*Beanstandungsrecht*).[233] As for the Supervisory Authorities, who are appointed in easch state to monitor private organizations, they can direct measures to be taken only "to eliminate technical or organizational shortcomings."[234]

German law does require, however, that data processing bodies maintain registers of certain data banks. For example, BDSG, § 18 requires public bodies to "maintain a register of the data-processing systems used."[235] This register is shared with the Federal Data Protection Commissioner and may be inspected by anyone. As David Flaherty has noted, "the register allows reflection on the bureaucratic development of public administration by identifying the reasons for the existence and use of certain data bases."[236]

In the private sector, the Supervisory Authority is also required to keep a register of certain data banks. The BDSG requires "[b]odies which store personal data as business" to notify the relevant supervisory authorities.[237] Electronic registration does not yet appear to be taking place in Germany. As Stefan Walz, the data protection commissioner of Bremen, has noted, the register is the

---

[232] BDSG, § 25.

[233] See, e.g., Hessisches Datenschutzrecht, § 27.

[234] BDSG, § 38(5).

[235] BDSG, § 18.

[236] David Flaherty, Protecting Privacy in Surveillance Societies 60 (1989).

[237] BDSG, § 32.

"foundation and the essential orientation for my inspection activities."[238] As noted above, these inspection activities take place under the authority granted in BDSG, §38(4).

The IuKDG remains within the traditional German approach to oversight. First, it requires no additional registration requirement. The IuKDG states, "Within the scope of the law, teleservices shall not be subject to licensing or registration."[239] This section means that the BDSG's registration requirement will control. To the extent that on-line services "store personal data as business,"[240] they will be required to register with the Supervisory Authority.

As for monitoring, the IuKDG also takes a traditional approach by granting power to the states' Supervisory Authority. The IuKDG gives the Supervisory Authorities monitoring power through a cross-reference to BDSG, § 38, which is the section that sets out this institution's power. The IuKDG extends this power; it does so by stating, "an examination may be carried out [by the Supervisory Authority] even if there are not grounds to suppose that data protection provisions have been violated."[241] This statement makes clear the Supervisory Authority's ability to monitor private sector data protection exists irrespective of investigations based on a suspicion of violations.[242]

As for the Federal Data Protection Commissioner, the IuKDG also assigns oversight authority to this figure. The Federal Data Protection Commissioner is to "observe the development of data protection as applied to the provision and utilization of teleservices and ... make relevant activities in the activity report he has to submit" to the German *Bundestag*.[243]

The IuKDG does not require any registration requirement beyond that of the BDSG. This approach means that the IuKDG itself will have no impact on the

---

[238] Landesbeauftragter für den Datenschutz, 19. Jahresbericht 47 (1997) [hereinafter cited as Bremen Data Protection Commissioner, 19th Report].

[239] IuKDG, Article 1, § 4.

[240] See BDSG, § 32.

[241] IuKDG, Article 2, § 8(2).

[242] BDSG, § 38.

[243] IuKDG, Article 2, § 8(2).

registration obligations for data processing related to on-line services. The process of registration could be greatly simplified, however, were electronic on-line registration possible in Germany. This possibility does not yet seem to be under discussion.

As for monitoring, both the state Supervisory Authorities and the Federal Data Protection Commissioners will play important roles in this area. In addition, the IuKDG strengthens the ability of the state Supervisory Authorities by making clear its ability to visit the premises of on-line service providers and demand information from them.

Early drafts of the IuKDG also discussed the concept of a data protection audit (*Datenschutz-Audit*). A data protection audit would be carried out by independent experts hired by on-line service providers. It would support the role of the internal data protection official and make possible the use of a "data protection seal of approval" for on-line services that met the approved standards. Unfortunately, the IuKDG as enacted fails to contain provisions for the data protection audit.[244] Although the IuKDG does not set up rules for a data protection audit, such a process can still be carried out on a voluntary basis.[245] In contrast to the IuKDG's failure to enact provisions for a data protection audit, the Media Services Interstate Agreement contains an explicit statutory provision that permits data protection audits to be carried out.[246]

2.2.4. United Kingdom2.2.4. United Kingdom2.2.4. United Kingdom2.2.4. United Kingdom

---

[244] The Federal Data Protection Commissioner has objected to this absence of provisions for a data protection audit. In his most recent report of activities, Dr. Jacob notes,

> The lack of a 'seal of quality,' which the audit would have made possible, prevents or makes more difficult the orientation that is necessary for a wide acceptance and that will above all make possible the widescale entry into the information society. The Federal Republic of Germany is thereby renouncing an important future advantage for itself in global competition-- namely its advantage in data protection, which it has won through experience.

Federal Data Protection Commissioner, 16th Activity Report, 143.

[245] For a discussion, see StefanEngel-Flechsig, Die datenschutzrechtlichen Vorschriften in neuen Informations- und Kommunikationsdienste-Gesetz,Recht der Datenverarbeitung 59, 66-67 (Heft 2/1997).

[246] Media Services Interstate Agreement, § 17.

As this Study has noted above, the Data Protection Registrar has critical powers through the registration process.[247] The Data Protection Act requires registration of a data user who holds personal data unless all the data are exempt. A register entry must include a description of the personal data held and the purposes for which the data are held or used, the sources from whom the data user may obtain the information constituting the data, and the overseas country to which the data user may transfer the data.[248]

Over the past two years, considerable discussion has taken place regarding potential simplification of the registration process. In response, the registration process has been revised and streamlined. Registration is now possible on-line with the use of templated registration forms, based on the nature of businesses. In addition, access to the public register is now available on-line.[249] Approximately 500 applications to register are currently made each week.[250] Additional changes are also planned regarding registration. The Home Secretary and the Data Registrar both seek to replace the current registration model with a new "notification" scheme. The process for notification is intended to further simplify the required process and to minimize the details that the controller has to provide.[251]

The United Kingdom does not have a particular statutory provision enumerating specific registration/notification requirements for on-line services or for Internet activities. The Data Registrar has issued a paper, however, regarding

---

[247] Through the registration process, the Data Protection Registrar can serve an Enforcement Notice that directs a registered person to take specific steps to comply with the Data Privacy Law and in particular to the data protection principles. The Registrar can also issue a De-registration Notice that cancels from the Register the whole or part of any registration entry and a Transfer Prohibition Notice that prevents the transfer of personal data overseas. If the Registrar takes such enforcement action, the data user may appeal this action to the independent Data Protection Tribunal. See Data Protection Act 1984, Part II.4-20.

[248] See id at 6-9.

[249] http://www.open.gov.uk/dpr/register.htm

[250] Data Protection Registrar, Thirteenth Annual Report 5 (1997).

[251] Home Office, Data Protection: The Government's Proposals at 5.3; Paper 4, Data Protection Registrar, Questions to Answer: Data Protection and the EU Directive 33-46 (1996).

"Data Protection and the Internet" that examines registration issues.[252] In this document, the Registrar states her view that most businesses who are planning to use the Internet for activities currently carried out by other means are likely to be already registered. For these data users, use of the Internet will require review of the register entry and decisions as to the extent that circumstances of data use may have changed.[253]

One important area in which the Internet changes the circumstances of publication is when biographical details of an organization's staff are published on the World Wide Web. As the Registrar states:

> There are some cases ... where the use of the Internet as the medium, for example, to publish information greatly increases the potential for access to the information.... Such information may have been made available to enquirers anyway, but publication over the Web is quite different to publication by more traditional means.[254]

The Registrar recommends that in such cases where extensive use is made of the Internet, the data user describe the use of the Internet in the registration in free text.

In instances where the Internet is utilized to provide access to personal data, further international transfer of the data is easily possible. The Data Protection Registrar recommends that if a possibility exists that access to personal data "might be available widely over the Internet," the "worldwide" box on the registration form should be checked with a free text description. The Registrar suggests use of the following text, "Personal data held for this purpose may be transmitted over the Internet. Transfers of personal data may therefore take place, potentially to any country in the world."[255]

The Registrar appears to be taking a cautious approach as to whether or

---

[252] Data Protection and the Internet: Guidance on Registration, <http://www.open.gov.uk/dpr/internet.htm>.

[253] Id.

[254] Id at 2.

[255] Id.

not foreign website must register in the United Kingdom if they collect personal data in the United Kingdom. The Registrar has noted:

> [M]erely accessing personal data on the Internet by a person who does not control the contents and use of the data does not create a liability for registration. However, downloading and retaining a copy of the data for further processing implies control over the contents and use of the copy, and, unless the data are exempt, is likely to require registration.[256]

This statement may indicate that a foreign business will be subject to the registration requirement if it controls this information. This statement may be intended, however, only to refer to domestic data users.

The Home Office has recently offered a comment regarding the geographical extent of any new Data Protection Law.[257] In its proposal, a new British data protection law is to apply to processing: (1) by a controller established only in the United Kingdom; (2) for the purposes of the United Kingdom branch of a controller established in more than one more European Union country; (3) by a controller established outside the United Kingdom but in a place where United Kingdom law applies; (4) by a controller not established in the European Union but who uses equipment in the United Kingdom. In the fourth case, the organization in question is to be obligated to designate a representative as controller in the United Kingdom.[258]

This proposal raises significant questions in the context of on-line services, but the Home Office's proposal does not explicitly define the activities that will constitute the "use of equipment in the UK." This language itself follows that found in the European Directive.[259] Two further sources can be examined

---

[256] Id. at 4.

[257] Data Protection: The Government's Proposals, 2.23. <http://www.homeoffice.gov.uk.datap4.htm>.

[258] Id.

[259] See Directive 95/46/EC of the European Parliament and of the Council, article 4(1)(c) ("Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through

regarding the issue on registration in the on-line world. The UK Data Protection Act states that it "does not apply to a data user in respect of data held... outside the United Kingdom."[260] Here, the critical concept is that data must be treated as "held" where the data user exercises control over them.[261] The Data Protection Act further refers to "control over data" as control "over the contents and use of the data comprised in the collection."[262] Due to the international nature of the Internet, on-line processing activity in the Australia, Hong Kong or the United States may also involve computers in the United Kingdom itself. It may be that the "control" over the contents of the data will be exercised *outside* of the United Kingdom. If so, foreign websites will not be required to register in the United Kingdom or be subject to British data protection law.

The Consultation Paper on the Data Protection Directive offers some final light on the issue of registration.[263] This paper states that when data is processed outside of the Community, the national law to apply is "the law of the Member State in which the equipment used for processing (eg a computer) is situated."[264] The paper then offers the following example, "[A] controller based in, for example, the United States, who carried out processing operations using equipment in the United Kingdom, France and Germany would be subject to the national law of each of those Member States in respect of the particular processing operations carried out using the equipment in the Member State in question."[265] Here, too, the question of the geographic extent of British law turns on the nature of "using equipment" in the United Kingdom. An Internet operation with its server in the United States can easily access personal data of an individual located in the United Kingdom-- such activity will require "use" of equipment inside and outside the United Kingdom.

---

the territory of the Community.").

[260] Data Protection Act 1985, § 39.

[261] Id at § 39(2)(a).

[262] Id at § 1(2)(b).

[263] Consultation Paper on the EC Data Protection Directive, at 2.22. <http://elj.warwick.ac.uk/jilt/Consult/ukdp/dataprot.htm>.

[264] Id. at 2.25.

[265] Id. at 2.25.

Finally, as a general observation about registration in the United Kingdom, there appear to be a number of difficulties with compliance. As already noted, the Data Protection Registrar hopes to improve the number of registrations through on-line registration and streamlining of requirements. Moreover, statistics indicate that registrations are on the increase and that knowledge of the Data Protection Act is at an all time high.[266] Nevertheless, it is likely that the number of current registrations cannot begin to approach all those within the United Kingdom who process personal data.[267] This observation can probably also fairly be made regarding other countries with a registration requirement.[268]

As more data processing takes place on-line, the number of businesses and individuals subject to a registration requirement is likely to increase greatly. As the Registrar has noted of computing, "It is all pervasive, almost universal and employed not just by very large organizations in a highly structured manner, but by businesses of all sizes and millions of individuals."[269] Despite the Registrar's ongoing efforts to simplify registration requirements and to increase awareness of the Data Protection Act, it is not clear that a high level of compliance will exist in the on-line environment. For example, two of the United Kingdom's leading on-line newspapers, the Times and the Electronic Telegraph, collect personal information from their on-line readers as part of a registration process that is a condition to reading the web version of their periodicals.[270] Yet, as of December 5, 1997, neither newspaper had registered with the Data Protection Registrar.

2.3 Transparency2.3 Transparency2.3 Transparency2.3 Transparency

As noted above, transparency is one of the core principles of European

---

[266] Data Protection Registrar, 13th Activity Report at 29-34.

[267] In 1996-97, there were 200,864 registered data users in the UK. 13th Annual Report at 21.

[268] See, e.g., Landesbeauftragter für den Datenschutz, Freie Hansestadt Bremen, 19.Jahresbericht (1997) (122 registrations for the state of Bremen).

[269] Questions to Answer, at 4.

[270] <http://www.the-times.co.uk/;http://www.telegraph.co.uk.>

data protection law.[271] This standard requires that the processing of personal information be structured in a fashion that is open and understandable for the individual. Moreover, transparency requires that individuals have rights of access and correction to stored person information.[272]

In the context of on-line services and the Internet, this data protection standard is subject to great stress. In current practice, on-line service participants do not generally offer information about how they handle personal data. While many service providers are beginning to offer notice to their subscribers,[273] many web sites collecting personal information do not. Yet, such transparency is technically capable of being provided. Thus, as the first part of this Study has noted, one world wide web site even permits individuals to test in real time the information that a server can collect about him.[274]

Similarly, access and correction rights do not generally appear to be offered by on-line service participants. Like transparency, these rights are technically feasible in the on-line environment.

2.3.1 Belgium2.3.1 Belgium2.3.1 Belgium2.3.1 Belgium

The Belgian law requires notice to individuals at the time of collection of personal information if such information is being collected directly from the individual.[275] The notice must inform the individual of the identity of the person responsible for the processing, the finality of the data being collected, the possibility to find additional information from the declaration to the CPVP, and the individual's right to access and correct the stored personal information.[276] If information is only collected indirectly, then the individuals must be notified

---

271 See supra _ 1.2.2.

272 Id.

273 See, e.g., Part I, __ I.4.3, I.5.2 ; Part II, case studies.

274 See, e.g., <http://www.anonymiser.com>.

275 Loi du 8 décembre 1992, art. 4(1).

276 Loi du 8 décembre 1992, art. 4.

contemporaneously with the storage of the information.[277] Nevertheless, separate contemporaneous notice for indirect collections of personal information is not required if a contractual relationship exists between the individual and the person processing the information.[278] Notice is also not required when:

- notice has previously been provided and the purposes have not been modified since the delivery of the notice;
- the treatment of the information relates exclusively to the identification of individuals for the purpose of public relations, social or professional relations provided, however, that the person concerned directly communicated the information;
- the information is uniquely incorporated as secondary information incidental to processing of information about another person and provided such incidental information is not processed independently and not used for any other purpose;
- the processing consists of information made public by the person concerned and the exclusive purpose of processing is the pursuit of the purpose for which the person concerned made the information public;
- the processing involves information made public by law or regulation and the processing conforms to the purpose of the publication.[279]

When notice is required, Belgian law appears to require reasonably specific information about the nature of the processing and, in particular, to require finality. For example, a court found that a bank informing its clients that the bank «guarantees that personal information will be used exclusively for legal purposes, namely the preparation and execution of contracts in the framework of providing financial services and optimizing the relationship between the bank and the client» is not sufficient as a notice for use of the information in connection with insurance

---

277 Loi du 8 décembre 1992, art. 9.

278 Loi du 8 décembre 1992, art. 9.

279 Arrêté royal (no. 15) du 15 mars1996 modifiant l'arrête royal no. 9 du 7 février 1995, M.B., 15 mars 1996, p. 5830.

solicitations.[280] The Belgian court viewed the notice as fairly referring only to pure banking services such as means of payment, account address, savings plans, investments, loans and the like. The court also justified its finding by noting that the insurance activities were a recent addition to the bank's services.[281] This approach reflects a strict interpretation of finality and is significant for the consequences of notice statements made by online service participants to their clients. Since on-line services are inherently dynamic, the adaptation of information uses is likely to fall outside the scope of finality originally notified to individuals. Consequently, on-line services may frequently be required to update their notices to individuals.

The transparency principle in Belgium also includes a right of access to personal information held by the controller[282] as well as a right of correction of inaccurate data.[283] The controller may require that an individual pay a fee of 100BF (2.5 ECU) to cover the administrative expenses of responding to the access request,[284] though in the case of an access demand for consumer credit information, the consultion must typically be free of charge.[285] Yet, these rights may be complicated for an individual to exercise in the context of on-line services. For any particular transaction, the organization qualifying as a «controller» may shift in accordance to the flows of clickstream data. Hence, an individual may have to approach several «controllers» to obtain a clear picture of the information circulating about him.

---

280 Trib. Comm. Anvers, 7 juillet 1994, *reprinted in* 1994/4 D.I.T., pp. 52-53.

281 Id.

282 Loi du 8 décembre 1992, art. 10.

283 Loi du 8 décembre 1992, art. 12.

284 Arrêté Royal No. 4 du 7 septembre fixant le montant, les conditions et les modalités du paiement de la redevance préalable au maître du fichier lors de l'exercice du droit de communication des données à caractère personnel fondé sur l'article 10 de la loi du 8 décembre 1992.

285 See Y. Poullet & A. Lefebvre, Vie privé et crédit à la consommation, protéger le consommateur ou sa vie privée: un choix difficile, in LE CRÉDIT À LA CONSOMMATION, p. 121 (G.-A. Dahl, ed., 1997)(citing Article 70(2) of the Law on Consumer Credit and Article 10 of the Royal Decree of November 20, 1992.)

2.3.2. France2.3.2. France2.3.2. France2.3.2. France

French law requires that individuals receive notice of automatic processing of nominative information.[286] This obligation attaches only to those collecting information directly from individuals.[287] This limitation on the obligation to provide notice is significant in the network environment; many providers of on-line services may not collect personal information directly from the individuals concerned. When notice is required, it must inform the individual: (a) whether the information must be given or is voluntary, (b) what consequences will follow in the absence of a response, (c) who will receive the information, and (d) that the individual has a right of access and correction to the information.[288] Individuals have the right to oppose processing of nominative data for legitimate reasons (other than processing performed in conformance with a regulatory mandate.)[289] In the case of sensitive data, individuals must consent explicitly in writing to the processing of such information.[290] Individuals also have a right of access to any nominative information held pursuant to a declaration[291] and have a right to require the correction of any erroneous, incomplete, equivocal, stale or improperly used information.[292]

The CNIL has been extremely vigilant in assuring notice and consent for the treatment of personal information and, in particular, for on-line services. At the tenth year anniversary of the French law, a CNIL study reported that the agency gives a broad interpretation to the meaning of 'collection of personal information,' including situations where information is generated automatically in

---

[286] Loi No. 78-17 du 6 janvier 1978, art. 27.

[287] See, e.g., CNIL, Dix ans d'informatique et libertés, p. 16 (1988)

[288] Loi No. 78-17 du 6 janvier 1978, art. 27.

[289] Loi No. 78-17 du 6 janvier 1978, art. 26.

[290] Loi No. 78-17 du 6 janvier 1978, art. 31. While the law does not mention any formalities for the consent, the CNIL, as confirmed by the Conseil d'Etat, understands this provision to require a written consent. CNIL, Dix ans d'informatique et libertés, p. 23.

[291] Id., art. 34.

[292] Id., art. 36.

the course of business.[293] The purpose for this broad interpretation is to avoid circumvention of the individual's right to know about the processing of personal information. More recently, the CNIL has focussed on the notice given to individuals in the context of directory information on the Internet[294] and has carefully scrutinized the processing of medical information on the Internet to assure that patients receive an explicit consent form at the time of data collection.[295]

In terms of the content for an adequate notice, the CNIL has insisted in its Internet decisions that the notice must include the «logic of processing»[296] and must inform users of the purpose for the information and that Internet transmissions are less secure that other forms.[297] In addition, the CNIL's strong position on directory information is that the individual must be informed specifically that such information will be placed on the Internet and must be told of the special risks associated with the accessibility of personal data on the Internet.[298]

With respect to «opposition» which is the right of individuals to object to

---

[293] CNIL, Dix ans d'informatique et des libertés, pp. 17-18.

[294] CNIL, 16e Rapport d'activité, pp. 84-86 (1996); CNIL, 17e Rapport d'activité, 69-83 (1997).

[295] Délibération No. 96-062 du 9 juillet 1996; Délibération No. 96-063 du 9 juillet 1996; CNIL, 17e Rapport d'activité, pp. 83-87 (1997).

[296] CNIL, Voix, image et protection des données personelles, 55 (1996). While the CNIL does not elaborate on the meaning of «logic of processing,» the term refers to the type of analysis performed to make inferences about individuals.

[297] See, e.g., Délibération No. 97-051 du 30 juin 1997 concernant une demande d'avis présenté par la Mairie de Paris relative à un traitement d'informations nominatives mis en oeuvre dans le cadre du site Internet de la Ville de Paris; Délibération No. 97-032 du 6 mai 1997 relative à la demande d'avis présenté par le premier ministre concernant un modèle-type de traitements d'informations nominative opérés dans le cadre d'un site Internet ministériel.

