5

Regulating Identity Management

Eleni Kosta[1], Aleksandra Kuczerawy[1], Ronald Leenes[2], and Jos Dumortier[1]

[1] KU Leuven
[2] Tilburg University

5.1 Introduction

The notions of identity, privacy, personal information and data protection are closely related to each other. Privacy, according to Alan F. Westin 'is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others' [Wes67, p.7]. Another definition, provided by Lee Bygrave, states that privacy is 'a condition or state in which a person ... is more or less inaccessible to others, either on the spatial, psychological or informational plane' [Byg02]. Discussions regarding to the nature and sense of 'privacy' is long-lasting and complex. This chapter will not go into this particularly challenging debate, but rather it will sketch the legal framework in which privacy enhancing identity management operates.

Despite the various understandings of the concept of privacy, it is crucial to keep in mind, what specific interest the law should protect. It is clear that the vital point of a or the 'right to privacy' is the protection against misuse of personal information [Wac, p.10]. As discussed in the previous chapters, the advent of new technologies, have created many new privacy threats, whereas others have just gotten a much wider scope. Some of the already existing risks have changed appearance due to technological advancements. The now famous example of the 'dog poop girl' in Solove's 'The future of reputation' [Sol07] is telling in this respect. The story is a about a Korean teenage girl traveling on the subway when her dog pooped. She was asked to clean it up, but refused. In previous times she would have been cursed, but this being the 21st century,

J. Camenisch, R. Leenes, and D. Sommer (Eds.): Digital Privacy, LNCS 6545, pp. 73–89, 2011.

her acts were caught on camera by someone's mobile phone. The pictures were posted on a popular Korean blog. The picture and post went viral and were picked up by the mainstream Korean media. The girl became infamous throughout the country, harassed wherever she went and forced to drop out of university because of the shame. Since the incident, many people, also outside of Korea have seen the images and heard the story.

Privacy-enhancing identity management has a future in limiting privacy threats associated to the online world. However, in order to play such a role and be effective for private and business practices, they have fit into the existing legal framework regarding privacy and data protection. This chapter explores these legal frameworks. The chapter starts by a brief introduction on the European history of data protection regulation in Section 5.2. Next, in Section 5.3, we describe the core principles of the EU data protection regulation. Section 5.4 discusses some of the issues regarding the applicability of the current legal framework in an evolving online world. Finally, Section 5.5 provides some concluding remarks.

5.2 A Brief History of European Data Protection Regulation

The right to privacy protection originates directly from human rights law. The general opinion is that privacy constitutes a fundamental right of the individual and is one of the essential values in a democratic society (see also chapter 4). It can be found in all major international treaties, agreements on human rights and in the constitutions of most countries around the world.[1]

In Europe, one of the first documents recognising the fundamental right to respect privacy was the European Convention of Human Rights and Fundamental Freedoms (ECHR).[2] Article 8 ECHR states that 'everyone has the right to respect for his private and family life, his home and correspondence'. Further, in Article 8(2), ECHR expresses the need to keep the balance between the right for privacy and other interests stating that 'there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society 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'. The

[1] For an overview of the international instruments in the field of data protection see: `http://ec.europa.eu/justice_home/fsj/privacy/instruments/index_en.htm`; For an overview of national legislation in over 50 countries see: "An International Survey of Privacy Laws and Developments", Electronic Privacy Information Centre and Privacy International: `http://www.privacyinternational.org/survey`; See also: `http://www.epic.org`.

[2] European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Council of Europe, Rome, 1950, `http://conventions.coe.int`.

lawfulness of these restrictions has been refined in a number of judgements and decisions, issued by the European Court of Human Rights.[3]

Soon after the Convention came into effect it became obvious that the sheer recognition of the fundamental and constitutional principle of privacy is insufficient to effectively safeguard the growing need to protect the right of privacy. This became particularly clear when the full potential of information technologies for controlling data became apparent. This discovery led to a new approach to the issue based on enacting comprehensive national data protection laws applicable to both the private and public sector. Since the start of the seventies many countries followed the trend and enacted more detailed data protection laws. At the same time international developments led to a set of international policy instruments that affected the process of enacting data processing legislation.

The most prominent of these for privacy protection are the Guidelines governing the protection of privacy and transborder flows of personal data issued by the Organisation for economic Co-operation and Development (OECD) and Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe.

The OECD Guidelines, adopted on September 23, 1980, represent international consensus on general guidance concerning the collection and management of personal information. They apply to data held in public and private sector, which pose a threat to privacy and individual liberties, due to the manner in which they are processed, or because of their nature or the context in which they are used. The development of Guidelines aimed to contribute to the harmonisation of national privacy legislation, while complying with human rights, and, simultaneously, to prevent interruptions in international flows of data. This latter aim was considered necessary by the OECD Member countries which feared that disparities in national legislations could hinder the free flow of personal data across frontiers. The guidelines introduce a set of basic principles which should serve as a foundation for national legislations and which should be complied with by the data processors. The principles are: *collection limitation*, *data quality*, *purpose specification*, *use limitation*, *security safeguards*, *openness*, *individual participation*, and *accountability*.