[298] The CNIL approved, for example, a model for the treatment of personal information by Internet sites operated by government ministries and emphasized the terms of notice to be provided. See Délibération No. 97-032 du 6 mai 1997 relative à la demande d'avis présenté par le premier ministre concernant un modèle-type de traitements d'informations nominative opérés dan le cadre d'un site Internet ministériel.

processing, the CNIL distinguishes the distribution of personal information on the Internet from other disseminations.[299] Consequently, the CNIL has sought to assure that distribution by one channel such as a telephone book does not preclude opposition to Internet dissemination.[300] The notices generally must indicate that individuals have a right of opposition to the treatment of personal information.

Because the obligation to provide notice is restricted to collections of personal information directly from the concerned individuals, many providers of on-line services may escape the requirement and not be required to give notice to individuals. Personal information may also be collected indirectly from individuals on the Internet, such as is the case of data for log files acquired by a host site from the individual's Internet service provider. In these situations, the Internet service provider would have the obligation to notify individuals of the transfer of nominative information to third parties, but the recipient would not. The CNIL has also suggested that Internet service providers should bear responsibility for notification of the information practices of intelligent agents where those agents make use of profiles of nominative information.[301] Nevertheless, in cases of a recipient's indirect acquisition of personal information, if the recipient then collected information directly from the individual, such as through the use of «cookies» or a questionnaire at the site, notice complying with the legal standards would be required. Yet, the mere fact of a «cookies» alert appearing on screen through an Internet browser or the implicit awareness of data collection when a user completes a questionnaire would be unlikely to satisfy the content standards for notice; these mechanisms do not, for example, usually indicate the compulsory nature of responses, the logic of processing, the finality, or the heighten risks from an open network environment.

The transposition of the European Directive will necessitate an increase in the French notice requirements because the European Directive requires notification for indirect collections of personal information.[302] In the on-line

---

299 CNIL, 17e Rapport d'activité, pp.72-73 (1997).

300 Id.

301 CNIL, Voix, image et protection des données, p. 56-57 (1996).

302 See Directive 95/46/EC, art. 11; CNIL, Voix, Image et Protection des données personnelles, p. 54 (1996).

world, technical means can readily be developed to achieve these notifications. For example, just as a small icon appears on some browsers to indicate the use of encryption protocols,[303] a small icon could appear to indicate the transfer of personal information. The CNIL has taken tentative steps in this direction by noting, for example, that a screen with a notice of opposition rights along with a clickable link to register opposition was an appropriate mechanism to provide notice of collection of personal information and the required opt-out.[304]

Finally, French law will have to include a broader range of exclusions from the notice requirement than exist presently in order to comply with the European Directive.[305] The European Directive provides a variety of derogations not found in French law (e.g. national security, defense, public security, breaches of ethics for regulated professions, an important economic or financial interest of a member state or of the European Union).[306] These derogations are likely to prove significant for on-line services due to omnipresent security issues that will be endemic in an open network environment.

2.3.3 Germany2.3.3 Germany2.3.3 Germany2.3.3 Germany

The IuKDG builds on the existing BDSG provisions regarding for transparency and, in particular, notice.[307] The IuKDG emphasizes the importance of notice at several places. In its Article 2, § 3(5), it states, "The user shall be informed about the type, scope, place and purposes of collection, processing and

---

[303] Netscape Navigator uses a small key in the bottom left corner of the user's screen to indicate the current use of secure transmission capabilities.

[304] Délibération No. 97-050 du 24 juin 1997 relative à une demande d'avis présenté par France Télcom concernant un traitement automatisé d'informations nominatives dénommé «Minitelnet.»

[305] French law only provides an exception for the collection of information necessary to establish a violation. Loi No. 78-17 du 6 janvier 1978, art. 27 alinéa 2.

[306] Directive 95/46/EC, art. 13(1).

[307] See BDSG, § 19: "The data subject shall, upon request, be provided with information on 1. stored personal data concerning him, including their origin and recipients, and 2. the purpose of storage."

use of his personal data." This fundamental rule about notice is strengthened by specific rules about automated procedures, such as cookies, under which personal data are collected.

The IuKDG's rules about cookies requires both notice and a chance to waive notice. The Law states, "In case of automated processing, which permits subsequent identification of the user and which prepares the collection, processing or use of personal data, the user shall be informed prior to the beginning of the procedure."[308] This obligation is placed on "providers" who are defined as "natural or legal persons or associations of persons who make available teleservices or who provide access to the use of teleservices."[309] The obligation extends, however, only to circumstances when cookies permit "subsequent identification of the user."[310] The IuKDG also indicates that the responsibility for notification about cookies will belong to the party who places the cookie, whether Internet Service Provider (ISP) or web site. The web site falls into the category of those "who make available teleservices"; the ISP, those "who provide access to the use of teleservices."[311]

Information about this "automated processing" is to be accessible to the user at any time.[312] Moreover, the "user may waive such information."[313] This waiver of receiving information about automated processing, such as cookies, is not, however, considered to be consent for purposes of permitting the performance of teleservices or for further use of data collected for performing teleservices.[314]

The IuKDG also requires providers to inform users "of any reforwarding to another provider."[315] As this Study has pointed out above, the IuKDG also

---

[308] IuKDG, Article 2, §3(6).

[309] IuKDG, Article 2, § 2(1).

[310] Id.

[311] IuKDG, Article 1, § 3.

[312] IuKDG, Article 2, § 3(5).

[313] Id.

[314] Id.

[315] IuKDG, § 4(3).

requires the user to be informed about the option of "anonymous use and payment of teleservices or use and payment under a pseudonym."[316] In addition, the user is to be told of any information that is stored under his pseudonym.[317] The IuKDG requires that a user have access, free of charge, to "stored data concerning his person or his pseudonym."[318]

As for consent, the IuKDG places this at the center of its principles for data protection and carefully polices the conditions under which consent is to be granted. The Law also provides for consent to be provided in an electronic fashion. The IuKDG's consent provisions point to a way to bring data protection into the next century. Permitting the electronic gathering of consent lowers the cost of obtaining agreement for on-line service providers. At the same time, the IuKDG establishes strict limits on the conditions under which consent may be obtained. These limits seek to insure that consent is both: (1) truly informed, and (2) truly voluntary.

Under the IuKDG, data may only be collected and processed if the law permits such action or if the user has given his permission.[319] In addition, the IuKDG requires individual consent to be sought for certain kinds of additional processing of "contractual data," which are those data required for concluding a contract on the use of teleservices.[320] The IuKDG states, "Processing and use of contractual data for the purpose of advising, advertising, market research or for the demand-oriented design of the teleservices is only permissible if the user has given his explicit consent."[321] This provision places strict limits on further use of basic information which service providers must collect about each of their customers.

Consent as a principle of data protection can easily be abused. Past

---

[316] IuKDG, Article 2, § 4.

[317] IuKDG, Article 2, § 7.

[318] IuKDG, Article 2, § 7. The BDSG's general rule is also that "[i]nformation shall be disclosed free of charge." BDSG, § 34.

[319] IuKDG, Article 2, § 3(1).

[320] IuKDG, Article 2, § 5(2).

[321] Id.

reliance on consent to data processing in the United States, for example, has shown that two particular difficulties can arise.[322] First, data subjects may have *no real alternative* except to consent when their permission is sought before data processing. Second, data subjects may be unable to make *an informed choice* due to inadequate information about planned processing. The IuKDG attempts to prevent these two kinds of abuse of its consent provisions.

As to the lack of a real choice, the IuKDG requires that access to on-line services be provided irregardless of permission being granted to further processing of personal data. The statute states, "The provider shall not make the rendering of teleservices conditional upon the consent of the user to the effect that his data may be processed or used for other purposes if other access to these teleservices is not or not reasonably provided to the user."[323] In addition, the user is to be informed "about his right to withdraw his consent at any time with effect for the future."[324] This statutory language guarantees reasonable access to teleservices even if a user does not consent to additional use of his personal data.

As for the danger of uninformed consent, the IuKDG requires specific kinds of information to be shared with the data subject as part of the consent process. The Law states, "The user shall be informed about the type, scope, place and purposes of collection, processing and use of his personal data."[325] These detailed provisions safeguard the consent process by requiring that users receive the kinds of information that are likely to be necessary for well-informed decisionmaking by teleservices consumers.

In another advance for data protection law, the IuKDG explicitly permits consent to be declared electronically. In Article 2, § 3(7), the Law provides that consent can be declared electronically if certain conditions are met. According to the IuKDG's legislative history, this statute develops these procedural protection because of the special risks of electronic consents. These risks are due to the lack of both "embodiment (no writing form)" and "biometrical marks (no signature in

---

[322] These problems are particularly acute in the context of the processing of health care information. See Paul M. Schwartz & Joel R. Reidenberg, DATA PRIVACY LAW, 167-71 (1996).

[323] IuKDG, Article 2, § 3(3).

[324] IuKDG, Article 2, § 3(6).

[325] IuKDG, Article 2, § 3(3).

one's own hand)."[326]

Consent therefore is valid under the IuKDG only if the provider ensures that electronic consent is given through a process that is tailored to the digital world. As the Law states:

> Consent can also be declared electronically if the provider ensures that
>
> 1. such consent can be given only through an unambiguous and deliberate act by the user,
> 2. consent cannot be modified without detection,
> 3. the creator can be identified
> 4. the consent is recorded and
> 5. the text of the consent can be obtained by the user on request at any time.[327]

One of the most important of these requirements for electronic consent is that the consent only be made "through an unambiguous and deliberate act by the user." Here, the legislative history states, "In this sense, a consent is authorized, for example, through a confirmed repetition of the command to transfer that is simultaneously accompanied on the viewing screen by a declaration of consent at least in extracts."[328] As to the requirement that consent cannot be modified without detection, the federal government stated, in introducing the draft IuKDG, that "suitable technical processes" must be made available to prove the authenticity and authorship of the consent.[329]

German law protects not only consent, but also rights of access and correction. The IuKDG provides the user the right "at any time to inspect, free of charge, stored data concerning his person or his pseudonym at the provider's."[330]

---

[326] Deutscher Bundestag, 13. Wahlperiode, Gesetzentwurf der Bundesregierung, Drucksache 13/7385, Seite 23 (09. April 1997).

[327] IuKDG, Article 2, § 3(7).

[328] Gesetzentwurf der Bundesregierung, Drucksache 13/7385, Seite 23.

[329] Id.

[330] IuKDG, Article 2, §7.

It also states, "The information shall be given electronically if so requested by the user."[331]

The IuKDG itself does not provide rights to correct personal data. In this gap, the Federal Data Protection Law's requirements will control. The BDSG provides, "Personal data shall be corrected if they are inaccurate."[332]

These rights of access and correction are of enormous importance in the on-line world. Data subjects will be able to find out the information that providers have stored on them. They will also be able to correct this information when incorrect.

Finally, some comments about current practices in Germany are possible. The IuKDG's rights regarding transparency are impressive. Actual practices may not yet be responding, however, to these legal requirements. Examination of web sites that fall under the Law's definition of "teleservices" finds some noteworthy failures to follow the statutory requirements that this section has discussed.

A few examples will suffice. Within the IuKDG's definition of "teleservices" are "goods and services offered and listed in electronically accessible data bases with interactive access and the possibility for direct order."[333] Thus, web sites that offer products for sale clearly fall under the statute's requirements for transparency. Nevertheless, a survey of German web sites reveals that the IuKDG's requirements are not yet uniformly followed. This phenomena can be at least partially explained by the statute's entering into force only a few months ago.

As an initial example, *Der Spiegel*, a leading German magazine, offers a popular web site that contains news articles and offers extensive goods and services for sale.[334] This site sells audio CDs, CD-Roms, videos, books as well as tickets for events and shows taking place all over Germany. These products can all be ordered on-line at the *Spiegel* website. Yet, the *Der Spiegel* website furnishes no indication of the planned use of personal data that are collected as part of its selling of goods. Another web site that offers goods and services for sale is that of the Kaufhof, a leading German department store.[335] Here too, the

---

[331] Id.

[332] BDSG, § 35(1).

[333] IuKDG, Article 1, § 2(5).

[334] <http://www.spiegel.de/shop/right.html>

web site provides no information about its fair information practices (if any).

As a final example, KaDeWe, the upscale Berlin department store, offers its products for sale on line through the "my-world" web site.[336] This site does provide on-line information about its security practices. Specifically, the my-world web site uses SSL, the Secure Socket Layer, which is a encryption process.[337] The "my-world" site uses SSL to "offer you the security that your personal data-- such as your address or your credit card number-- will not fall into the wrong hands."[338] Nevertheless, this web site does *not* supply information about any other fair information practices.

2.3.4 United Kingdom2.3.4 United Kingdom2.3.4 United Kingdom2.3.4 United Kingdom

As one of its core data protection principles, British law requires that an individual is entitled "at reasonable intervals and without undue delay or expense ... to be informed by any data user whether he holds personal data of which that individual is the subject."[339] Notice also forms part of the "fairness" principle of data protection. In determining whether or not personal information has been obtained fairly, one factor, according to the Act, is "whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed."[340] The right of notification has been further developed by decisions of the Data Protection Tribunal. In particular, three decisions of this body are worthy of note.

First, in the *Linguaphone* decision of 1996,[341] the Data Protection Tribunal

---

[335] <http://www.kaufhof.de/hilfe.html>. Among the many products for sale on its web site are official souvenirs for the Federal Garden Show, including wooden animals and wooden flowers that one can exhibit in one's own garden. < http://www.kkaufhof.de/cgi/ktest/html/online/bundesgarten>.

[336] <http://www.my-world.de>

[337] <http://www.my-world.de/bestellen/tips/SSL.html>

[338] Id.

[339] Data Protection Act of 1984, at Schedule 1, Part I.1(7)(a).

[340] Id. at Part II.1.

[341] The decision is set out at Data Protection Registrar, The Twelfth Annual Report 82 (1996).

criticized one data user's notification to individuals as insufficient. This notification was not of a proper size and prominence to provide effective information to the individual.[342] Second, in a judgment regarding the use by utility companies of personal information in their supply data bases for non-supply purposes, the Data Protection Tribunal found that "individuals should be informed of any non-obvious purpose for which their data may be used or disclosed at the time that they enter into a relationship with a data user."[343] Thus, notice, if it is to promote fairness in data use, must be provided when the data collection relationship first begins.

As a final example, the Data Protection Tribunal in *Innovations (Mail Order) Ltd v. The Data Protection Registrar,* stressed the importance of notice being given at the correct time.[344] In some cases, Innovations had informed its customers of its rental of mailing lists only when it acknowledged receipt of their orders. The Registrar objected to this timing of notice, and the Tribunal stated, "We have reached a conclusion that the words 'fairly obtained' in the First Data Protection Principle direct attention to the time of obtaining not to a later time."[345] Timing of notification is thus a key element to providing adequate notice in British data protection law.

These decisions emphasize that notice must be of proper size and prominence, and that it must be provided when data is first provided to the data user. Application of this approach in the on-line world will require certain behavior of both Internet Service Providers and web sites. Following the Tribunal's interpretation of notification in these decisions, Internet Service Providers would be required to provide adequate notification of planned data use at the time that a contract is initially concluded with the individual. As for web sites that collect and process personal information, they would have to supply prominent notification when they collect personal information from the person who is visiting their site. Finally, this notice must be sufficiently detailed because of the flexibility of processing and open access afforded to data on the Internet.

---

[342] See Data Protection Registrar, The Twelfth Annual Report 82 (1996).

[343] 13th Annual Report, pg 27.

[344] For a discussion, see Data Protection Registrar, Data Protection Guidance for Direct Marketers 21 (1995).

[345] Id.

In the United Kingdom, consent is viewed as an essential element of the "fairness" principle. The Data Protection Act of 1984 provides that personal information must be obtained and processed "fairly and lawfully."[346] In the United Kingdom, formal consent is usually not required of individuals. Rather, information is to be provided to the individual, who, in his affirmative choice to use the services of the data user will be presumed to have consented to the planned data processing. This general rule regarding consent is subject to some limitations. First, in cases where individuals have no realistic choice other than to give their information to a particular data user, the Registrar has argued that "the data user should provide the individual with the opportunity to opt out of additional uses or disclosures of information which go beyond the primary purposes for which the information was supplied."[347] One example where no real choice exists is when a monopoly suppler provides an essential service.[348] The Data Protection Registrar has also extended this analysis to quasi-monopoly suppliers and those with "a very dominant market position."[349] In these cases, the companies in question were public utilities,[350] but the analysis can be extended to telecommunication companies. The Registrar has argued that individual customers should be viewed as having restricted the use of their personal data to supply and billing purposes in the absence of a positive consent for any additional purposes.[351]

Second, consent should be sought in some instances for third party marketing. One of the most important of these circumstances is when "data users have chosen not to inform the sources of their information of their intention to use personal data for host mailing or list rental when first obtaining a data subject's details, even though that was their intention."[352] A mere letter to customers

---

[346] Data Protection Act 1984, Schedule 1, Part I.1.

[347] Data Protection Registrar, Data Protection Guidance for Direct Marketers § 63, 22 (1995).

[348] Data Protection Registrar, Thirteenth Annual Report, 27 (1997).

[349] Id.

[350] Id. at 26.

[351] Id.

[352] Id. at § 65, 22-23.

informing them of list rental practices is *not* enough to assume that consent has been obtained from all those who have not objected.[353] This approach to consent creates an opt-in requirement when data users choose not to inform the individual of their plan to engage in mailing with the personal information that they gather.

Finally, the Data Protection Registrar has taken the position that the nature of the consent, express or implied, depends on a contextual analysis. Consent relates to the notion of "fair obtaining" of information, after all, and "[w]hat is fair in a particular case can only be determined in the light of industry practices and consumer expectations."[354] As these practices and expectations change, the standard for compliance with the Data Protection Act's fair obtaining requirement will continue to evolve.

In addition to this established approach to consent, the UK Data Protection Registrar has made specific comments regarding the on-line world. The Registrar has spoken to the need for users of the Information Superhighway "to control the use of their personal data and have real choice."[355] In particular, the Registrar has pointed to privacy enhancing technologies as a promising way to respond in this area.

One important proposal of the UK Data Protection Registrar regarding consent in the on-line world concerns "suppression markers in Internet addresses."[356] Through use of this device, individuals could indicate their objection "to have data about them collected or to receive unsolicited, promotional e-mails as a result of visiting particular sites or taking part in particular groups."[357] A suppression marker would allow individuals to block contact with those who might use the Internet to collect data or send them unsolicited junk mail (spamming).

The idea of an email suppression marker builds on existing British privacy law. In the United Kingdom, privacy preference services exist for postal direct

---

[353] Id at 23.

[354] Id. at § 63, at 22.

[355] 13th Annual Report, at page 53.

[356] Privacy Enhancing Technologies, Suppression Markers in Internet Addresses, Appendix 14 in UK Data Protection Registrar, Thirteenth Annual Report (1997).

[357] Id.

marketing and for telephone direct marketing.[358] These services allow consumers to register their preference not to receive unsolicited direct marketing communications. In addition, a fax preference service is under development. An email suppression marker, as proposed by the Data Protection Registrar, would allow individuals to indicate and communicate their wishes directly via their email address. As the Registrar states regarding an individual's desire not to receive unsolicited email, "There seems to be no reason on the Internet to divorce that message from the address itself."[359]

One difficulty with this proposal is that it cannot work without an appropriate not-yet-existing infrastructure. Another shortcoming is that the expression of privacy preferences can itself raise privacy issues. For example, unless other informational safeguards are in place, marketers might use information in the privacy preference address to develop individual profiles. Yet, the Registrar's proposal by its own confession "deals only with suppression not with obtaining information in the first place."[360] Thus, a kind of meta-privacy preference might also be needed regarding the fair use of privacy markers in settings outside the Internet.

How then is United Kindom data protection law likely to respond to the issue of consent in an on-line environment? First, British law's contextual approach to consent is likely to emphasize the need for a positive consent requirement should no real choice as to the underlying service be available and where inadequate information has been provided to the individual at the time of collection. One example of such an area might be concerning the transmission of clickstream data. Thus, positive consent to data use might be required should a limited number of Internet Service Providers be available in a geographic area. Moreover, web sites that initially fail to provide adequate information about planned future data use might be required to seek affirmative consent for such

---

[358] Data Protection Guidance for Direct Marketers 23-24 (1995).

[359] A "privacy marker" might indicate these following privacy preferences: (1) no messages are to be sent to the individual, or (2) communication from the website visited would be accepted, but from no other parties. These markers would also allow "the freedom to make different choices about different contacts." Privacy Enhancing Technologies, Appendix 14, in UK Data Protection Registrar, Thirteenth Annual Report. For example, an individual might express a certain privacy preference for one site but use a different marker for a different site.

[360] Id.

secondary use as sharing information with third parties. Finally, British data protection law is likely to seek the use of privacy enhancing technologies that will permit consent to be indicated in a rapid, low cost fashion.

British data protection law contains no explicit provision concerning access and correction in the on-line context. Yet, the Data Protection Act of 1984 does allow an individual to access personal data held by a data user and "where appropriate, to have such data corrected or erased."[361] Under British data protection law, data subjects have a right to see any data concerning themselves, subject only to certain limited exceptions.[362] Access requests are, moreover, to be answered promptly by the data user.[363] British data protection law allows a fee up to £10 (15 ECU) to be charged for an exercise of subject access rights. In its paper regarding implementation of the European Directive, the Government has indicated that it does not intend to change this fee requirement.[364]

As yet, little guidance exists as to how these rights will be applied in the on-line world. The Data Protection Registrar has stressed, however, that a data user must make efforts to find personal data that it has stored in different systems to fulfill its obligation to satisfy the access right. The Registrar has observed:

> Difficulties may occasionally arise where the data in question are stored in different systems. For instance, a marketer who has become a data user in respect of mailing lists which have been rented in or leased, in addition to an existing customer data base, must ensure that both sets of data are searched.[365]

Websites that collect personal data and then share this information with affiliated

---

[361] Data Protection Act 1984, at Schedule 1, Part I.7.

[362] See Data Protection Act 1984, Part III.21: "[A]n individual shall be entitled - (a) to be informed by any data user whether the data held by him include personal data of which that individual is the data subject; and (b) to be supplied by any data user with a copy of the information constituting any such personal data held by him."

[363] Data Protection Registrar, Homeworking and Computer Information 24 (June 1997).

[364] www.homeoffice.gov.uk.datap5.htm.

[365] Data Protection Registrar, Data Protection Guidance for Direct Marketers, 37.

websites may have an obligation to provide access and correction rights beyond their own data system.

Another possible development regarding access/correction rights in the on-line world concerns the form in which access will be provided. The Government has stated that any new data protection law should take advantage of the flexibility provided by the Directive, which allows communication of information "in an intelligible form."[366] Specifically, the Government has pointed to the possible for "electronic communication and possibly other means."[367] The choice as to means should be left to the data subject, who "will still be able to request a hard copy of the information, which will have to be granted except in limited cases where this is unreasonable or involves disproportionate effort."[368]

This statement points to a data protection regime that will permit subject access to take place on-line. The British data protection law might encourage websites and Internet Service Providers to develop technical means that will allow data subjects on-line access to the information that is stored about them. This approach would allow low cost means of obtaining access to information about oneself. Such a development would be consistent with the Data Protection Registrar's interest in privacy enhancing technologies.[369] It is as yet unclear how the data user's right to charge for access will be interpreted in an age where such access can be provided at low cost-- indeed, without human interface.

British law contains no explicit provision concerning access/correction in an on-line environment. Yet, its existing data protection statute provides these rights. The meaning of these rights in an on-line environment is only beginning to be explored. One important issue to be resolved is the circumstances under which subject access fees will be charged.

2.4 Profiling and Sensitive Data2.4 Profiling and Sensitive Data2.4 Profiling and Sensitive Data2.4 Profiling and Sensitive Data

---

366 <http:// www.homeoffice.gov.uk.datap5.htm.>

367 Id.

368 Id.

369 See, e.g., Data Protection Registrar, 13th Annual Report, at 115-17.

On-line services often rely on profiling individuals for the development of customized services and for marketing activities. Profiling raises many issues associated with the finality of data use as required by the European Directive.[370] For example, search engines enable on-line directories, on-line public data bases and message board postings to be used for multiple purposes. The commonplace matching of one set of data generated from on-line transactions with other complementary information also raises an issue concerning finality. Furthermore, the recording and use of behavioral patterns implicates additional issues of consent, data storage, and purging that are also the subject of mandates in the European Directive.[371]

The manner in which Member States treat these issues will have a fundamental impact on the structure of on-line services. Similarly, the characterization of individuals according to their behavior implicates another fundamental tenet of data protection: the special consideration to be afforded to sensitive data. Data profiles may frequently approach the categories of sensitive data that are subject to processing prohibitions under the European Directive.[372] Although isolated pieces of personal information acquired during the course of on-line service activities may not be «sensitive data,» the context of such information, especially in light of profiling practices, may bring the personal information within the meaning of the definition of «sensitive data.» The responses of the Member States to on-line concerns for sensitive data will be highly instructive for the analysis of the substantive harmonization of the national laws.

2.4.1 Belgium2.4.1 Belgium2.4.1 Belgium2.4.1 Belgium

The bedrock of Belgian data protection law is the statutory provision that personal information may only be processed for a legitimate and specified purpose and can not be used in a manner incompatible with that purpose.[373] Belgium

---

370 Directive 95/46/EC, Art. 6(1)(b).

371 Directive 95/46/EC, Art. 6(1)(c), 7,

372 Directive 95/46/EC, Art. 8.

373 C. de Terwagne et Y. Poullet, *Les annuaires téléphoniques au carrefour des droits*, Journal des Tribunaux, 1er juin 1996, p. 425, 432.

interprets finality in a strict manner. For example, in a significant, but unreported court case, Mercedes lost a suit for a breach of finality by using motor vehicle registration information for a marketing purpose, namely to solicit Mercedes owners to have their cars serviced in Mercedes garages.[374] Mercedes had acquired the information from the Ministry of Communications and Infrastructure through F.E.B.I.A.C. (the trade association for car and motorcycle manufacturers.) The court noted that the law authorizing the release of state-held motor vehicle registrations prohibited the use of administrative documents for commercial purposes and given that the state could not delegate its public service mission to the private sector, Mercedes' claim that the communications to car owners promoted public safety was unavailing.[375] According to commentators on this case, the court found that the use of the state's motor vehicle registration information by an automobile manufacturer for commercial solicitation purposes was illegitimate.[376]

A sectoral law also affects the purposes for treatment of personal information associated with on-line payments. The consumer credit law would prohibit many profiling activities.[377] This sectoral law limits the treatment of personal information to the exclusive purpose of «evaluating the financial situation and the credit worthiness of the consumer.»[378] This finality restriction applies to all contracts for credit involving consumers;[379] credit information may only be used

---

374 Chambre actions cass. Bruxelles, 20 mars 1995. See also J.P. Buyle, L. Lanoye, Y. Poullet & V. Willems, *Chronique de la jurisprudence: L'informatique (1987-1994)*, Journal des tribunaux, 23 mars 1996, pp.235-236 (commenting on the trial court decision).

375 Chambre actions cass. Bruxelles, 20 mars 1995 (citing Loi du 11 avril 1994 relative à la publicité de l'administration, art. 10.)

376 Id.

377 An interesting issue arises as to which law controls, the later general data protection law or the earlier sectoral consumer credit law. Commentators have argued that general issues are governed by the Loi du 8 décembre 1992 and specific issues for the credit sector are covered by the the Loi du 12 juin 1991. See Y. Poullet & A. Lefebvre, *Vie privée et crédit à la consommation, protéger le consommateur ou sa vie privée: un choix difficile*, in LE CREDIT A LA CONSOMMATION, 103, 105 (G.-A. Dahl, ed., 1997)

378 Loi du 12 juin 1991 relative au crédit à la consommation, art. 69.

379 Id., at art. 2.

for the granting and management of credit.[380] The law further limits the type of information that may be processed in connection with credit transactions.[381] Similarly, under the general data protection law, payment transaction data may not be used for purposes other than executing payment. This has been confirmed by several court cases in which banks were found in violation of finality by using payment records to profile customers and solicit them for commercial purposes.[382]

To the extent that electronic commerce transactions involve consumer credit, this sectoral law imposes important finality rules, excluding profiling for non-payment purposes, on any collections of transaction data.

The scope of finality will be an important constraint on the treatment of personal information generated by on-line services. With a strict interpretation of finality, the complexity and fluidity of data processing for on-line activities will necessarily result in fragmented decisions for finality and in an attempt to impose narrow uses for personal information.

In any event, Belgian data protection law does permit secondary use with the individual's consent. For consent, the trend in Belgium is to require differentiated levels of assent. In some instances, consent may be required on an opt-in basis. For example, the publication of directories for public officials may only contain work addresses unless express consent is granted to include home information.[383] Similarly, the CPVP has required express consent to include an individual's name and address on an advertising list[384] and to profile the

---

[380] Id., at art. 69; see also, CPVP, Rapport d'activité 1992-1993, pp. 68-72.

[381] Id., at art. 69. For example, the Commission has objected to the treatment of information related to an individual's nationality. CPVP, Rapport d'activité 1992-1993, p. 77 (1997). The Royal Decree implementing data reporting to the Banque nationale de Belgique followed this opinion and excluded nationality as a permissible type of data for processing in connection with credit transactions. Arrêté royal du 20 novembre 1992 relatif au traitement des données à caractère personnel en matière de crédit à la consommation.

[382] Trib. comm. Bruxelles, 15 sept. 1994, reprinted in 1994/4 D.I.T., 45-50; Trb. Comm. Anvers, 7 juillet 1994, reprinted in 1994/4 D.I.T., 51-55. See also J.P. Buyle, L. Lanoye, Y. Poullet, & V. Willems, Chronique de jurisprudence: L'informatique (1987-1994), Journal des tribunaux, 23 mars 1996, p. 232.

[383] CPVP, Avis no. 23/94 du 13 juillet 1994; CPVP, Rapport d'activité 1994-1995, p. 27 (1997).

[384] Recommandation no. 1/95 du 18 juillet 1995; CPVP, Rapport d'activité 1994-

prescription practices of physicians.[385] In its consideration of the applicability of the data protection law to telephone directory information, the CPVP recommended that Belgacom, the national telephone company, implement several levels of opt-outs: (i) consent to all uses; (ii) objection to commercial uses of personal information («liste orange»); (iii) objection to any dissemination of personal information («liste rouge».)[386] The CPVP noted that Belgacom had to inform its subscribers of these possibilities and their rights under the data protection law.[387] Similarly, the courts have noted that a company may make internal use of personal information outside the scope of the original purpose for collection if the individuals have notice and the ability to opt-out.[388]

In the context of on-line services, consent can be readily obtained on an opt-in basis by technical means. The various technical protocols such as «cookies» alerts or the P3P labelling and filtering initiative at W3C[389] enable users to make affirmative choices. However, appropriate notice is still necessary for the consent to be meaningful.

Nevertheless, for the treatment of sensitive data, the Belgian law generally requires advance consent.[390] The Royal Decree implementing protections for sensitive data tries to track the European Directive. Under the Royal Decree, the processing of sensitive data treats consent as valid only if it shows that the agreement was «expressly voluntary, freely given, specific and informed.»[391] This

---

1995, pp. 29-30 (1997).

[385] Recommandation No. 01/96 du 23 septembre 1996 à propos de l'analyse de la consommation de médicaments en Belgique basée sur des informations issues des prescriptions médicales, pp. 6-7.

[386] Recommandation no. 02/93 du 7 septembre 1993; CPVP, Rapport d'activité 1994-1995, p. 28 (1997).

[387] Id.

[388] See, e.g., Trib. comm. Bruxelles, 15 sept. 1994, reprinted in 1994/4 D.I.T., 45-50; Trib. Comm. Anvers, 7 juillet 1994, reprinted in 1994/4 D.I.T., 51-55.

[389] See Joel R. Reidenberg, The Use of Technology to Assure Internet Privacy: Adapting Labels and Filters for Data Protection, Lex Electronica III:2, <www.lex-electronica.org> (November, 1997)(discussing the P3P and W3C initiatives). For a further discussion, see *infra* § 3.3

[390] Arrêté royal (No. 14) du 22 mai 1996, M.B., 30 mai 1996, p. 14515 (superceding Arrêté royal (no. 7) du 15 février 1995); CPVP, Rapport d'activité 1996, p.38 (1997).

[391] Arrêté royal (No. 14) du 22 mai 1996, art. 1(e), M.B., 30 mai 1996, p. 14515,

decree amended a prior rule for sensitive data that did not match the standards of the European Directive. However, in the new decree, an important degree of ambiguity exists with respect to the form of the consent. Court decisions prior to the change of the new Royal Decree required written consent.[392] The new Royal Decree, however, is silent as to the form. For on-line services, this ambiguity presents a clear obstacle to electronic consent to the collection and processing of sensitive information.

As an important corollary to finality for profiling practices, Belgium requires that those collecting personal information minimize the amount of data processed. Article 5 of the statute mandates that the information not be «excessive with respect to the finality» of processing.[393] The Belgian law also stipulates that only information relevant for the purposes of processing may be used.[394]

Finally, the CPVP is also quite concerned about the duration of storage of personal information. The Belgian law interdicts storage of non-relevant information and consequently prohibits storage beyond the duration required by finality.[395] In a recent advisory opinion, the CPVP criticized a draft Royal Decree for credit information because of an inadequate restriction on the duration of storage for positive credit information.[396] This attention to storage is likely to create a legal obligation for the rapid deletion of stored on-line services data.

2.4.2. France2.4.2. France2.4.2. France2.4.2. France

Under French law, the use of personal information is strictly limited to the purposes declared at the time of collection.[397] This finality obligation is considered

---

14532; See also Rapport au Roi, M.B., 30 mai 1996, p. 14515, 14520.

[392] Arrêté royal (No. 14) du 22 mai 1996, M.B., 30 mai 1996, p. 14515 (superceding Arrêté royal (no. 7) du 15 février 1995); CPVP, Rapport d'activité 1996, p.38 (1997).

[393] Loi du 8 décembre 1992, art. 5 (data «must be adequate, relevant and non-excessive with respect to the finality.»)

[394] Loi du 8 décembre 1992, art. 5 (data «mustbe adequate, relevant and non-excessive with respect to the finality.»)

[395] Loi du 8 décembre 1992, art. 16(1)(4). Article 17(3)(2) requires that the duration of storage be indicated on the declaration of processing.

[396] CPVP, Avis no. 10/97 du 9 avril 1997.

[397] Loi No. 78-17 du 6 janvier 1978, art. 19 (requiring the declaration of finality) &

«omnipresent in the text of the law.»[398] The principle derives particular strength from the criminal sanctions that may attach to secondary uses of personal information. The law further states that «the evaluation of human behavior cannot be based on the automatic processing of information resulting in the definition of a profile or of the personality of the person concerned.»[399] This provision, in effect, prohibits data profiling as the sole basis for decision-making.[400] Profiles may, however, be considered along with other factors to be evaluated by a live person in connection with decisions about individuals.[401]

In the context of on-line services, the profiling of transaction information may also lead to the creation of sensitive information. The law generally prohibits the computerized storage of any information that directly or indirectly reveals: racial origins, political opinions, philosophical opinions, religious beliefs, or union membership.[402] If the individual consents explicitly in a writing independent of the data collection, then the sensitive information may be processed.[403] This consent requirement imposes a significant constraint for on-line services because they will be obliged to obtain consent off-line in advance of any processing that results in the treatment of sensitive data.

Under the French law, individuals have a fundamental right to object to the

---

art. 44 (providing criminal sanctions for use of personal information that is inconsistent with the declared purpose).

398 CNIL, Dix ans d'informatique et de libertés, pp. 36-37 (1988).

399 Loi No. 78-17 du 6 janvier 1978, art. 2.

400 See CNIL, 14e Rapport d'activité, pp. 59-64 (1994); Délibération No. 93-032 du 6 avril 1993 relative au contrôle effectué le 2 octobre 1992 à la Caisse regionale de crédit agricole de Dordogne.

401 CNIL, Dix ans d'informatique et libertés, pp. 47-48 (1988).

402 Loi No. 78-17 du 6 janvier 1978, art. 30. Religious organizations along with philosophical, political or union groups are exempted from this interdiction to the extent of maintaining a membership list in computerized form. Id. In addition, for reasons of «public interest,» essentially state security, government decrees may exempt certain processing from this restriction, but only after approval by the CNIL.

403 See CNIL, Dix ans d'informatique etlibertés, pp. 44 (1988)(refering to Arrêt du Conseil d'État du 5 juin 1987); CNIL, 14e Rapport d'activité, pp. 40-42 (1994)(noting that express consent means written consent for the storage of the particular data that is considered sensitive.)

processing of personal information.[404] Individuals for «legitimate reasons» may require the suppression or purging of personal information held by others. However, the «public interest» may defeat the legitimacy of an individual's reasons.[405]

The duration of data storage is also subject to careful limits under French law. The law prohibits the storage of personal information any longer than necessary to accomplish the purposes for collection of the information.[406] The CNIL has historically been quite vigilant in its monitoring of the length of data storage.[407]

The Telecommunications Law of 1996[408] may also have an impact on the treatment of personal information for profiling purposes. According to the new law, telecommunications operators must respect the secrecy of correspondence.[409] This provision may mean that an Internet service provider such as Wanadoo, operated by France Telecom, will not be allowed to provide identifiable information on users' on-line activities to third parties. In addition, the provision may even forbid the use of transaction information for profiling purposes.

As the CNIL examines on-line services, it pays particular attention to the respect of the finality principle. For Internet discussion groups, the CNIL has indicated that finality precludes using information gleaned from the discussion group for purposes other than those proposed by the discussion group itself; the accessibility of the information does not mean that it can be used to «enrich databases intended for example to be used for commercial purposes.»[410] This suggests that the use of search engines external to the discussion group, such as

---

404 Loi No. 78-17 du 6 janvier 1978, art. 26.

405 CNIL, 17e Rapport d'activité, pp. 116-117 (1997).

406 Loi No. 78-17 du 6 janvier 1978, art. 28.

407 CNIL, Dix ans d'informatique et libertés, 31-32 (1988).

408 Loi No. 96-659 du 26 juillet de réglementation des télécommunications.

409 Loi No. 96-659 du 26 juillet de réglementation des télécommunications, art. L. 32-II alinéa 5.

410 CNIL, 17e Rapport d'activité, 92 (1997)(discussing the discussion group of the Caisse nationale de prévoyance.)

<www.dejanews.com>, that offer profiling capabilities of message posters could violate the principle of finality. The significance for on-line service offerings is that French discussion groups might need to mask their existence from search engines. Or alternatively, search engines might need to suppress research on French discussion groups to avoid contravening the finality principle of the postings to those discussion groups. At the present ttime, no indication exists that such infrastructure arrangements are either being implemented or contemplated.

For electronic commerce, behavior profiling of customers is emerging as a key component in corporate strategy. The CNIL has addressed behavior profiling in the financial services sector and indicated that client profiling is legitimate only in connection with the development of business strategy and that the profiling can only be used for that purpose.[411] In connection with the endorsement of the Kléline electronic payment system for the Internet, the CNIL noted that the payment transaction records would be particularly valuable and that users were to be informed of their right to oppose any sale of personal information by Kléline.[412] The CNIL also seems to have used its series of decisions regarding the dissemination of professional directories on the Internet as a vehicle to address the possibility of profiling being performed on the traces left in electronic transactions. The CNIL requires that a web server post a conspicuous notice that the information in the directory is subject to the rights and obligations of French law and that collection of directory information to enhance databases for secondary uses, especially marketing purposes, is illegal.[413] At the same time, the CNIL recognizes that the enforceability of finality on the Internet is far from settled; the CNIL requires that notice be provided to the individuals identified in the directories warning those individuals of the enhanced risks of Internet

---

411 CNIL, 14e Rapport d'activité, p. 61 (1994).

412 CNIL, 17e Rapport d'activité, p. 93.

413 Délibération No. 95-131 du 7 novembre, 1995 portant sur la demande d'avis présenté par le Centre national de calcul parallèle des sciences de la terre concernant un traitement automatisé d'informations nominatives pour la publication d'un annuaire sur un réseau international ouvert; Délibération No. 96-065 du 6 juillet 1996 portant avis sur le projet de décision présenté pour le Centre national de la recherche scientifique concernant un modèle type de traitement automatisé d'informations nominatives pour la publication d'annuaires des unités propres ou mixtes sur un réseau international ouvert; Délibération No. 95-131 du 7 novembre 1995; CNIL, 17e Rapport d'activité, p. 70 (1997); CNIL, 16e Rapport d'activité, pp. 84-85 (1996).

dissemination.[414]

In reviewing directories on the Internet, the CNIL has argued that data accessible to the general public does not lose its protection as «nominative» information.[415] Specifically, the CNIL noted that consent for disclosure of directory information in a paper format should not preclude opposition to disclosure of the same information on-line or on CD-ROM.[416] The rationale for this distinction lies in the CNIL's concern for the risks to finality that arise with the availability of directory information on-line. The CNIL requires the web site to display a screen preceding the release of any information that identifies the data's finality.[417] In contrast, the CNIL has, in effect, created an opt-out regime for secondary use of certain public data in connection with the creation of government Internet sites. The decisions authorize distribution over the Internet of information regarding public officials and the exercise of public functions by those officials only after the officials have been advised of unlimited uses that may occur on the Internet and their right to object to Internet dissemination.

Another difficult area for on-line services will likely be the relationship between the French interdiction of the storage of sensitive information[418] and profiling techniques. In particular, to the extent that profile information reveals an individuals «morals,» as illustrated by the individual's surfing patterns or viewing habits, such profiling comes within the ban on the collection of sensitive information. The CNIL appears to allow an exception to this interdiction when the individual grants express consent in writing independently of the collection of sensitive information.[419] Given the seriousness with which the CNIL regards the

---

414 See supra.

415 See CNIL, 17e Rapport d'activité, 73 (1997)

416 CNIL, 17e Rapport d'activité, 73 (1997).

417 Délibération No. 96-065 du 6 juillet 1996 portant avis sur le projet de décision présenté pour le Centre national de la recherche scientifique concernant un modèle type de traitement automatisé d'informations nominatives pour la publication d'annuaires des unités propres ou mixtes sur un réseau international ouvert; Délibération No. 95-131 du 7 novembre 1995; CNIL, 17e Rapport d'activité, p. 70 (1997); CNIL, 16e Rapport d'activité, pp. 84-85 (1996).

418 Loi No. 78-17 du 6 janvier 1978, art. 31.

419 CNIL, Dix ans d'informatique et libertés, p. 44 (1988).

processing of sensitive information, an on-line consent to processing may not be sufficient. To the extent that a search engine, for example, generates a profile revealing «sensitive» information, its use would be illegal.

The necessary restraints on profiling and sensitive information pose a number of issues for the intelligent agents that are increasingly useful in electronic commerce. For example, collaborative filtering and relational agents necessarily develop user profiles and may match them against third party profiles to make a decision or choice automatically. Information delivery services such as PointCast may, for example, customize a subscriber's on-line news in relation to profiles of like-minded subscribers. Only news that would appeal to like-minded subscribers will be delivered to the particular subscriber. To an extent, these agents may conflict with the fundamental provision in French law that no automatic decision be made on the basis of a behavioral profile. Similarly, such functions appear to contradict the policy positions on behavioral profiling. Finally, to the extent that these profiles elicit «sensitive» information, they may be prohibited.

Yet, the regulatory difficulties for intelligent agents are also compounded by their technical features. Not all agents will automatically make decisions. An agent may, for example, search for the best CD-ROM for a client, but not actually execute an order on behalf of the client. If the CD-ROM turns out to be the best Christian music of the 1990s, the agent will be processing sensitive information and confront the special restrictions requiring written consent in advance.

In a similar fashion, the emerging infrastructure for Internet advertising challenges the French principles. The decisional mechanisms for placing banner advertisements on a web surfer's screen, such as DoubleClick, depend on the development of a user profile based on log file information and «cookies.» Since both of these types of information appear to be treated as «nominative» data by the CNIL, the profiling that results in an automatic decision regarding which advertisement to show the user triggers a potential problem; the French law bars any «private decision involving an appraisal of human conduct ... based solely on any automatic processing of data which describes the profile... of the person concerned.»[420] This is especially problematic if the advertisements are selected on the basis of preferences that reveal sensitive information.

Finally, the CNIL has also insisted that the right of opposition permit the subscriber of an e-mail account to refuse the sale of name, address and phone

---

[420] Loi No. 78-17 du 6 janvier 1978, art. 2.

number.[421] The CNIL also expresses particular concern over the secondary use of e-mail addresses by third parties acquiring those addresses from Internet communications.[422] Outside the context of e-mail, the CNIL continues to insist that individuals have an effective right to the suppression from processing of their personal information. Consistently throughout the decisions on professional directories disseminated over the Internet[423] and the review of an on-line payment mechanism,[424] the CNIL has stressed that the concerned individuals be informed of and have a means to suppress the processing of their personal information. In addition, the CNIL is likely to seek affirmative consent, rather than implicit «opt-out» consent, for the commercial distribution of profile information. For example, in its recent endorsement of a financial services discussion group, the CNIL noted that membership on a mailing list of relevant materials was through an opt-in link on the company's site.[425]

Data storage also seems to be a high level concern for the CNIL. The approval by the CNIL of an insurance company's Internet discussion group noted that messages would not be stored longer than three months.[426] Similarly, the advice given by the CNIL for government web sites insisted on the deletion of log files within fifteen days.[427] The short duration of storage is likely to confront the tendency to amass electronic transaction data for future use.

2.4.3 Germany2.4.3 Germany2.4.3 Germany2.4.3 Germany

---

421 Délibération No. 97-050 du 4 juin 1997 relative à une demande d'avis présenté par France Télcom concernant un traitement automatisé d'informations nominatives dénommé «Minitelnet.

422 CNIL, 17e Rapport d'activité, p. 93 (1997).

423 See supra.

424 CNIL, 17e Rapport d'activité, pp. 92-93 (1997)(discussing Kléline).

425 CNIL, 17e Rapport d'activité, p. 91 (discussing the mailing list for the CNP.)

426 Id.

427 See supra.

The BDSG contains no section that explicitly regulates profiling. In contrast, the IuKDG places strict and explicit limits on data profiling. It permits the creation of user profiles only "under the condition that pseudonyms are used."[428] Moreover, once profiles are created that are retrievable under pseudonyms, these data are explicitly forbidden from being combined with data related to the bearer of the pseudonym.[429]

The BDSG also contains no section that explicitly provides higher protection for sensitive data. Nevertheless, its standards for permitting the storage and communication of personal data inherently provide greater protection for such information. Thus, one ground for preventing storage and communication is when the data subject has "legitimate interests" that override "justified interests of the controller of the data."[430] This balancing approach will offer greater protection to sensitive personal data.[431] Like the BDSG, the IuKDG offers no explicit protection for sensitive information. To the extent, however, that it guarantees anonymity in cyberspace and places strict limits on the creation of user profiles, this statute has addressed some of the most critical concerns regarding sensitive personal information.

The IuKDG provides finality by restricting further use of data. It states, "The provider may use the data collected for performing teleservices for other purposes only if permitted by this Act or some other regulation or if the user has given his consent."[432] As this Study has noted above, the Law also seeks to restrict the potential for abuse of this consent provision. The IuKDG contains safeguards to ensure that consent is (1) truly informed, and (2) truly voluntary. Another finality provision of the IuKDG requires the separate processing "of personal data relating to the use of several teleservices by one user."[433]

---

[428] IuKDG, Article 2, § 4(4).

[429] IuKDG, at Article 2, § 4(4).

[430] See BDSG, § 28(1)(2).

[431] Peter Gola & Rudolf Schomerus, Bundesdatenschutzgesetz § 28, 7.1, Seite 383 (6th ed. 1997).

[432] IuKDG, at Article 2, § 3(2).

[433] IuKDG, at Article 2, § 2(4).

Combination of such data are permitting only when "necessary for accounting purposes."[434]

One of the most important ideas of the IuKDG is to require a minimization of the personal data that are collected as part of the provision and utilization of on-line services. The Law's central principle regarding the minimization of data is to require this idea to be reflected in the design of technology. The IuKDG states, "The design and selection of technical devices to be used for teleservices shall be oriented to the goal of collecting, processing and using either no personal data at all or as few data as possible."[435]

Another way that minimization is to be ensured is by requiring personal data to be erased at stated intervals. Thus, utilization data are to be erased "as soon as possible, at the latest immediately after the end of each utilization, except those that are at the same time accounting data."[436] As for accounting data, the Law requires that they be erased "as soon as they are no longer required for accounting purposes."[437]

A final way that the IuKDG seeks to guarantee a minimization of personal data is by limiting the information that is revealed on invoices for on-line services. The Law states, "The invoice concerning the use of teleservices must not reveal the provider, time, duration, type, content and frequency of use of any particular teleservices used unless the user requests such detailed records."[438]

2.4.4 United Kingdom2.4.4 United Kingdom2.4.4 United Kingdom2.4.4 United Kingdom

British data protection law requires finality in data processing and places limits on data storage. As for finality, a number of the data protection principles

---

[434] Id. For a discussion, see Stefan Engel-Flechsig, Die datenschutzrechtlichen Vorschriften im neuen Informations- und Kommunikationsdienste-Gesetz, Recht der Datenverarbeitung 62 (Heft 2/1997).

[435] IuKDG, Article 2, § 3(3).

[436] IuKDG, Article 2, § 6(2)(1).

[437] IuKDG, Article 2, § 6(2)(1).

[438] IuKDG, Article 2, § 6(5).

stress the importance of this fair information practice. The second principle states, "Personal data shall be held only for one or more specified and lawful purpose."[439] The third principle also protects finality by providing, "Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes."[440] Much of the Registrar's interpretation of the idea of finality concerns the registration notice itself. Thus, the Registrar has stated, "use of personal data for any purpose is permitted, without breach of the [incompatibility] Principle, so long as the use of those personal data for that purpose is described in the data user's register entry."[441] The fairness principle does require, however, that data users know of these additional uses and disclosures before they are required to supply information.[442]

British data protection law also requires limits on data storage. One of the data protection principles requires that personal data "shall not be kept for longer than is necessary."[443] It also requires data to be erased "where appropriate."[444] According to the Registrar, this principle implies that "data users should establish procedures for the erasure of data which are no longer used."[445] One suggestion of the Registrar is that data users who hold more than "a very small amount of personal data ... adopt a systematic policy of deleting data."[446] Such data purges would take place at the end of a standard life cycle for records of a particular category.[447]

British data protection law contains no special provisions concerning

---

[439] Id at I.2.

[440] Id. at Part I(3).

[441] Data Protection Guidelines, at 60.

[442] Id. at 54.

[443] Data Protection Act 1984, Part I(6).

[444] Id. at 7(b).

[445] Data Protection Guidance for Direct Mailers, at 36.

[446] Data Protection Registrar, The Guidelines 64-65 (Third Series November 1994).

[447] Id.

profiling, but responds to it as part of its data protection principles. Of particular relevance is the principle of fairness in processing. The Data Protection Registrar has stressed that the duty to obtain information fairly requires steps to be taken to make the individual "aware of the additional purposes for which the information will be held and the additional uses and disclosures before he or she is required to supply the information."[448] This language essentially approaches profiling through a notice requirement. This approach is echoed by the Code of Practice of the Internet Service Provider's Association (ISPA).[449] The ISPA speaks of the requirement of its members to use "reasonable endeavors to ensure that services which involve the collection of personal information ... must make it clear to the relevant party the purpose for which the information is required."[450] No particular provision in this Code addresses profiling.

It is increasingly difficult for individuals to know the kind of profiling that is occurring in the on-line world. The application of the fairness principle to profiling by Internet Service Providers or websites is as yet unsettled.

The Data Protection Act permits the Secretary of State to supplement the data protection principles to provide additional safeguards for four categories of sensitive data. These categories pertain to information as to the data subject's (1) racial origin; (2) political opinions or religious or other beliefs; (3) physical or mental health or his sexual life; or
(4) criminal convictions.[451] These powers have not yet been exercised; the Secretary of State has not issued such a statutory instrument.

As part of the process of compliance with the European Directive, explicit protection for sensitive information is likely to be added to the UK Data Protection Act.[452] One proposal, which was made by the Data Protection Registrar in its

---

[448] Data Protection Registrar, The Guidelines 54 (Third Series November 1994).

[449] <http://www.ispa.org.uk>

[450] Id.

[451] Data Protection Act 1984, 2(3).

[452] See Consultation Paper on the EC Data Protection Directive, 4.1 (1996) ("Article 8 [of the Directive] sets special rules for the processing of data which are regarded as being particularly sensitive. Such special rules are effectively new to United Kingdom law.") <http://elj.warwick.ac.uk/jilt/Consult/ukdp/
dataprot.htm>.

response to the official Consultative Paper on the Directive, calls for the Secretary of State to implement a Sensitive Data Decree.[453] As a model for potential British efforts, the Registrar pointed to the Netherlands' Sensitive Data Decree.[454] The Registrar has also advocated a new category for sensitive data in registration.[455]

Although no specific British statute explicitly addresses the minimalization of personal data on the Internet, the principle of minimalization is well established in British data protection law. In particular, the UK Data Protection Registrar's advocacy of privacy enhancing technologies has stressed the importance of minimalization of data. As the Registrar stated in its response to a governmental prospectus for the electronic delivery of government services, "The key principle underlying the privacy enhancing design approach is that the quantity of personal information in any transaction should be the minimum required for that transaction."[456] This governmental proposal, entitled "government.direct," offers, according to the Registrar, an ideal opportunity for a commitment to technology design that will collect the least amount of personal data possible.

The relationship between privacy enhancing technologies and data minimalization requires the right questions to be asked when technology is being designed. Among these questions, the Registrar views the following as an essential part of technology design, "Do I need to collect any personal data at all?"[457] The Data Protection Registrar is currently searching for pilot schemes in which to promote the privacy enhancing philosophy and technique.

2.5 Security2.5 Security2.5 Security2.5 Security

---

[453] Data Protection Registrar, Consultation Paper on the EC Data Protection Directive, Our Answers 5.3. <http://www.open.gov.uk/dpr/answer/ans4-5.htm>.

[454] See id. at Appendix II.

[455] Data Protection Registrar, The Future of Registration. www.open.gov.uk/dpr/chap5-8.htm#standard.

[456] Response to Government.Direct Including a Paper of Privacy Enhancing Technologies, in UK Data Protection Registrar, The Thirteenth Activity Report 102 (1997).

[457] Id.

One of the most controversial areas, at present, for the Internet and online services is the balance between cryptography and law enforcement concerns. On one hand, commercial services and individuals need and seek to improve the security of communications by using different kinds of cryptography for on-line transmissions of personal data, especially in the context of electronic payments.[458] The European Directive requires the implementation of «appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.»[459] The European Directive further requires that «such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected» with due consideration of the state of the art and the cost of implementation.[460] On the other hand, some law enforcement agencies in Europe argue that cryptography must be limited so police will be able to gain the access to online data necessary to fight organized crime. A debate that began in the United States concerning key escrow proposals and limits on the exportation of cryptography has been taken up throughout Europe. For example, the German Interior Minister has recently announced his own key escrow proposal.[461] Some German data protection commissioners are currently contesting this proposal's likely effectiveness. The European Commission has also taken a strong position in favor of the freedom of private parties to encrypt information.[462]

2.5.1 Belgium2.5.1 Belgium2.5.1 Belgium2.5.1 Belgium

---

[458] See Part I, _ II.1.3

[459] Directive 95/46/EC, art. 17.

[460] Id.

[461] For a further discussion, see _ 2.5.3 below.

[462] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Ensuring Security and Trust in Electronic Communications: Towards A European Framework for Digital Signatures And Encryption COM (97) 503 (October 7, 1997).

The Belgian data protection law both directly and indirectly requires the «controller» of personal information to use appropriate security for the processing of the data. «Controllers» must assure the protection of personal information against access by anyone whose functions do not require such access and against «modifications, additions, erasure, disclosures, or combinations and interconnections that are unforseen, unauthorized or forbidden» by anyone with access.[463] Controllers must further «take the technical and organizational measures required to protect files against accidental or unauthorized destruction, accidental loss, as well as against the modification, access or any other unauthorized processing of personal information.»[464] These technical measures must guarantee an adequate level of protection considering the state of the art, the cost of the security measures and the nature of the risks associated with the particular personal information.[465] Royal Decrees may also mandate specific security standards for any processing or type of processing.[466]

These security requirements imposed by the data protection law have a significant impact for online services. Electronic commerce functions must take measures to assure transmission integrity. While no specific decisions appear yet to exist, a reasonable inference is that Belgian data protection rules will require the use of cryptography and some forms of digital signature for online transactions. Similarly, the requirement imposed upon «controllers» may have implications for the function of search engines. A «controller» for personal information maintained on a web site might have to take measures to block access by search engines if the processing by the person launching the search is unauthorized, such as the situation in which the person launching the search seeks to exceed the finality permitting the storage of the personal information.

In contrast to the data protection law's mandate for security, the wiretapping law[467] undercuts any absolute security measures. Belgian law imposes

---

463 Loi du 8 décembre 1992, art. 16(1)(4).

464 Loi du 8 décembre 1992, art. 16(3).

465 Id.

466 Id.

467 Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées.

an obligation on network operators to insure that the technical infrastructure allows law enforcement access to the contents of communications.[468]

Because of the CPVP's predisposition for strong security, the CPVP has been critical of regulation limiting cryptography. In an advisory opinion on proposed changes to the wiretapping and pen register law, the CPVP reported that the imposition of key escrow was an «excessive and disproportionate measure with respect to security needs.»[469] The CPVP prefered the approach advocated by various international bodies, notably at the OECD and at the European Union.[470] The CPVP, in particular, objected to the delegation of regulatory authority through Royal Decrees.[471] Prominent industry leaders in Belgium are also opposed to key escrow.[472]

For the moment, the Belgian government has accepted the relaxation of cryptography regulation. In a draft bill, dated May 1997, the Ministry of Communications and Infrastructure has accepted to allow cryptography to be «unregulated»[473] rather than have it subject to key escrow. However, the explanatory report from the Ministry says that this liberalization «does not signify that the legislature has completely abandoned all hope of having the ability to access clear text messages in the future .... this issue will be reviewed at a later date in light of technological evolutions or abusive use of cryptography.»[474]

---

[468] Loi du 21 mars 1991 portant réforme de certaines entreprise publiques économiques, art. 70bis.

[469] CPVP, Avis no. 09/97 du 20 mars 1997, p.7

[470] Id.

[471] Id.

[472] See, e.g., BELINFOSEC, Rapport soumis à l'approbation sur les aspects juridiques de la sécurité informatique-- La cryptographie en droit belge (Juillet, 1996).

[473] Ministère des Communications et de l'Infrastructure, Avant-Projet de loi modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques afin d'adapter le cadre réglementaire aux obligations en matière de libre concurrence et d'harmonisation sur le marché des télécommunications découlant des décisions de l'Union européenne, art. 76 (27 mai 1997)(«L'emploi de la cryptographie est libre.»)

[474] Id., Exposé des motifs, at 51.

This tension between the Belgian government efforts to seek regulation of data security and the CPVP's objections will create a degree of instability for on-line services.

2.5.2. France2.5.2. France2.5.2. France2.5.2. France

France has two significant and potentially contradictory legal requirements for the security of nominative information. The data protection law obligates anyone processing personal information «to take all useful precautions in order to protect the security of information and particularly to prevent that such information becomes corrupted, damaged or communicated to unauthorized third parties.»[475] The security obligation requires the reliability of hardware and software mechanisms and the ability of these mechanisms to resist tampering.[476]

At the same time, the 1996 Telecommunications Law[477] creates a new framework for the use of encryption. Prior to the new law, all encryption for information security was subject to government licensing. The new telecommunications law provides for freedom to use cryptographic means to authenticate or to assure the integrity of messages.[478] Encryption may be used to secure the contents of message transmission if the encryption keys are deposited with a trusted third party.[479] The trusted third party must be licensed by the state.[480] However, the terms of licensing have not yet been specified by ministerial decree and there is no indication if foreign escrow agents will be permitted. Any other cryptography must be specifically licensed by the Prime Minister.[481] This reform package is intended to strike a balance between the needs of users to

---

475 Loi No. 78-17 du 6 janvier 1978, art. 29.

476 CNIL, Dix ans d'informatique et libertés, pp. 49-50 (1988).

477 Loi No. 96-659 du 26 juillet 1996.

478 Loi No. 96-659 du 26 juillet 1996, art. 17.

479 Id.

480 Id.

481 Id.

engage in secure transactions and the interests of national defense and public security to gain access to encrypted communications. The new law grants law enforcement access to the encryption keys deposited with licensed trusted third parties. In effect, the purported liberalization of encryption remains far from an encouragement to secure treatment of personal information as contemplated in the data protection law.

The CNIL has repeatedly emphasized security measures to assure the finality of personal information. A series of decisions in the context of health information and patient records emphasize the crucial security elements.[482] For ministerial Internet sites, the CNIL has pointedly noted the essential need for security mechanisms to assure the integrity and finality of data processing.[483] The CNIL has also noted that even directory information placed on public web servers must have sufficient security to assure no other public access to personal information.[484] In addition, the CNIL has focused on the use of security to assure the integrity of personal information. For example, Kléline, the electronic payment service for the Internet, received a favorable review by the CNIL due in part because of Kléline's emphasis on security mechanisms.[485] The CNIL noted that consultations with national security officials was a necessary part of the examination of the data processing arrangements to ascertain that satisfactory, legal security mechanisms were deployed.[486]

Yet, security issues have had varying meaning over the last few years. In 1993, for example, the CNIL favored the use of pre-paid chip cards because they provided security for anonymous payment transactions and accepted the

---

[482] Id., at 108-123.

[483] See Délibération No. 97-032 du 6 mai 1997 relative à la demande d'avis présenté par le premier ministre concernant un modèle-type de traitements d'informations nominative opérés dabs ke cadre d'un site Internet ministériel.

[484] Délibération No. 96-065 du 6 juillet 1996 portant avis sur le projet de décision présenté pour le Centre national de la recherche scientifique concernant un modèle type de traitement automatisé d'informations nominatives pour la publication d'annuaires des unités propres ou mixtes sur un réseau international ouvert; Délibération No. 95-131 du 7 novembre 1995; CNIL, 17e Rapport d'activité, p. 70 (1997); CNIL, 16e Rapport d'activité, pp. 84-85 (1996).

[485] CNIL, 17e Rapport d'activité, pp. 92-93 (1997).

[486] Id., at 92.

introduction of chip cards for medical services due, in part, to the security measures that would assure limited access to stored personal information.[487] By contrast, the intelligence service of the Ministry of Interior viewed the 1997 introduction of the Mobicarte, a payment card for mobile telephones, as a fundamental challenge and required that France Telecom build in the capacity for tracking and identifying callers.[488] In this case, security was a means to identify and track individuals rather than create anonymity.

The access by law enforcement to personal information is likely to become an area of increasing friction. The French law's declaration requirements are inapplicable to cases involving national security, defense or public safety.[489] Similarly, public sector data processing involving national security, defense or public safety need not be disclosed through publication of the authorizing regulations. Special procedural rules apply to the exercise of the individual's right of access to personal information if the processing implicates national security, defense or public safety.[490]

2.5.3 Germany2.5.3 Germany2.5.3 Germany2.5.3 Germany

For on-line services, the IuKDG places an obligation to provide security on the provider. It requires that the user be protected against third parties obtaining knowledge of her use of teleservices and that personal data generated in connection with accessing teleservices generally be immediately erased.[491] The IuKDG also creates a scheme for the voluntary use of digital signatures,[492] which will be discussed below.

---

[487] CNIL, 14e Rapport d'activité, pp. 72-73 (1994).

[488] La mobicarte de France Télécom épinglé par le ministère de l'intérieur, Agence France Presse, March 27, 1997.

[489] Loi No. 78-17 du 6 janvier 1978, art. 19.

[490] Loi No. 78-17 du 6 janvier 1978, art. 39.

[491] IuKDG, Article 2, §2(2) & (3).

[492] IuKDG, Article 3.

As part of its provisions for on-line security, Germany currently places no restrictions on the use of cryptography within Germany, or on the import or export of cryptography software. This situation may change, however, as a vigorous debate is now underway concerning the need for a so-called "Crypto-Law" (*Kryptogesetz*) that would limit cryptography. The German Minister of the Interior, the German Intelligence Community, and some elements of the CDU have taken a position in favor of limits on cryptography. Other German ministers, state data protection commissioners, and German industry have taken a vigorous position against any restrictions on cryptography.[493]

The parties who seek limits on cryptography have argued that such measures are needed to protect the activities of law enforcement authorities. As a CDU argument in favor of the regulation of cryptography states, "The introduction of widespread encryption can have the result of making seriously more difficult the work of the authorities responsible for prosecution of crimes by causing legally monitored communication to become 'unreadable.' This result would disadvantage law abiding citizens."[494] Such potential harm to law enforcement's ability to monitor communications is the most frequently cited policy reason in favor of regulation in this area.[495]

In one internal articulation of the government's favored approach, which

---

[493] See generally Tobias Stroemer, Bonner Streit um Kryptogesetz (1997) <http://www.netlaw.de/newstick/krpto-2.htm>; Lorenz Lorenz-Meyer, Das Kreuz mit der Kryptographie, Spiegel Online Archiv-Dokument 3/1997 <http://www.spiegel.de/special.heft2/krypto.html>.

[494] CDU, Argumente gegen eine Kryptoregelung und Erwiderungen. <http://www.cdu.de/bpt/archiv97/krypto.html>.

[495] More specifically, some government agencies have pointed to the use of encryption by criminals and by extremist groups. In the latest report of the Bureau for the Protection of the Constitution (*Amt für Verfassungschutz*), for example, this agency noted that the use of new electronic communication media was increasingly important for extremist groups. Amt für Verfassungschutz, Verfassungsschutzbericht 1996, Linksextremistische Bestrebungen I., 2.3. http://www.bundesregierung.de/inland/ministerien/bmi/vsber96/links_i.html.

These extremist groups were also found to be using encryptions algorithms, in particular "Pretty Good Privacy," to encode their communications. Id. Among the strongest advocates for limitations on encryption software are the Bureau for the Protection of the Constitution, the Federal Information Agency (*Bundesnachrichtdienst*), and the Minister of the Interior, Manfred Kanther.

Der Spiegel revealed, an inter-ministerial group of experts advocated the establishment of a three-step approach to the control of cryptography.[496] First, those who offer encryption products and services would be obliged to offer data in clear text to government authorities. This demand has already been met as far as telecommunication providers are concerned. While German law places no current restrictions on end-to-end encryption, the Telecommunications Act requires telecommunications providers to make technical provisions to allow their networks to be open to surveillance by the appropriate authorities.[497] Second, the utilization of encryption systems would require authorization by government. This utilization would be tied to the possibility that reconstruction of encrypted data could be made in a fashion that was "current and subject to reasonable expenditures." Finally, the use of non-authorized encryption processes would be forbidden.[498]

The acceptance of this proposal is far from certain. Numerous voices in Germany have been raised against any proposal to regulate cryptography.[499] Some of these voices are within the federal government. Thus, the Federal Justice Minister Edzard Schmidt-Jortzig, the Technology Minister Jürgen Rüttgers, and the Commerce Minister Günter Rexrodt, have expressed skepticism regarding limits on encryption. On May 2, 1997, for example, Dr. Rexrodt issued a press release that claimed the Federal Ministry of Commerce has taken an active role during the last years to block the federal government from introducing any measure restricting encryption.[500]

State data protection commissioners have also taken a highly active role in this debate. The Schleswig-Holstein Commissioner has found, for example, that encryption tools are no less than a "gift from heaven." In his most recent report of

---

[496] Lorenz Lorenz-Meyer, Das Kreuz mit der Kryptographie, Spiegel Online Archiv-Dokument 3/1997 <http://www.spiegel.de/special.heft2/krypto.html>.

[497] Telekommunikationsgesetz vom 25 Juli 1996, § 88.

[498] Lorenz Lorenz Meyer, Das Kreuz mit der Kryptographie, Spiegel Online Archiv-Dokument 3/1997 < http://www.spiegel.de/special.heft2/krypto.html>.

[499] See generally Tobias H. Stroemer, Bonner Streit um Krypto-Gesetz (1997) <http://www.netlaw.de/newstick/krypto-2.htm>.

[500] Bundesministerium für Wirtschaft, Rexrodt weiter strikt gegen Kryptographieverbot (May 2, 1997). http://www.bmwi.de/presse/1997/0502prm.html.

activities, Dr. Bäumler advocates the use of encryption without restrictions as a way to protect communications and financial transactions in open nets. This report states:

> It remains to hope that policymakers grasp that encryption represents *a unique chance* to protect the private sphere in a problematic, technical environment. Moreover, the experts are fairly unanimous that *forbidding* or a limitation of cryptography would be *ineffective*. It would be easy to circumvent these restrictions precisely by those against whom they were raised-- namely members of sophisticated organized crime organizations.[501]

While encryption offers a powerful step forward for data protection, any attempts to limit it are said to be doomed to failure.

The Data Protection Commissioner of Hesse has followed up on the idea that encryption will be impossible to limit. In the 25th Annual Activity Report of this Commissioner, Dr. Rainer Hamm argues in favor of government renouncing its regulation of encryption technology because of the technical difficulties of enforcing effective limits on cryptography. Dr. Ham found that "Every governmental regimentation of the introduction of encryption processes by the transfer and storage of data will be for naught."[502] This result follows from such factors as the ease in which this regulation can be circumvented, that oversight of encryption is hardly possible, and that it opposes other governmental and economic interests in the security of data.[503] Dr. Hamm also objected to key escrow proposals, which he felt raised additional risks to the security of keys.[504] Other data protection commissioners have also raised strong objections to limits on encryption based on these notions.[505] Another objection to encryption views legal restrictions on this technology as unconstitutional. One data protection

---

[501] 19.Taetigkeitsbericht, 2.3 (1996)(emphasis in original).

[502] Der Hessische Datenschutzbeauftragte, 25. Tätigkeitsbericht 161 (1996).

[503] Id. at 155-161.

[504] Id.

[505] See, e.g., Berliner Datenschutzbeauftragter Jahresbericht 1996, § 3.4 (1997), <http://www.datenschutz-berlin.de/jahresbe/96/teil3.htm>.

expert has pointed to a potential violation by encryption controls on the Basic Law's Article 10, which protects the privacy of communications.[506] A law that limits encryption is likely to infringe on this constitutional right without any positive effect on any other constitutional interest. As such, limits on encryption are said to be unconstitutional due to their ineffectiveness and unsuitability.[507]

Finally, German industry has played an active role in supporting unrestricted use of encryption. For example, the German Information Technology Manufacturer's Association (*Fachverband Informationstechnik*) has stated that any regulation of cryptography would "create only unnecessary administrative and cost expenditures in considerable amounts and reduce the export chances for German security products."[508] The Telesec, a division of the Deutsche Telekom, the newly privatized German telecommunications provider, has also objected to restrictions on encryption.[509] This opposition has also been accompanied by resistance among experts and among the population in the general.[510]

As for digital signatures, the German lawmaker has provided for their use in the IuKDG. While this provision provides for anonymous use of digital signatures, the IuKDG's Digital Signature Law also permits law enforcement authorities to find out the names of those who use such digital keys under a pseudonym. Finally, the Digital Signature Law contains provisions concerning data protection vis-a-vis the certification authorities' own collection of data.

The IuKDG's Article 3 regulates the use of digital signatures. This section of the Law, which is termed the Digital Signature Act (*Signaturgesetz*), establishes the "conditions under which digital signatures are deemed secure and forgeries of

---

[506] Johann Bizer, Rechtliche Bedeutung der Kryptographie, 21 Datenschutz und Datensicherung 203 (1997).

[507] Id. See also Norbert F. Poetzl, Kuverts fuer E-mail, Spiegel On-Line. <http://www.spiegel.de/special/heft2/ss03100.html>.

[508] Fachverband Informationstechnik, Position zur Einfuehrung des "Gesetzes zur digitalen Signatur" und zur Regulierung von Verschluessungsverfahren. http://www.telesec.de/fvit.htm.

[509] Telesec, Kryptokontroverse. <http://www.telesec.de/recht3.htm>.

[510] Two elaborate web sites that reflect this more general opposition the encryption are <http://www.crypto.de and www.thur.de/ulf/krypto/verbot.html>.

digital signatures or manipulation of signed data can be readily ascertained.[511] The German lawmaker enacted legislation in this area as an essential step to encourage commercial activities on the Internet.[512]

The IuKDG's Digital Signature Act sets up a licensing procedure that involves two critical actors: the "competent authority" and the "certification authority." Under the Law's approach, the competent authority, a governmental body, gives licenses to assign public signature keys to certification authorities. The competent authority is a specific government agency, which the Law also identifies; according to the Digital Signature Act, the competent authority is the "Regulatory Authority of the Telecommunication and Postal Services" (*Regulierungsbehörde*).[513] This body is located within the Commerce Ministry *(Ministerium für Wirtschaft*).[514]

In its role granting licenses to distribute digital signatures, the Regulatory Authority (called the "competent authority" in the IuKDG) makes the digital certificates which it has issued available for verification and retrieval at all times over publicly available telecommunication links.[515] The Regulatory Authority also has an important role in monitoring the behavior of the certification authorities, who are the bodies responsible for distributing the digital signatures. The Regulatory Authority can forbid the use of unsuitable technical components and

---

[511] IuKDG, Article 3, § 1(1).

[512] As the federal government (*Bundesregierung*) stated in introducing the IuKDG, "The development of information and communication technology opens new possibilities for data transfers and for economic activities." Gesetzentwurf der Bundesregierung, Deutscher Bundestag, 13.Wahlperiode, Drucksache 13/7385 (09. April 1997) at 25.

In place of the omnibus standards of the BDSG and any uncertainty regarding their application, a sector law would create legal certainty for these new data transfers and economic activities. In addition, with increasing electronic transfers of personal information, including sensitive data in the medical sector, the German government pointed to a "urgent need" for a digital solution to protect data from unnoticed alteration.
Id.

[513] IuKDG, Article 3, § 3. This section references the Telecommunications Act, § 66.

[514] Telecommunications Act, § 66.

[515] IuKDG, Article 3, § 4.

oversee the activities of a certification authority by visiting its sites.[516] This provision has no territorial limit on it, which would suggest that a body outside of Germany that sought licensing by the German Regulatory Authority would also be subject to it. On the other hand, the Digital Signatures Law contains provisions regarding certificates issued by other countries, which may indicate that only German entities can certify keys as a certification authority.[517] Finally, the Regulatory Authority can also revoke licenses "in the event of non-fulfillment of obligations" arising under the Digital Signature Law.[518]

As to the role of the certification authorities, these bodies are responsible for the issuing of key certificates to the parties who wish to affix a digital signature to a document.[519] According to the Digital Signatures Law, digital certificates are to contain information regarding: (1) the name of the owner of a signature key or the distinctive pseudonym assigned to the key's owner; (2) the public signature key that is assigned; (3) the names of the algorithms with which the public key of the owner of the signature key and the public key of the certification authority can be used; and (4) an indication as to whether use of the signature key is restricted in type or scope to specific applications.[520]

The Digital Signature Law permits the certification authority to collect personal data only under limited circumstances. These data must be collected only (1) when this information is required for the purposes of a certification, and (2) directly from the party concerned.[521] Any collection of data from third parties may be permitted only with the consent of the party concerned.[522]

According to the Digital Signatures Law, certificates issued by other countries for a digital signature are deemed equivalent to digital signatures issued

---

[516] IuKDG, Article 3, §§ 4-5.

[517] IuKDG, Article 3, § 15.

[518] IuKDG, at Article 3, § 13(3).

[519] IuKDG, at Article 3, § 4.

[520] Id. at Article 3, § 5-7.

[521] IuKDG, Article 3(12).

[522] Id.

under this Law when the foreign digital signature is as secure as a German one.[523] Finally, certification authorities are explicitly forbidden from the storage of private signature keys-- although such devices themselves are not forbidden by German law.[524]

As the requirements for digital certificates indicate, digital signatures may be issued to individuals who wish to use them under a pseudonym. Making digital signatures available for use with a pseudonym allows a person to enter into cyber-life and maintain anonymity, which provides an important measure of data protection. As the Federal Data Protection Commissioner observed in his 16th Report of Activities:

> Through the [establishment of a pseudonym] the amount of personal data that is automatically created about a person in the context of business transactions over telecommunication connections can be seriously reduced. The availability of user profiles, the surveillance of consumer behavior as well as direct advertising by companies will thereby be almost entirely precluded.[525]

The handing out of publicly certified digital signatures on a pseudonymous basis is subject, however, to access to information about one's true identity by law enforcement agencies.

The Digital Signature Law contains standards that permit a range of governmental bodies to gain data pertaining to a person's actual identify when this information has been masked behind a publicly certified digital signature. This Law permits the de-anonymization of pseudonym provided for digital signatures for a defined set of law enforcement purposes:

> the prosecution of criminal or administrative offences, for averting danger to public safety or order or for the discharge of statutory duties by the Federal and State authorities for the protection of the Constitution, the Federal Intelligence Service (*Bundesnachrichtendienst*), the Military

---

[523] Id. at Article 3, § 15(1).

[524] Id. at Article 3, § 5(4).

[525] 147.

Counter-Intelligence Service (*Militaerischer Abschirmdienst*) or the Customs Criminological Office (*Zollkriminalamt*).[526]

All requests for information are to be documented and are generally to be share with the owner of the signature key at a later date.[527]

The IuKDG contains another section regarding law enforcement access to personal data. In its Article 2, §6, it carves out a law enforcement exception to its protection for utilization and accounting data. This section first forbids the transmission of these data "to other providers or third parties," and then declares, "This shall not affect the powers of criminal prosecution agencies."[528] The Federal Data Protection Commissioner has criticized this aspect of the law as giving a disproportionate power to law enforcement authorities.[529] More details regarding the use of the digital signatures are to be provided by the Digital Signature Regulation (*Verordnung zur digitalen Signatur*). The German government released a draft of this bill on October 8, 1997.[530]

2.5.4 United Kingdom2.5.4 United Kingdom2.5.4 United Kingdom2.5.4 United Kingdom

Data security is an important element of data protection in the United Kingdom. The eighth and final data protection principle requires data security. It states, "Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data."[531] According to the Registrar, "The prime responsibility for creating and putting into practice a security policy must rest with

---

[526] IuKDG, Article 3, § 12(2).

[527] Id.

[528] Id. at Article 2, § 6.

[529] Federal Data Protection Authority, 16th Activity Report, 144.

[530] Verordnung zur digitalen Signatur in der Fassung des Beschlusses der Bundesregierung vom 8.Oktober 1997 <http://www.iid.de/rahment/sigv.html>.

[531] Data Protection Act 1984, Part I, Schedule 1(8).

the computer user."[532] This policy must take all reasonable steps to insure security. The reasonableness of security will be measured according to the "risk of harm to individuals from a breach of security."[533]

Risks to data security are likely to increase in the on-line world, and the Data Protection Registrar has begun to address this issue in its guidance on "Homeworking and Computer Information."[534] This guidance examines both e-mail in particular and the Internet in general.

Concerning e-mail, the Registrar states that e-mail is generally likely to be at some risk. These risks are due to the nature of the Internet and e-mail systems:

> As a form of network the Internet is particularly insecure and cannot be relied on to provide protection for personal data. In addition it is probable that the service provider will have access to the mailbox as well as the person to whom the mailbox is assigned.
>
> However, in reality, the risks associated with the use of e-mail for routine nonsensitive messages are not great. While it may be possible for the mailbox to be accessed by unauthorised people, they are unlikely to attack the computers remotely accessing the mailbox. The time spent accessing the mailbox is short and does not allow much of an interval for interference.[535]

According to the Registrar, use of the Internet without encrypting messages may be generally consistent with the requirement for appropriate security. Where sensitive personal information is contained in messages, however, use of the Internet may be appropriate only if an "appropriate form of encryption" is utilized.[536]

As for the Internet in general, the Registrar discussed the need for organizations to take general security measures to assure the integrity of

---

[532] Data Protection Registrar, The Guidelines 66 (Third Series 1994).

[533] Id. at 68-69.

[534] Data Protection Registrar, Homeworking and Computer Information 25 (June 1997).

[535] Id. at 28

[536] Id.

information. These include the installation of "firewalls," taking care as to the personal data that are included on a website, and seeking informed consent of anyone whose data will be used on a website.[537] The Registrar also warned of the possibility of credit card theft on the Internet and suggested the use of "appropriate security measures, such as encryption."[538]

As in other countries, a vigorous debate is underway in the United Kingdom regarding the regulation of cryptography. The Department of Trade and Industry is playing a key role in this debate; much of the discussion is being shaped by its consultation paper, "Licensing of Trusted Third Parties for the Provision of Encryption Services."[539] This governmental paper argues in favor of official licensing of Trusted Third Parties (TTP) who will provide encryption services.

Under the proposed scheme, the government is to provide licenses to TTPs, "which will provide encryption services to a wide range of bodies across all sectors."[540] Of this voluntary licensing scheme, the Department of Trade and Industry states:

> The licensing regime will seek to ensure that organisations who wish to establish themselves as TTPs will be fit for the purpose. It will aim to protect consumers as well as to preserve the ability of the intelligence and law enforcement agencies to fight serious crime and terrorism by establishing procedures for disclosure to them of the encryption keys, under safeguards similar to those which already exist for warranted interception under the Interception of Communications Act 1985.[541]

As this statement makes clear, the Department of Trade and Industry plans both licensing and a key escrow approach.

Of licensing in general, the Department's plan is to ensure that TTPs can be

---

[537] Id.

[538] Id.

[539] Department of Trade and Industry, Licensing of Trusted Third Parties for the Provision of Encryption Services: Public Consultation Paper (March 1997) <http://dtiinfo1.dti.gov.uk/pubs>.

[540] Id. at § 40.

[541] Id. at § 17.

trusted by the entities that they serve. Licensing will protect consumers, allow interoperability of secure services, and allow UK business to take advantage of secure electronic trading.[542] Moreover, use of a licensed TTP will be entirely voluntary. As the paper states, "The market will decide if it wants to use TTP services and not Government. The Government believes that the benefits of this scheme will far outweigh any others.»[543]

Although use of a TTP is voluntary, the TTP itself is to have no choice regarding its participation in a key escrow scheme. Issuance of a warrant to law enforcement officials would require a TTP to disclose in a timely manner the cryptographic key material to a central repository, which would act on behalf of an governmental agency. The Department of Trade and Industry has set out the role of the central repository in language worth quoting in some detail:

> For purpose of legal access, a central repository might be nominated or established by the UK authorities. The purpose of this central repository will be to act as a single point of contact for interfacing between a licensed TTP and the security, intelligence and law enforcement agencies who have obtained a warrant requiring access to a client's private encryption keys. The central repository would, therefore, be responsible for serving the warrant (whether by physical or electronic means) on the TTP and distributing the encryption key to the appropriate agency.[544]

The entire process of obtaining keys, from the time the central repository serves the warrant to the delivery of the keys, is intended to take no more than one hour.[545]

The Department of Trade and Industry also foresees a process by which foreign TTPs will share keys with competent authorities in the United Kingdom. The government plan will allow foreign TTPs to be chosen by UK clients. Yet, the Department states, "It will therefore be necessary (for law enforcement purposes)

---

[543] Id. at § 42

[544] Id. at § 77.

[545] Id at § 78.

to establish arrangements with other countries for the exchange of keys.[546] These arrangements are to be on the basis of "dual legality," which means that a demand for access must meet criteria in both countries. The Department observes, "The keys held by UK licensed TTPs will not, under this legislation, be permitted to be disclosed to the authorities of other countries unless such requests satisfy UK law and are authorised by the competent UK authority."[547] Finally, the Department of Trade and Industry states that no recovery of keys will be allowed regarding an "integrity function."[548] By this term, the Department refers to the use of encryption for reasons other than encoding information, such as verifying digital signatures.

This official proposal has met with various levels of criticism. To begin with the Data Protection Registrar's response, her comments are divided into responses to two principle issues: (1) the regulation of encryption and encryption services; and (2) the circumstance under which law enforcement agencies should have access to encrypted data.[549] Concerning the regulation of encryption, the Registrar "welcomes the proposals to license Trusted Third Parties to the general public ... and particularly welcomes the fact that the use of the licensed services is to be on a voluntary basis."[550] In particular, the Registrar found merit in establishing a regulatory regime for those who provide encryption services for others to assure standards for these services.[551]

As for lawful access to encrypted data, the Data Protection Registrar accepts that circumstances exist under which relevant authorities should be able to obtain access to information. Here, the Registrar cites the European Human

---

[546] Id. at § 55.

[547] Id. Annex B to the report contains further details regarding international aspects of the government's proposal.

[548] Id. at § 46.

[549] Response of the Data Protection Registrar, Licensing of Trusted Third Parties for the Provision of Encryption Services (March 1997) < http://www.open.gov.uk/dpr/ttpfinal.htm>.

[550] Id. at § 3.5(d).

[551] Id. at § 2.2.2 ("There is merit in establishing a regulatory regime for those who are providing encryption services to others: to set and assure the standard of those services.").

Rights Convention, which spoke of limits on privacy being acceptable "in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others."[552] This limitation on privacy is potentially broad, of course, and the Data Protection Registrar stresses that lawful access to encryption codes should be made through judicial process.[553] In addition, lawful access should take place as a part of a general regime of transparency regarding the implications of lawful access.[554] As the Registrar states:

> Users of licensed TTPs should be aware that the potential for lawful access to their keys without their knowledge means that they cannot assume that encrypted data is ever fully secure. They should also be aware that lawful access may be granted to others based outside the UK.[555]

The Data Protection Registrar finds that even with key escrow the level of risk for the majority of individuals and businesses will be acceptable.[556] Finally, the Registrar stresses that the ability of authorities to encrypt data should not put them in a position of being able to impersonate anyone.[557] The use of encryption for authentication should not be put into question by a regime of access to encryption codes.

Both industry and the civil liberty community in the United Kingdom have raised vigorous objections to encryption. For example, British Telecommunications' (BT) objection to the Department of Trade and Industry's paper is that it places too little emphasis "on the mechanisms of trust" as opposed

---

[552] European Human Rights Convention, Article 8.

[553] Response of the Data Protection Registrar, Licensing of Trusted Third Parties for the Provision of Encryption Services, at § 3.7 < http://www.open.gov/uk/dpr/ttpfinal.htm>.

[554] Id. at § 3.6.

[555] Id. at § 3.6.

[556] Id. at § 3.6.

[557] Id. at § 3.8.

to "ensuring that government is able to intercept encrypted communications."[558] BT also expresses concern regarding plans for international warrants to obtain disclosures of keys. The fear is that such a provision will encourage international industrial espionage. In BT's words, "There is a need for caution here in so far as this may allow for some countries to make use of law enforcement and security agencies to obtain information to enable their own 'flagship' businesses to obtain competitive advantage."[559] Finally, BT stresses that encryption keys used for authentication and protection of data integrity should not be made available to law enforcement without the legal owner's permission.[560] The law must differentiate between processes for access to keys which are used to protect confidentiality and keys that are used for authentication and checks of data integrity.[561] Other UK industry spokespersons have contested the government's plan for regulating encryption technology.[562]

Civil liberty organizations have also objected to the Department of Trade and Industry's proposal for encryption. The Cyber-Rights and Cyber-Liberties (UK) group has protested key escrow as creating "an unprecedented technical capability for mass surveillance."[563] This group also felt that centralized storage

---

[558] BT's Comments on the Public Consultation Paper "Licensing of Trusted Third Parties for the Provision of Encryption Services" (May 1997). <http://www.bt.com/regulate/otherresp/hmgothers/encryption/doc.htm>

[559] Id. at 61. <http://www.bt.com/regulate/otherresp/hmgothers.encryption/response.htm>

[560] Id. at Appendix. <http://www.bt.com/regulate/otherresp/hmgothers/encryption/annexa.htm>.

[561] Id.

[562] See, e.g., Intel Corporation (UK) Ltd response to the UK Government Consultation Paper, <http://www.cs.ucl.ac.uk/staff/I.Brown/dti/intel.htm>; for an interesting comment on the UK proposal from a committee of the American Bar Association, see ABA Science & Technology Information Security Committee, Response to the Department of Trade and Industry's "Licensing of Trusted Third Parties for the Provision of Encryption Services" (1997) <http://dev.abanet.org/scitech/ec/isc/ukkeyr1.html>.

[563] Cyber-Rights & Cyber-Liberties (UK), First Report on UK Encryption Policy 12 (May 30, 1997) <http://www.leeds.ac/uk/law/pgs/yaman/ukdtirep.htm>

for keys would present an irresistible target for theft by intruders.[564]

[564] Id. at 19.

3. STRATEGIC ANALYSIS3.STRATEGIC ANALYSIS3.STRATEGIC ANALYSIS3. STRATEGIC ANALYSIS

This section will analyze the uniformity of existing and likely regulatory responses in the four Member States to the identified issues of data protection for on-line services. Initially, the section will address divergences among the national laws of the Member States that are significant for on-line services. This analysis will also refer to the potential impact of the transposition of the European Directive on these divergences as well as the transposition of the sectoral ISDN Directive.[565] The section will then turn to an examination of the obstacles to the internal market that remaining divergences may pose. This assessment will identify the type of regulatory obstacles that on-line services will face and will offer specific examples of on-line services confronting regulatory obstacles.

Finally, this section will examine policy options for data protection drawn from infrastructure technologies. The discussion addresses technical solutions for a number of the data protection issues. This section concludes by analyzing options for effective regulatory policy protecting personal information in an on-line environment. The conclusion treats technical infrastructure design as a form of regulatory decision, presents a set of policy instruments that data protection officials might use to participate in crucial technical decision-making, and offers a jurisdictional basis under the European Directive's provision on codes of conduct that might be used to advance such data protection through technical standards.

3.1 Divergences in Member State Law and Transposition of the European Directive and the ISDN Directive 3.1 Divergences in Member State Law and Transposition of the European Directive and the ISDN Directive 3.1 Divergences in Member State Law and Transposition of the European Directive and the ISDN Directive 3.1 Divergences in Member State Law and Transposition of the European Directive and the ISDN Directive

---

[565] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunictions sector, O.J. L24 (30 Jan. 1998).[Hereinafter ISDN Directive].

In each of the five threshold areas discussed above, the Study shows that some similarities exist in the doctrine that is evolving within the Member States for the treatment of personal information in the on-line environment. But, nevertheless, divergences among these Member States exist in the interpretation and application of the basic data protection principles. These divergences have potential significance for the structure and development of on-line services.

3.1.1 Jurisdictional Scope of «Personal Information»3.1.1 Jurisdictional Scope of «Personal Information»3.1.1 Jurisdictional Scope of «Personal Information»3.1.1 Jurisdictional Scope of «Personal Information»

While each of the Member States offer protections for personal information, whether directly or indirectly nominative, the interpretation of when information relates to an «identifiable» person is not uniform. These differences create important ambiguities in the application of data protection laws to critical on-line information such as IP addresses. For example, the United Kingdom looks at a contextual analysis that emphasizes whether the identity of the individual can be established «from [the data] itself and other information *in the possession of* the data user.»[566] French law appears to take a broader approach to the notion of an «identifiable individual» and will examine whether it is at all *possible* to trace the information back to an individual in order to assure protection in the event that linkages are made.[567] Belgian law even goes in an opposite direction, in some instances, and excludes a number of types of otherwise qualifying «personal information» from protection, such as data made public by the person concerned.[568] In contrast, Germany has explicit rules set out in the new Information and Communications Services Act, the IuKDG, that spell out a requirement for anonymous and pseudonymous interactions.[569] The specific

---

[566] Data Protection Registrar, Data Protection and the Internet, <http://www.open.gov.uk/dpr/internet.htm> (1997) (emphasis added).

[567] See 2.1.2

[568] See 2.1.1. The data is only excluded from the protection of the statute if the purpose for the public disclosure is respected. If the purpose for the disclosure is respected, the law's protections, such as notice of use, rights of access and error correction, will not apply.

[569] See 2.1.3.

German rules also apply certain data protection rights, such as access to stored data, to pseudonymous information.[570]

These ambiguities across the Member States' national laws raise an important issue for the structure of data flows. The complexity and flexibility of data flows for on-line activities can present an overwhelming array of concerns and problems for data protection. These data protection concerns might become more manageable if information were segmented into «identifiable» and «unidentifiable» data. The emphasis in the Member States on anonymous and pseudonymous interactions reflects this conceptual approach.[571] In practical terms, the case studies also show that the commercial arrangements for the collection of data and the types of data that are collected in on-line contexts have significant variation and may be structured to avoid the provision of identifying information to many of the intermediary participants.[572] Yet, few interactions will truly be considered anonymous if the technical capacity to trace information back to an individual results in the legal classification of all such information as relating to an «identifiable» person. To such an extent, data protection principles will apply and will need to be developed in extensive detail no matter how networks configure the data flows.

The transposition of the European Directive will encourage greater convergence for the jurisdictional scope of the data protection principles. The European Directive contains an explanatory recital that interprets «whether a person is identifiable, account must be taken of all the means likely reasonably to be used either by the controller or by any other person to identify said person.»[573] The recital also stipulates that the principles of data protection should not apply to anonymous data.[574] Nevertheless, the European Directive's context-based appreciation leaves room for both narrow and broad understandings as to the difficulty of actually identifying the person about whom information may only relate indirectly. The consequences for data processing are significant if one

---

570 See 2.1.3.

571 See 2.1.1, 2.1.2, 2.1.3, 2.1.4.

572 See Part II.

573 Directive 95/46/EC, Recital 26.

574 Id.

Member State views the data as «personal information» and another does not; data protection law will apply in one, but not in the other Member State.[575]

The transposition of the ISDN Directive is not likely to resolve this remaining divergence. While the ISDN Directive is intended to apply throughout the telecommunications sector,[576] the provisions are drafted with a specificity that emphasizes data protection for telephone and fax communications. The ISDN Directive is silent on the definition of personal information and, thus, defers to the general framework directive for the scope of «identifiable» information.[577] The ISDN Directive does, however, contain special restrictions on «traffic data relating to subscribers and users»[578] and calling-line identification information.[579] Yet, both of these provisions seem to contemplate telephone calls rather than on-line communications. For example, «traffic data» refers to the information processed «to establish calls»[580] rather than to establish «connections» or «communications» which would be more meaningful for the on-line environment. Moreover, if the traffic data relates to a subscriber or a user, then at the conclusion of the call, the data must be erased or rendered anonymous.[581] The ISDN Directive does not offer any guidance to determine whether information would «relate» to a subscriber or user. In any case, the ISDN Directive is silent on the requirements for information to be considered anonymous.

In a similar vein, the calling-line identification provision requires that a calling user have the possibility «to eliminate the presentation of the calling line identification on a per-call basis.»[582] This is does not make sense in the on-line

---

575 See 3.2.2

576 Directive 97/66/EC, Art. 1(1).

577 See Directive 97/66/EC, Art. 1(2) [stating that «the provisions of this Directive particularise and complement Directive 95/46/EC.»]

578 Directive 97/66/EC, Art. 6.

579 Id., at Art. 8.

580 Id., at Art. 6(1).

581 Id.

582 Id., at Art. 8(1).

environment: web useage is not «per-call» and a user's suppression of his IP address would entirely preclude communication on the Internet.[583] Thus, the transposition of these provisions in the ISDN Directive are unlikely to clarify the divergences concerning the scope of «personal information.»

3.1.2 Jurisdictional Scope of Registration and Supervision3.1.2 Jurisdictional Scope of Registration and Supervision3.1.2 Jurisdictional Scope of Registration and Supervision3.1.2 Jurisdictional Scope of Registration and Supervision3.1.2 Jurisdictional Scope of Registration and Supervision

The analysis of registration requirements illustrates a number of common features among the Member State laws, but also shows significant differences in the territorial reach of those laws. In each of the Member States, anyone processing personal information must generally notify a supervisory authority.[584] However, certain activities may be either exempted from the declaration requirement, as is the case in Belgium, or subject to simplified procedures, as is the case in France. For foreign on-line service sites, the territorial scope of Member State laws are not identical. Under present British law, the location where data is stored will likely determine the applicability of the Data Protection Act.[585] Foreign web sites, for example, appear unlikely to fall within the obligation to register in the United Kingdom. By contrast, France and Belgium appear poised to treat the foreign web sites that collect information from within their respective countries as under the subject matter jurisdiction of their respective national data protection law.[586] In Germany, however, it is unclear whether foreign web sites must register with supervisory authorities.[587]

The formalities of registration with national authorities also reveal a

---

583 In the on-line environment, the anonymity desired by blocking CLI may be achieved by the use of an anonymizer. However, an anonymizer still transmits an IP address, just not that of the ultimate user.

584 See 2.2.1, 2.2.2, 2.1.3, 2.2.4.

585 Data Protection Act 1984, _ 39 (excluding application of the Act to data held outside the United Kingdom).

586 See 2.2.1, 2.2.2.

587 See BDSG, art. 32; IuKDG, art. X.

number of important differences. First, the content requirements for notification to national data protection authorities vary somewhat across the Member States. For example, France requires the declaration of the origin of any stored data,[588] Belgium does not, [589] and the United Kingdom asks for free text descriptions for on-line services.[590] Second, the manner of permissible registration differs. Belgium and the United Kingdom, for example, accept electronic registration notices; France and Germany do not. And, lastly, registration fees illustrate disparities among the Member States. For example, in Belgium the fee varies based on the number of people about whom the processing relates and the manner of filing, while in the United Kingdom a unitary fee applies. These divergences may have an effect on how companies structure the architecture of their network activities.

The European Directive seeks to harmonize the territorial application of Member State data protection laws.[591] The choice of law rules contained in the European Directive stipulate that each Member State shall apply its law when:

> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State...;
> (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
> (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of said Member State, unless such equipment is used only for purposes of transit through the territory of the Community. [592]

---

[588] Loi No. 78-17 du 6 janvier 1978, art. 19.

[589] Loi du 8 décembre 1992, art. 3.

[590] Data Protection Registrar, Data Protection and the Internet: Guidance on Registration (1997), <http://www.open.gov.uk/dpr/internet.htm>.

[591] The ISDN Directive contains no provisions to clarify or supplement the general directive's impact on territorial divergences.

[592] Directive 95/46/EC, art. 4(1).

For data processing within the European Union, the European Directive strives to create a choice of law that is exclusive in order to prevent overlapping rules and place limits on the territorial reach of the data protection laws of the Member States. The relevant recitals in the European Directive note that «the processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State.»[593] However, the recitals also warn that «within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive.»[594] In the on-line environment, the implementation of this choice of law provision is unlikely to be simple.[595]

At the same time, for data processing outside the European Union, the European Directive's choice of law provision also seems to ratify the more extensive reach of the French and Belgian laws. Presumably any information of European Union origin that is transmitted outside the Union will, by virtue of the last clause in the choice of law provision, be subject to the substantive law of the Member State of origin; the «use of equipment» within a Member State for processing the information, such as any hardware for transmission of information, confers jurisdiction on the laws of that Member State for the data. An ambiguity in the official translations of the European Directive does introduce, however, a significant potential for divergence. In the French text, Member State law applies to processing in third countries if «means» (*moyens*) are used within the Member State.[596] In the English text quoted above, the same clause refers to «use of equipment» within the Member State.[597] It is not clear that «means» and «use of

---

[593] Id., at Recital No. 18.

[594] Id., at Recital No. 9,

[595] See infra _ 3.2.1. For example, under the European Directive's choice of law provision, many data controllers are likely to be «established» in more than one Member State. If a web site places cookies on a user's computer, the web site will most likely be treated as having an «establishment» at the location of *each* user. The Recitals note that «establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements.» Directive 95/46/EC, Recital No. 19. Cookies make use of the user's computer through stable arrangements at the user's location and constitute effective and real activity. Thus, a web server located in one Member State placing and recovering cookies on a personal computer located in another Member State must be considered to have an «establishment» in the second Member State.

[596] Directive 95/46/EC, art. 4(1)(c).

equipment» are perfectly equivalent terms.

The transposition of the European Directive will also promote some convergence in terms of the content of registration statements. The European Directive stipulates a set of disclosures that constitute the minimum information that must be contained in notifications made to the supervisory authorities[598] and provides for certain exemptions or simplification of notification in particular situations.[599] The sectoral-specific rules found in the ISDN Directive do not, however, provide further convergence for notification of processing in the context of telecommunications services. The ISDN Directive is silent on registration statements.[600] Yet, for on-line services, additional registration requirements imposed by one Member State, such as notification of the duration of storage and the means by which individuals are given notice of the processing,[601] introduce a potentially significant burden when rapidly changing, interactive on-line services are provided throughout the European Union. A similar burden occurs if one Member State chooses to grant a simplification or exemption from notification for particular processing, but another Member State does not.[602] In both instances, the user of personal information will be subject to differing administrative requirements.

On a number of these key points of divergence, the European Directive is silent. For example, the European Directive contains no stipulation as to the manner of registration-- paper versus electronic filing.[603] Likewise, the ISDN Directive is also silent on this point.[604] For on-line services operating exclusively

---

[597] Id.

[598] Id., art. 19(1).

[599] Directive 95/46/EC, art. 18(2).

[600] See Directive 97/66/EC.

[601] These content requirements, for example, exist in Belgian law, but not in the European Directive. *Compare* Loi du 8 décembre 1992, art. 17(3) *with* Directive 95/46/EC, art. 19(1).

[602] For example, France has established a list of simplified declarations that is similar, but not identical to the norms adopted by Belgium.

[603] See Directive 95/46/EC, art. 18(1).

[604] See Directive 97/66/EC. The ISDN Directive is entirely silent on registration for on-line services.

on the Internet, the manner of notification to supervisory authorities, and in particular the manner of updating notifications, has a number of implications for internal operations that are likely to have an impact on compliance rates for on-line services. As a practical matter, the national authorities seem to be moving in the direction of electronic registrations, which are already accepted in Belgium and in the United Kingdom. Yet, until all Member States permit electronic registrations, the divergence between paper and electronic filings will have an adverse impact on on-line services.

Finally, on the issue of notification fees, the European Directive does not promote any convergence. No provision in the European Directive sets a fee schedule.

3.1.3 Transparency3.1.3 Transparency3.1.3 Transparency3.1.3 Transparency

The Member States have each begun to address the application of national rules for transparency to on-line services. In these preliminary stages, a number of differences in existing doctrine have emerged that appear to have particular significance for on-line services.

While each Member State requires that notice be given to individuals, the scope of the obligation itself, the form and the content, is not uniform. With respect to the scope of the obligation, an important difference emerges for the responsibility of data collectors. In France, for example, notice is only required if information is collected directly from an individual.[605] In Belgium, on the other hand, notice is required both from direct and indirect collectors of personal information.[606] Germany does not differentiate between direct and indirect collection; the IuKDG contains strong notice provisions. These differences among Member States affect the obligations of on-line service providers profoundly because personal information in the on-line environment can readily be collected indirectly rather than directly. For example, clickstream information collected by a web site about a visitor's use of the site is actually obtained from the visitor's Internet service provider and not directly from the visitor.

The type of notice similarly presents a number of issues. While the basic

---

605 See 2.3.2.

606 See 2.3.1.

content of the required notice is similar across the Member States, a number of differences appear that are highly relevant for on-line services. For example, a French notice must contain among its disclosures information about the significance of the collected information, namely whether the collection of particular information is mandatory or voluntary, and the identity of any recipient of the collected personal information.[607] Belgium, however, asks for somewhat distinct information in the notice to individuals, namely that the finality be specified in the notice and that the existence of the public register of processing declarations be indicated.[608] Germany also has specific obligations to notify individuals if «cookies» will be used during Internet sessions, to notify of any re-forwarding of personal information, and to notify of options for anonymous interactions.[609] For the rapidly changing on-line environment, these particular elements of notice may require frequent revision of notice statements by collectors of personal information.

With respect to an individual's consent and right of opposition to data processing, the United Kingdom subsumes consent under «fairness.»[610] There, the Data Protection Registrar has called for a contextual analysis and positive consent in some specific circumstances.[611] While law in the United Kingdom has generally preferred opt-out, the Data Protection Registrar appears likely to expand positive consent requirements for on-line services.[612] Germany takes this idea a step further and has elaborated specific rules for consent with respect to «cookies» and has otherwise mandated strong positive consent in the on-line environment.[613] France has, also, approved a number of opt-out consents for Internet services

---

607 See 2.3.2.

608 See 2.3.1.

609 See 2.3.3.

610 See 2.3.4.

611 See 2.3.4.

612 See 2.3.4.

613 See 2.3.3.

(specifically, directory listings and message boards).[614] Nevertheless, French law requires advanced written consent for the processing of sensitive data.[615] In contrast, Germany expressly permits consent through on-line means.[616] These disparities may mean that different consent requirements may apply to a single on-line service provided across the Member States.

For the exercise by data subjects of their right of access to personal information, both the form and scope of access have some notable differences across the Member States. In Germany, for example, electronic access to personal information by data subjects is permissible. The United Kingdom appears to moving in this direction. By contrast, however, Belgium does not yet appear to have significant taken steps to permit electronic access to personal data by data subjects. Similarly, the scope of the access right may develop with significant variance across the Member States. Finally, some ambiguity may exist in the United Kingdom with respect to the full extent of the controller's obligation to provide access to information originating from that controller's web server. Such an obligation may also be present even if the information no longer resides on that web server.[617]

In addition, fees for access by data subjects to their personal information varies. In Germany, for example, the new teleservices law requires that access to on-line information must be offered free of charge.[618] In the other Member States, charges apply such as the 100BF (2.5ECU) fee charged in Belgium and the _10 (15 ECU) fee charged in the United Kingdom. This difference can affect where and how an on-line services participant designs the system architecture.

The transposition of the European Directive will have an incomplete effect on some of these divergences. The European Directive mandates that notice be provided to an individual when information is collected either directly or indirectly

---

614 See 2.3.2.

615 See 2.3.2.

616 See 2.3.3.

617 See UK Data Protection Guidance for Direct Marketers, p. 37 (1995).

618 IuKDG, at art. 2, _ 7.

from that person.[619] This harmonization requirement resolves one existing scope issue; collectors of personal information must provide notice whether the collection is directly or indirectly from the individual. However, the European Directive only stipulates the minimum content that Member States must require in notices provided to individuals.[620] Although these minimum content elements appear to combine different requirements in existing national law, additional points may still be imposed by Member State law, such as Belgium's required disclosure of the register of public declarations.

For divergences over consent and opposition, the European Directive contains some obligations that address these issues.[621] However, the European Directive does not provide criteria or a mandate for distinguishing between opt-in and opt-out consent. The exception to this silence is the explicit right to object to direct marketing uses of personal information.[622] In effect, this provision for direct marketing authorizes at least an opt-out regime.

The European Directive is also silent on the issue of on-line consent and on-line opposition to the processing of personal information. Although the on-line context increases the ease and efficiency of opt-in possibilities, the continued ability for the Member States to diverge on the permissibility of on-line consent and opposition is likely to have a real impact on the cost of on-line services and the management of those services. The ISDN Directive, while requiring consent for processing of telecommunications call traffic data[623] and an opt-out for the on-line availability of a subscriber directory,[624] is similarly silent on the means for obtaining the consent or exercising an opt-out.

As the European Directive is transposed in the Member States, the new Member State laws may not resolve all the issues pertaining to the form and the scope of access rights. The European Directive merely stipulates that the Member

---

619 Directive 95/46/EC, art . 10-11.

620 Directive 95/46/EC, art. 10-11.

621 Directive 95/46/EC, art. 7 (consent) and art. 14 (objection).

622 Directive 95/46/EC, art. 14(b).

623 Directive 97/66/EC, art. 6(3).

624 Directive 97/66/EC, art. 11(1).

States grant a right of access to the data subject against the controller.[625] The European Directive does not address whether on-line access should be permitted nor does the European Directive say anything about the potential responsibility of the original controller for access against subsequent controllers. The same is true of the ISDN Directive. The sector-specific rules are silent regarding on-line access and access through intermediaries for information processed by third-parties.

Finally, the European Directive is silent on the amount of any fee that may be charged for the data subject's access. Although the text of the European Directive stipulates that «Member States shall guarantee every data subject the right to obtain from the controller: ... without constraint at reasonable intervals without excessive delay or expense,»[626] there is no indication as to the fee amount that might constitute an «excessive expense.»[627] The transposition of the European Directive will, thus, not in itself address this issue that may affect how data flows are structured and how information may be storage by on-line services. Likewise, the ISDN Directive does not deal at all with the fees for data subject access.

3.1.4 Profiling and Sensitive Data3.1.4 Profiling and Sensitive Data3.1.4 Profiling and Sensitive Data3.1.4 Profiling and Sensitive Data

National data protection doctrines as they already exist and as they are likely to be applied to on-line services raise a number of issues vital to electronic commerce. In particular, user profiling, as shown in the case studies,[628] plays a fundamental economic role in shaping on-line activities. Yet, data protection laws remain unsettled in their treatment of profiling practices for on-line services. In France and Belgium, profiling is an issue of finality. On-line services must provide

---

625 Directive 95/46/EC, art. 12.

626 Directive 95/46/EC, art. 12.

627 See Directive 95/46/EC, Recital 41. While a literal interpretation of this clause might suggest that the European Directive requires the Member States to ban any charge for access to personal information, the recital provides no support for such an interpretation.

628 See Part II.

clear notice of any profiling activities. In the United Kingdom, profiling is an issue of fairness, and the Data Protection Registrar has not yet settled the application of the fairness principle to service providers and web sites. By contrast, in Germany, profiling is subject to specific rules that permit profiling only under the condition that pseudonyms are used. These requirements in existing Member State law raise serious questions with regard to the permissibility of using search engines and intelligent agents.[629] For example, a search request to find web sites and message board postings will often create a profile of particular individuals through the indirect collection of personal information. The user of the search engine acts as the data controller and would be required to comply with all applicable data protection laws provisions on notice and consent, though the user may not learn the identity of the profiled individual until the profile comes into existence.

In addition, the Member States, while each requiring that only relevant data be collected for the contemplated uses, arrive at a requirement of data minimization somewhat differently. France achieves minimization through purpose limitations. The United Kingdom has recently argued for technical design requirements to accomplish data minimization. And, Germany has recently adopted an express statutory provision that calls strictly for data minimization. With these different starting points, the interpretation of relevancy may differ for the same on-line service provider within all of the Member States; one Member State may view specific information as relevant for the intended purpose, while another Member State does not.

Another important profiling issue arises in the context of anonymous interactions. In Germany, the IuKDG explicitly requires on-line interactions to be anonymous to the greatest extent possible.[630] This new German statute also applies special data protection rules to pseudonymous information.[631] The other Member States also appear to encourage the use of non-identifiable information. Outside of Germany, however, truly anonymous information is not likely to fall within the scope of data protection law.[632] Moreover, in Belgium and France, the

---

[629] See 2.4.2 (discussion of automated decision-making restrictions and collaborative filtering).

[630] See 2.4.3.

[631] See 2.4.3.

[632] See 2.1.

broad scope of the definition for «identifiable» information will increasingly necessitate judgmental decisions as to the applicability of data protection law. The United Kingdom will similarly face interpretive decisions for on-line data to determine if such data are 'personally identifiable'; however, the United Kingdom appears to be making a narrower interpretation of this term than Belgium and France. As a result, different Member States are likely to have varying standards for anonymizing information.

In the context of processing and profiling sensitive data for on-line services, the Member States have focused somewhat differently on the form that consent is to take. Germany explicitly permits electronic consent provided that specific conditions to protect the informed and voluntary nature of the assent are satisfied. The United Kingdom is considering a possible future decree on electronic consent. In contrast, France has a stringent doctrine favoring written consent, while Belgium does not appear to have addressed the particular issue.

The transposition of the European Directive as well as the ISDN Directive will provide some additional certainty for the disposition of profiling and the treatment of sensitive data in an on-line context. The European Directive contains specific provisions for marketing practices,[633] but does not expressly cover profiling in the sense that the German law explicitly establishes processing rules. Similarly, the European Directive does not definitively resolve the judgments that will inevitably need to be made concerning the scope of «identifiable» information.[634] Finally, as noted above, the European Directive will not resolve the issues of the form of consent by individuals for profiling or the treatment of sensitive data.[635] In contrast, the ISDN Directive does specifically condition the use of subscriber billing data for marketing purposes on the subscriber's express consent[636] and requires that subscribers be able to indicate in directory listings that personal information may not be used for direct marketing purposes.[637] For on-line services, the restriction on billing data will have a harmonizing effect, but will

---

633 See, .e.g., Directive 95/46/EC, art. 14(b).

634 See 3.1.1.

635 See 3.1.3.

636 Directive 97/66/EC, art. 6(3).

637 Directive 97/66/EC, art. 11(1).

not cover the full range of clickstream information, and the directory clause of the European Directive will harmonize the creation of differentiated listings throughout the Member States.

3.1.5 Security3.1.5 Security3.1.5 Security3.1.5 Security

As illustrated previously, the success of electronic commerce initiatives depends on information security.[638] The Member State's data protection laws and interpretations generally encourage the use of encryption to protection personal information. However, a number of opposing legal rules exist for the techniques that might be used to secure information on the Internet. Within the Member States, key escrow remains an open and sensitive issue. France, while purporting to liberalize its encryption rules in 1996, will require the licensing by the government of trusted third parties who provide encryption services.[639] French authorities still have not issued the implementing decree setting out the criteria for licensing. Germany does not restrict encryption, but has established voluntary licensing for trusted third parties; these licensed trusted third parties will be required to release encryption keys to law enforcement authorities in possession of a warrant.[640] Belgium and the United Kingdom are each considering proposals for key escrow schemes. At the same time, in Belgium and Germany, the laws also require telecommunications carriers to maintain «wiretap-ready» systems for law enforcement access.[641]

The transposition of the European Directive and ISDN Directive are unlikely to be dispositive for the encryption debate. The European Directive, like the Member State laws, contains a clause requiring that the Member States provide that the controller «must implement appropriate technical and organizational measures to protect personal data ... in particular where processing involves transmission over a network ... [h]aving regard to the state of the art and the cost

---

638 See Parts I & II.

639 See 2.5.2.

640 See 2.5.3.

641 See 2.5.1.

of their implementation.»[642] The ISDN Directive similarly requires:

> The provider of a publicly available telecommunications service must take appropriate technical and organisational measures to safeguard security of its services .... Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.[643]

However, both the European Directive and the ISDN Directive exempt processing of personal data that concerns public security and «the activities of the State in the areas of criminal law.»[644] Since the heart of the encryption debate revolves around law enforcement's access to encrypted information, the European Directive's security requirements will be limited by the legal competence of the Community to act on matters involving state security and law enforcement. The same limitation applies to the ISDN Directive.

3.2. Obstacles to the Internal Market3.2. Obstacles to the Internal Market3.2. Obstacles to the Internal Market3.2. Obstacles to the Internal Market

The divergences in data protection among the Member States that the transposition of the European Directive and the ISDN Directive are unlikely to resolve for the on-line environment raise a series of important obstacles to the Internal Market. The selection of applicable law in itself offers a number of persistent issues for the development of on-line services. While many of the divergences appear to be within the «margin of manoeuvre» for the Member States permitted by the European Directive, these ostensibly slight differences in protection of personal information can result in dramatic consequences or create strong pressures on developers of on-line services as well as users of those services.

---

642 Directive, 95/46/EC, art. 17(1).

643 Directive 97/66/EC, art. 4(1).

644 Directive 95/46/EC, art. 3(2); Directive 97/66/EC, art. 1(3).

3.2.1 Applicable Law3.2.1 Applicable Law3.2.1 Applicable Law3.2.1 Applicable Law

The significance of divergences in the treatment of personal information in the context of on-line services will be influenced by the choice of applicable law. If multiple data protection laws apply to the same on-line service activity, then any divergence between the laws imposes an inherent conflict in the applicable rights and responsibilities for data protection. Permissible activities in one jurisdiction, such as the processing of log files without registration, may be prohibited in another. In an effort to avoid these obstacles, the European Directive strives to exclude overlapping jurisdiction of the Member States for data protection matters. The European Directive provides a specific choice of law provision that selects the law of the Member State where the controller is established.[645] The European Directive also provides that «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[the fundamental rights and freedoms of freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data].»[646] The European Court of Justice has recognized that home state supervision may be exclusive.[647]

Nevertheless, the recitals in the Directive explicitly recognize that «Member States will be left a margin for manoeuvre ....[and] within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of this Directive, and this could have an effect on the movement of data within a Member State as well as within the Community.»[648] Under the European Directive's choice of law provision, a controller is subject to the law of each Member State where it is «established.»[649] As explained in the Recitals, a Member State's law thus applies if there is «effective and real exercise

---

645 Directive 95/46/EC, art. 4.

646 Directive 95/46/EC, Art. 1(2).

647 See, e.g., Konsumentombudsmannen (KO) v. DE Agostini (Svenska) Forlag AB, Cases C-34 to 36/95, [1997] ECR I- (July 9, 1997).

648 Directive 95/46/EC, Recital No. 9.

649 Directive 95/46/EC, art. 4(1)(a)

of activity through stable arrangements.»[650] This definition of «establishment» suggests that the systematic collection of information from within any Member State using servers or other computing equipment within the Member State may be treated as an «establishment.» The use of cookies, for example, creates an establishment wherever the user is located since interaction with the user's hard drive is a stable arrangement located at the site of the user that provides effective and real exercise of activity for the controller who places the cookie. In effect, the controllers operating in the on-line environment may typically be deemed to be established in several Member States for the same on-line activity. As a result, several data protection laws may apply to various aspects of an on-line service. Notification of cookies must, for example, comply with the notice requirements of the place where the user is located, while the server's processing must comply with the requirements of the law where the server is located.

The uniform choice of law rule that the European Directive requires will still not displace all possible territorial overlaps. Under the jurisdictional doctrine of the European Court of Justice,[651] home country supervision for data protection would not preclude independent regulation of the treatment of personal information for other goals such as consumer protection.[652] For example, the crucial data protection provisions for on-line services in Germany arise under the Teleservices Data Protection Act. As such, these provisions might be applied regardless of the European Directive's choice of law rules.

In addition, the European Directive does not displace any provisions of criminal law.[653] To the extent that Member States include data protection offenses within their criminal law, those criminal laws may apply to acts undertaken within the Member State regardless of the European Directive's preferred choice of law. For example, France's penal code criminalizes the «act of collection of data by fraudulent, unfair or illegal means, or to undertake processing of nominative information concerning physical persons who have opposed such

---

650 Directive 95/46/EC, Recital No. 19.

651 See Konsumentombudsmannen (KO) v. DE Agostini (Svenska) Forlag AB, Cases C-34 to 36/95, [1997] ECR I- (July 9, 1997).

652 The recitals also make this clear. See Directive 95/46/EC, Recital 71.

653 Directive 95/46/EC, art. 3(2). Criminal law is outside the scope of competence of Community law.

processing, when such opposition has a legitimate basis.»[654] French criminal law also specifies that, in the absence of an individual's express consent, the storage of nominative information directly or indirectly revealing racial origins or political, philosophical or religious beliefs, union membership, or personal morals is a crime.[655]

In terms of the Internal Market, the effort to provide an exclusive choice of law and the possibility that overlapping jurisdiction may still occur raise substantial incentives for developers of on-line services to try to circumvent particular data protection rules through infrastructure architecture. The on-line environment is geographically flexible. Controller's functions may be disaggregated and routed to take advantage of differences in the «margin of manoeuvre» among the Member States. For example, a French on-line service provider may allocate dynamic IP addresses on equipment located in the United Kingdom to try to avoid the applicability of French data protection law for the recipients of those IP addresses. Under this scenario, United Kingdom law would apply to the IP addresses allocated by the British server and might result in the IP addresses falling outside the scope of data protection for the recipients of those addresses.[656]

3.2.2 Specific Examples3.2.2 Specific Examples3.2.2 Specific Examples3.2.2 Specific Examples

The applicable law and divergences within it manifest themselves as obstacles to the Internal Market in three particular types of cases. First, regulatory responses to on-line services may result in the prohibition of certain services in some, but not all Member States. Second, data protection rules may impose additional difficulties on the provision of particular services in some, but not all Member States. And lastly, the differences may result in the distortion of competition in the development of on-line services across the Member States. This section will address each of these types of obstacles to the Internal Market.

3.2.2(a) Prohibition on the Provision of Services

---

654 Code pénal, art. 226-18.

655 Code pénal, art. 226-19.

656 See infra _ 1.3.4.

As previously reported,[657] electronic transactions are growing rapidly through the use of web sites for both the dissemination of product information and execution of sales transactions.[658] These sites run the significant risk of facing prohibitions on the collection of transaction data in some member states, but not others. For example, on-line bookstores will face inherent obstacles. Certain book titles along reveal sensitive data about those who purchase them. Moreover, on-line bookstores will typically use a «shopping basket» feature and place «cookies» on the buyer's hard drive without regard to the location of the buyer. These «cookies» enable the bookstore's web site to keep track of the buyer's purchases for billing.

If a user in France were to purchase books from an on-line bookstore in the United Kingdom such as *Catechism of the Catholic Church, Becoming Catholic: Even if you happen to be one* and *Raising Catholic Children*, the titles alone would be sensitive data. In France, the collection of such sensitive information requires express written consent under both the data protection statute and the criminal law. The bookseller, in this case, would violate French law by processing the transaction. Yet, the bookseller in the United Kingdom would not become aware of the problem until after the transaction were processed. In the United Kingdom, however, the transaction is permissible as no additional requirements have yet been imposed on the processing of sensitive data.[659] Because «cookies» are used by the bookseller from within France, under the European Directive's choice of law rule,[660] the bookseller will be established for purposes of application of the French data protection law. At the same time, the bookseller is a «controller» subject to British law.

A similar problem arises for the development of on-line services that rely heavily on advertising revenue generated by third-party advertisements placed on web pages through entities such as DoubleClick. In a typical arrangement, the

---

657 See Rapport No. 1: Situation Globale; Rapport No. 2: Etudes de cas

658 The FNAC in France and Burton's in the United Kingdom are two such prominent sites.

659 See 2.4.4.

660 See Directive 95/46/EC, art. 4(1).

web site contracts with an advertising agency who in turn collects information from the «hits» to place an appropriate advertisement on the user's display. For at least one advertising agency, the information used to make the advertisement selections involves IP addresses and patterns from previous visits through «cookies.» This collected data, however, does not include the specific identity of the user. If, in the case of the bookseller, a British server were used by the advertising agency, the service would face serious obstacles depending on the European country where the on-line shoppers were located. Under the British data protection law and doctrine, the agency might not be subject to data protection law because of the difficulty identifying the individual from the information that is being processed.[661] However, under the French and Belgian doctrines, the IP address information combined with the «cookies» data providing the previous visit patters would likely be treated as «personal data.»[662] As a result, in those Member States, the collection of information from users within those states by the advertising agency would be prohibited without the required notices to the individuals and the data protection authority.[663]

Other like examples might be found in the use of search engines or information harvesting methods. For instance, the German Teleservices Data Protection Act, unlike the data protection laws of the other Member States, prohibits the creation of profiles unless strict limitations are respected. Generally, German law requires that profiles be pseudonymous.[664] Since this requirement is not found in the laws of the three other Member States analyzed in this Study nor in the European Directive, the divergence threatens the legality of the use of search engines on the Internet. Search engines are not presently designed to create only pseudonymous profiles.

3.2.2(b) Difficulty in provision of services

Short of an outright restriction on the provision of particular on-line

---

661 See 2.1.3; 2.1.4.

662 See 2.1.1; 2.1.2.

663 See 2.2.1; 2.2.2; 2.3.1; 2.3.2.

664 IuKDG, art. 2, _ 4(4).

services, diverging data protection laws may create serious difficulties for the offering of on-line services throughout the European Union. Such difficulties can in turn raise obstacles to the Internal Market. Several examples illustrate these basic difficulties for critical features of on-line services. In Germany, on-line service providers must offer users various kinds of anonymous or pseudonymous options.[665] Other Member States have not set similar requirements. Hence, an Internet service provider must either offer the German options throughout the European Union or differentiate services for subscribers within Germany.

For robust electronic commerce to develop across Europe, digital signatures and certification of those signatures are widely viewed as essential. The evolution of these services in the Member States also face data protection difficulties. The German teleservices law contains special provisions for digital signatures and the collection of personal information related to signature certification, notably that data may only be collected directly from the individual concerned unless consent has been granted for collection from third-parties.[666] Other Member States have not developed comparable requirements. Thus, the use of digital signature certificates in Germany will be subject to special data protection provisions that are not found elsewhere in the Member States.

3.2.2(c) Distortion of the provision of services

Even if divergences in data protection among the Member States do not result in an outright prohibition or major difficulty with respect to the provision of on-line services, the divergences may still present obstacles to the Internal Market. In particular, the divergences may lead to distortions in the structural arrangements for on-line services. Network technology is extremely flexible and allows service providers to locate their information processing activities in various jurisdictions as well as to disaggregate components of their services for distinct processing activity. The application of Member State data protection laws to particular types of services may, thus, provide incentives for service providers to locate or re-locate their activities depending on how they wish to manage data protection.

A few examples can readily illustrate this distorting effect. The more

---

665 See 2.3.3.

666 See 2.5.3.

restrictive interpretation of information relating to an «identifiable» person found in the United Kingdom and Germany[667] suggests that ISPs will have an incentive to locate their address servers within those Member States. To the extent that those Member States would not treat dynamic IP addresses as «personal information» for web recipients, the ISP minimizes the applicability of data protection law, though in Germany the Teleservices Data Protection Act would apply. Similarly, the harvesting of e-mail addresses, which is desired by marketing firms, has the best chance of avoiding the requirements of data protection law in Member States such as the United Kingdom where such information will only be treated as nominative information if the recipient can reasonably make the identifying link.[668]

From the perspective of the user, these distortions are particularly troubling. The infrastructure arrangements in an on-line environment will often be unknown to the user, yet these arrangements may have a critical impact on the degree of data protection for the user's personal information. This is especially true for users from Member States such as France or Belgium that treat data protection more expansively than others. These users legitimately expect a certain degree of protection when engaging in information exchanges from their home countries, yet may be surprised to discover that the infrastructure situates the processing in a Member State with narrower protections. For example, a German user who expects that any clickstream profiling by the ISP will be done on an anonymous basis may be surprised to discover that the ISP has located clickstream profiling on a British server in an attempt to avoid the application of the German rule.

3.3 Technical Solutions and Regulatory Policy3.3 Technical Solutions and Regulatory Policy3.3 Technical Solutions and Regulatory Policy3.3 Technical Solutions and Regulatory Policy

The divergences in Member State law and the obstacles to the Internal Market reflect the complexities and difficulties of applying data protection to on-line services. These challenges to the protection of privacy raise two sets of options for regulatory policy. One set of options depends upon technological rules to establish data protection. This technological approach offers both advantages

---

667 See 2.1.3; 2.1.4

668 See 2.1.3; 2.1.4

as well as drawbacks. The second set of options looks to an effective regulatory policy that would combine a range of traditional legal policy objectives with non-traditional regulatory instruments to achieve data protection.

3.3.1 Technical Solutions3.3.1 Technical Solutions3.3.1 Technical Solutions3.3.1 Technical Solutions

Just as technology may be part of the problem for data protection, the technological infrastructure may also form part of the solution. Technological rules are becoming a key source of regulation in a network environment.[669] The Internet's architecture is dynamic and will continue to change. The architecture of the Internet can and should be developed in a way that promotes data protection goals.

To some extent, technological solutions may be able to minimize any conflicts over some of the divergences in the laws of the Member States. Anonymity can serve to protect citizen's rights and interests. If the network can be structured so that anonymity may be maintained for certain activities, but not others, then the infrastructure will contain a degree of flexibility that may offer a robust means to assure data protection in a complex, on-line environment.

Otherwise, technical solutions might be used to smooth over divergences among Member State laws. For example, the variations in the content of registration and user notice are susceptible to automated information brokering. Specifically, technical tools such as intelligent agents could be designed to streamline the process of filing registrations and providing notice. Such agents might match information about a site's practices with the particular disclosures required by the applicable law. Browsers might, for example, provide a default notice when personal information is transmitted, such as the security warning that often appears when an «insecure» document is accessed or transmission is attempted.[670] Similarly, an automated process might alleviate potential difficulties

---

[669] See Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 TEXAS LAW REVIEW 553 (1998); Lawrence Lessig, Reading the Constitution in Cyberspace, 45 EMORY LAW JOURNAL 869 (1996); Joel R. Reidenberg, Governing Networks and Rule-Making in Cyberspace, 45 EMORY LAW JOURNAL 911 (1996); M. Ethan Katsh, Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace, 1996 U. CHICAGO LEGAL FORUM 335.

[670] Netscape 3.0, for example, warns of the insecurity of certain activities or sites when a user is engaged in an on-line transaction.

with registration filings. For example, if automated registration is permitted, program routines can be developed to allow a real-time compliance system. One such idea might be a program that verifies the existence of a registration statement if information is collected or transmitted to domain names from within the European Union. Should no registration statement exist, the program might proceed first to file an electronic declaration with the appropriate supervisory authority before actually collecting or processing any personal information inbound from the European domain.

On the conceptual level, for a number of years, the data protection commissions in Europe have promoted privacy enhancing technologies (PETS) as a potential solution to data protection concerns. Typically, the PETS solution is an «either/or» response: anonymity or identity. In the on-line context, however, full anonymization may be undesirable in particular circumstances, such as those associated with criminal activity where legitimate reasons exist to identify the individual. Technologies can, however, also be seen as a way to address various concerns in different contexts.[671] An infrastructure may be designed to assure that only relevant information be collected when «identified or identifiable» information is required or may be structured to preclude any processing other than purposes compatible with the original goals for the collection.[672]

In response to pressure both from the enactment of the European Directive and from public hearings in the United States, industry groups are moving forward with a number of technical standards that will affect the design of on-line services. Yet, from a data protection perspective, the emerging standards have important weaknesses. The Open Profiling Standard («OPS»), for example, is a technical standard that enables the easy circulation of personal information between browsers and web sites.[673] As it is conceived, users would enter a profile of their personal information into standard data fields on their browser. Specific items can be tagged to authorize or forbid particular uses. The browser would then disclose,

---

[671] See, e.g., Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 TEXAS LAW REVIEW 553 (1998).

[672] For example, information distributed in a «secure» envelope, such as a cryptolope, precludes uses other than those originally intended by the distributor of the information.

[673] See Netscape Communications Corporation Submission Supplemental Comments V & VI, FTC Consumer Privacy Hearings (June 1997), <http://www.ftc.gov/bcp/privacy2/comments2/netscape.htm>.

to the extent authorized by the user, the profile information to web sites being visited by the user. While this solution has a certain degree of appeal, it also has significant disadvantages. First, the standardization of data fields for profile information can greatly enhance data matching. Second, the implementation of OPS may discourage protective anonymity since it is likely that browser developers will require users to create profiles as part of the initial browser configuration.

Another noteworthy initiative is being undertaken by the World Wide Web Consortium («W3C»). W3C continues to work on the «P3P» standard that would allow web sites and users to negotiate the privacy preferences for data collected by the web site.[674] The initiative is based on the PICS labeling and filtering technologies developed originally for the problem of Internet pornography. In these types of labeling and filtering initiatives, the design decisions will make fundamental policy choices.[675] As these examples indicate, technical decisions, architectures, and standards can be constructed to promote data protection goals, but will not automatically do so.

Technical solutions will not, therefore, be a panacea, and the development of data protection cannot stop because of the emergence of significant technical standards. The implementation by network participants will also be critically important. For example, although Netscape allows users of Communicator 4.0 more control over «cookies» than Netscape 2.0, the default setting for Communicator is to accept all «cookies» placed by web sites and not inform users of these information practices.[676] Where «cookies» are treated as personal information, the default implementation contravenes basic principles of European data protection law. Similarly, the P3P initiative holds tremendous promise for data protection,[677] but to date, the development process has been slow and is not

---

[674] See <www.w3c.org>.

[675] See Joel R. Reidenberg, Lex informatica: The Formulation of Information Policy Rules through Technology, 76 TEXAS LAW REVIEW 553 (1998); Joel R. Reidenberg,*The Use of Technology to Assure Internet Privacy: Adapting Labels and Filters for Data Protection,* LEX ELECTRONICA, <http://www.lex-electronica.org> (Fall, 1997).

[676] Netscape Communications Corporation Submission, FTC Consumer Privacy Hearings (June 1997), <http://www.ftc.gov/bcp/privacy2/comments2/netscape.htm>

[677] See generally, Joel R. Reidenberg,*The Use of Technology to Assure Internet Privacy: Adapting Labels and Filters for Data Protection,* LEX ELECTRONICA, <http://www.lex-

yet at a stage for implementation.

3.3.2 Effective Regulatory Policies3.3.2 Effective Regulatory Policies3.3.2 Effective Regulatory Policies3.3.2 Effective Regulatory Policies

In reviewing the application of data protection laws to on-line services in the Member States, the transposition of the European Directive will not completely address a number of critical issues raised for subject matter and territorial jurisdiction, transparency, profiling, and security. Many of the unresolved issues derive from the particular context of on-line services, namely the existing infrastructure design and current development of electronic commerce applications. Legal harmonization of data protection principles at such a detailed level in a dynamic environment will be cumbersome. In the face of a changing infrastructure, the political considerations will be significant and the length of time necessary to consider the issues and to complete the adoption process for any new directive will be excessively long. For example, the process to adopt and implement the European Directive took eight years from the initial proposal to the date for transposition into the national laws of the Member States-- an extraordinarily long period of time for the rapidly changing on-line environment.

By contrast, the Working Party established under the European Directive [678] appears well suited to consider these questions of divergence. Many of the divergences are susceptible to resolution through consensus on the interpretation of basic principles. For example, guidelines on anonymization of personal information might be drawn up by the Working Party to address the issues of «identifiable» information and data minimization. The Working Party might also address uniformity in the content for notice and registration statements and uniformity in mechanisms to satisfy these requirements electronically.[679]

Yet, policy guidelines standing alone will not be sufficient to assure data protection in the network environment.[680] Technical decisions have a rule-making

---

electronica.org> (Fall, 1997).

[678] See European Directive 95/46/EC, art. 29.

[679] Uniformity in this sense means a standardization of descriptions and type of information required to be disclosed and, in the context of electronic notices or registrations, a technical standard that specifies the data fields and locations.

[680] This combination of techniques is recognized in the current draft of the ISDN Directive. See Common Position (EC) No. 57/96 adopted by the Council on 12 September 1996

capacity and, consequently, have fundamental regulatory implications for the types of personal information circulating on the Internet and for the ways such information is processed.[681] The technical infrastructure arrangements for on-line data flows may enhance or frustrate data protection principles. At the same time, data protection rules may themselves cause unintended infrastructure arrangements. If Germany requires explicit notice of «cookies» and Belgium or the United Kingdom does not, then service providers may seek to locate processing activities in Belgium or the United Kingdom.

For the on-line environment, the most effective approach for fair information practices will combine substantive data protection rules and principles with technical arrangements that allow the most efficient and least intrusive compliance. On-line services will increasingly require technical and regulatory differentiation. A few key technical design principles have already been identified by the Berlin Group of national data protection supervisory authorities:

- sensitive data must be encrypted
- information and communications technologies must enable users to control and give feedback with regard to his personal data
- anonymous access to on-line services should be available
- secure encryption methods must be a legitimate option for Internet users
- «quality stamp» certification should be explored to improve transparency for users.[682]

These principles reflect that technical arrangements might narrow the scope of issues faced by legal regulation. For example, to the extent that access to on-line

---

with a view to adopting Directive 96/ / EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector, in particular in the integrated services digital network (ISDN) and in the public digital mobile networks, Recital 7. In addition, the International Working Group on Data Protection in Telecommunications has also stated that «it is mandatory to develop design principles for information and communications technology and multimedia hard- and software which will enable the individual user to control ... his personal data.» Data Protection and Privacy on the Internet: Report and Guidance (Berlin, 19th Nov. 1996).

681 See Joel R. Reidenberg, Governing Networks and Rule-Making in Cyberspace, 45 EMORY LAW JOURNAL 911 (1996).

682 Internet Working Group on Data Protection in Telecommunications, Data Protection and Privacy on the Internet: Report and Guidance (Berlin, 19 November 1996).

services is anonymous, few, if any, issues arise with respect to the collection and storage of transaction records. To maximize this narrowing feature of technical rules, data protection must include as a goal the development of technologies that allow for flexibility in different contexts and a *'marge de manoeuvre'* among the Member States, but also impose mandatory rules on information flows when derogations would violate citizen's rights. This nuanced approach, which uses technical rules to accomplish regulatory objectives, offers data protection officials a robust set of instruments to achieve policy goals.[683] The primary tools are:

(1) persuasion that can be used to pressure industry to develop appropriate technical rules and mechanisms;[684]
(2) participation by data protection officials in the work of standards organizations that can promote mechanisms to assure the policy objectives of data protection;[685]
(3) funding through programs, such as ESPRIT, that may be used to develop technologies that assure data protection;[686]
(4) procurement by public bodies that has a substantial influence on the development of private markets and that may be used as a concerted tool to promote data protection goals;[687]
(5) regulating behavior by imposing liability that can be used as an indirect stimulus for the development of technical rules to assure data protection in network environments;[688]
(6) regulating standards that assures particular data protection rules are

---

[683] See Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 TEXAS LAW REVIEW 553, 587-591 (1998).

[684] Id., at 588-89.

[685] Id., at 589.

[686] Id.

[687] Id. For example, all government purchases of browser software might require that particular data protection policies be implemented in the browser.

[688] Id., at 590. For example, the French telecommunications law holds service providers liable if they fail to offer subscribers filtering mechanisms.

not circumvented.[689]

As these tools reflect, the*Lex Informatica,* or policy rules through technology, will increasingly mean that creation of political choices will be made in the selection of protocols and standards. This phenomenon is well illustrated by the Internet labeling and filtering projects for data protection. The terms and criteria used to label data protection practices express political judgments.[690] Specifically, the translation of data protection principles into technical specifications reflects judgmental choices rather than specific expressions dictated by the drafting of the data protection principle. Moreover, this politicization of technical choices will be an inevitable fact of the Information Society.

Data protection regulators, namely the Commission and the national authorities, will have to combine the set of six instruments listed above if an effective regulatory policy is to emerge. No single approach will successfully work in the on-line environment. For example, the regulation of behavior in the on-line environment will still necessitate an appropriate technical capability and the regulation of a standard should not pre-empt future technological developments.

For the European Union, the European Directive already offers a significant mechanism to address data protection through such forms of technological rule-making. Many issues might effectively be resolved through the existing procedures dealing with codes of conduct.[691] The European Directive expressly contemplates that the Member States and the Commission:

> must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics for the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation.[692]

---

689 Id.

690 See Joel R. Reidenberg, *The Use of Technology to Assure Internet Privacy: Adapting Labels and Filters for Data Protection,* LEX ELECTRONICA, <http://www.lex-electronica.org> (Fall, 1997).

691 Directive 95/46/EC, art. 27.

692 Directive 95/46/EC, Recital 61.

This existing legal basis provides an avenue to seek consensus among the Member States on technical mechanisms that make data protection possible and widespread in the on-line environment. In effect, the technical rules and protocols that determine information flows are «codes of conduct» in precisely the same way that trade associations draft policy guidelines.[693] However, unlike traditional industry codes of conduct, these technical rules and protocols have self-executing force; they will be dispositive for the structure of information flows on the network.[694] In approaching the technical system designs as «codes of conduct,» the Commission, Working Party and national supervisory authorities have a clear mandate to participate actively in a variety of fora not traditionally associated with data protection, such as the International Organization for Standards.[695]

In sum, to assure data protection that fairly considers all of the principles contained in the European Directive in the context of the on-line environment, the

---

693 Professor Lessig even refers to the constraints of rules and laws embedded in software as the 'code'. Lawrence Lessig, Reading the Constitution in Cyberspace, 45 EMORY LAW JOURNAL 869, at 896 (1996).

694 See Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 TEXAS LAW REVIEW 553, 572-573 (1998).

695 The International Organization for Standards is presently considering the Canadian proposal to adopt a privacy standard along the lines of the Canadian standard. Canadian Standards Association, Model Code for the Protection of Personal Information (1996).

European Union's data protection officials must have political input into the technical infrastructure decisions that affect the nature and characteristics of data flows. Groups such as W3C and the other standards bodies increasingly have the equivalent of regulatory power in connection with data protection policy. To continue to have an effective role in data protection, the Commission and the Working Party will need to develop significant technical expertise and pursue data protection through a broader range of regulatory policy instruments than the traditional legal directive approach.

APPENDIXAPPENDIXAPPENDIXAPPENDIX

TABLE 1

DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES Jurisdiction: Scope of «Personal Information»				
	Belgium	**France**	**Germany**	**United Kingdom**
Definition of Information as «Identifiable» (e.g. dynamic IP address or e-mail chnologie	Broad	Broad	Contextual	Contextual
Special exclusions	Yes (e.g. public data, distributed database?)	No	No	No
Special inclusions	No	Yes (e.g. log files, cookies)	Yes (e.g. anonymous/ pseudonymous data)	No
Anonymity/ Pseudonymity	Encouraged	Encouraged	Required	Encouraged

TABLE 2

DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES Jurisdiction: Scope of «Personal Information» Effect of the Directives		
	Directive 95/46/EC	**Directive 97/99/EC**
Definition of Information as «Identifiable» (e.g. dynamic IP address or e-mail address)	Incomplete Convergence	Incomplete convergence (Billing data only)
Special exclusions	Limited Convergence (e.g. journalists, households)	Incomplete Convergence (E.g. call tracing)
Special inclusions	No effect	Some convergence (i.e. «traffic data»; CLI)
Anonymity/ Pseudonymity	Encouraged indirectly	Encouraged

TABLE 3

DATA PROTECTION LAW AND ON-LINE SERVICES:
REGULATORY RESPONSES

Jurisdiction: Registration and Supervision

	Belgium	**France**	**Germany**	**United Kingdom**
Declaration Obligation				
Detailed Declaration	Yes	Yes	Yes	Yes
If server located in Member State	Yes	Yes	Yes	Yes
If information on foreign web sites is accessible from within Member State	Yes	Yes	Unclear	Unlikely
Exemptions from Declaration	Yes	No	No	No
Simplified Declarations	No	Yes	No	Yes
Registration Filing				
Fees	Variable	N/A	No	Fixed
Electronic Filing	On Disk	Not yet	Not yet	Yes

TABLE 4

DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES Jurisdiction: Registration and Supervision Effect of the Directives		
	Directive 95/46/EC	**Directive 97/66/EC**
Declaration Obligation		
Detailed Declaration	Incomplete Convergence	No effect
If server located in Member State	Convergence	No effect
If information on foreign web sites is accessible from within Member State	Incomplete convergence	No effect
Exemptions from Declaration	Some convergence	No effect
Simplified Declarations	Convergence	No effect
Registration Filing		
Fees	No effect	No effect
Electronic Filing	No effect	No effect

TABLE 5

DATA PROTECTION LAW AND ON-LINE SERVICES:
REGULATORY RESPONSES

Transparency

	Belgium	**France**	**Germany**	**United Kingdom**
Notice for Direct Collection	Yes	Yes	Yes	Yes
Notice for Indirect Collection	Yes	No	Yes	Perhaps
Content of Notice	Detailed	Detailed	Detailed	Detailed
Special Notices for On-line Services		Purposes and Risks	Cookies Reforwarding Anonymity Options	Explicit notice of additional purposes for sensitive data
Special Consent for Internet	No	Yes	Yes	No
Access Fees	2.5 ECU	3.0 ECU (public sector) 4.5 ECU (private sector)	No	15 ECU

TABLE 6

DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES Transparency Effect of the Directives		
	Directive 95/46/EC	**Directive 97/66/EC**
Notice for Direct Collection	Convergence	Incomplete Convergence (E.g. traffic data)
Notice for Indirect Collection	Convergence	No effect
Content of Notice	Incomplete Convergence	No effect
Special Notices for On-line Services	No effect	Limited Convergence (e.g. on-line directories)
Special Consent for Internet	No effect	No effect
Access Fees	No effect	No effect

TABLE 7

DATA PROTECTION LAW AND ON-LINE SERVICES:
REGULATORY RESPONSES

Profiling and Sensitive Data

	Belgium	**France**	**Germany**	**United Kingdom**
Sectoral Finality rules	Yes (e.g. consumer credit profiles)	Yes (e.g. Internet sites' disclosure of finality)	Yes (e.g. pseudonymous profiling on-line)	No (But, some limits through «fairness» and consent principles
Automated Decisions	No specific restraint	Prohibited	No specific restraint	No specific restraint
Consent required for processing on-line sensitive data	Advanced, perhaps written	Advanced, Written	No special requirements	No special requirements

TABLE 8

DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES Profiling and Sensitive Data Effect of Directives		
	Directive 95/46/EC	**Directive 97/66/EC**
Sectoral Finality rules	Authorizes	Convergence
Automated Decisions	Convergence	No effect
Consent required for processing on-line sensitive data	No specific effect (Special protections apply generally)	Convergence (i.e. subscriber billing data)

TABLE 9

DATA PROTECTION LAW AND ON-LINE SERVICES:
REGULATORY RESPONSES

Security

	Belgium	**France**	**Germany**	**United Kingdom**
Obligation to provide security for on-line services data	Yes	Yes	Yes	Yes
Regulation of Digital Signatures	Not yet	Not yet	Voluntary	Not yet
Cryptography	Law enforcement access for communications contents	Licensed	Unrestricted	Unrestricted
Key Escrow	Under consideration	Regulations pending	Under consideration	Under consideration

TABLE 10

DATA PROTECTION LAW AND ON-LINE SERVICES: REGULATORY RESPONSES Security Effect of the Directives		
	Directive 95/46/EC	**Directive 97/66/EC**
Obligation to provide security for on-line services data	Convergence	Convergence
Regulation of Digital Signatures	No effect	No effect
Cryptography	Encourages	Encourages
Key Escrow	No effect	Limited Convergence (i.e. any mandatory features other than those required by law enforcment may not impede the free circulation of equipment)