On January 28, 1981, the Council of Europe adopted Convention No. 108. In its preamble, it recognises the need to reconcile the fundamental values of the respect for privacy and the free flow of information between people. It also clearly states that the aspiration of the Council of Europe is to enhance the safeguards for everyone's rights and fundamental freedoms. In particular, the focus of the Council of Europe is placed on the right to the respect for privacy, in order to tackle the new challenges of the increasing flow of

[3] Klass,06.09.1978; Sunday Times, 26.04. 1979; Malone, 02.08.1984; Leander, 26.03.1987; Kopp, 25.03.1998; Rotaru, 04.05.2000; Amann, 16.02. 2000; Lambert, 24.08.1998; Valenzuela Contreras, 30.07.1998; Kruslin, 24.04. 1990; Huvig, 20.04. 1990. These judgments are available at: `http://www.echr.coe.int/Hudoc.htm`.

personal data across frontiers and undergoing automatic processing. Just like the OECD Guidelines, Convention 108 spells out a set of principles that should be followed when processing the data. Its main points claim that personal data should be obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and kept up to date; preserved in an identifiable form for no longer than is required for the purpose for which those data are stored; adequately secured; accessible by the data subjects for the rectification or erasure.

Europe, in the mid 1990s, decided to take the lead in harmonizing the data protection regulation. The result of the developments is that current data protection regulation in Europe is primarily based on few key instruments while relevant details specific for particular Member States, their legal systems and traditions, are contained in the national laws in the member states.

5.2.1 The EU Data Protection Directive

The EU went a step further than the OECD guidelines and Convention No 108 of the Council of Europe and enacted regulation for the EU member states pertaining to data protection. The core of data protection is laid down in the general Data Protection Directive 95/46/EC, constituting a data protection framework, and in the Directive 2002/58/EC, known as the ePrivacy Directive, as amended by Directive 2009/136/EC, the Citizen's Rights Directive. Additionally, Directives 2000/31/EC on Electronic Commerce and 1999/93/EC on Electronic Signatures are, to some extent, significant for the current discussion.

The aim of the general Data Protection Directive is to promote the free movement of personal data within the European Union, and to ensure a high level of protection of both, the right to privacy, and of the fundamental rights and freedoms of the individuals with regard to the processing of personal data in all Member States. These two objectives, of ensuring that personal data can move unrestrictedly within the Single Market of the European Union on the one hand, and that a level of protection of the individual's rights on his personal data is uniform within the whole EU on the other, are explicitly mentioned in the Directive's preamble. The fact that the level of protection of privacy provided in national laws of various Member States differed was considered as a major threat to the internal market. It could constitute an impediment to economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law. In order to prevent these threats to the internal market, the harmonization of the national laws was desired, with a margin for maneuver left to the Member States. The overall effect of these actions was to result in improvement of privacy protection in the European Community.

The scope of the Directive is very broad as the concept of 'personal data' applies to text, sound and image data. Furthermore, it covers any information relating to an identified or identifiable natural person — a data subject. The Directive clarifies that under the term 'identifiable person' it understands every person who can be identified, either directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. In order to ascertain whether a person is identifiable, according to Recital 26 of the Directive, account should be taken of all the means likely to be used either by the controller or by any other person to identify the said person. This proves an expansive approach as every data that could be a link to an identifiable individual will come under the scope of the Directive. It brings data, whatever its form, under the 'personal data' umbrella as soon as it is possible to identify the person to whom the information refers, now or in the future.[4] Recital 15 seems to confirm such approach stating that processing of sound and image data is only covered by the Directive, if it is automated or if the data processed are contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question.

The concept of 'processing' is defined by the Directive in a similarly broad way. According to Article 2 (b) it refers to any operation performed on personal data such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This, basically, means any activity that could be performed on data. Even a single consultation or retrieval of a file containing personal data, for example, would constitute processing and has to comply with the provisions of the Directive. Also the sole storage of personal data on a server is considered to be processing, even if nothing is done with the data.

Moreover, the Directive defines several terms relevant for the data subject and introduces specific requirements, which are indispensable in order to render the data processing legal and lawful. These requirements address the 'data controller'. In the context of data protection, 'controller' is every individual or entity who determines the purposes and means of the processing of the data. Who the controller actually is depends on the factual context. In some cases of personal data processing there can be more than one responsible controller. Apart from the concept of data controller, the directive introduced the term of 'data processor', who is a third party who merely processes personal data on behalf of the data controller. The distinction made between 'data controller' and 'data processor' is important for the issue of the liability for violations of the Data Protection legislation. As a rule of thumb, it can be said that the responsible party will be data controller.

[4] See also the discussion on whether IP addresses constitute personal data in Section3.6.6.

In order to prevent the possibility that individuals in the European Union are deprived of any privacy protection if the controller has no establishment in a Member State, the Directive states that it is applicable when the controller makes use of equipment for processing of personal data which is situated on the territory of a Member State. The term 'equipment' covers all possible means like computers, telecommunication devices, impression units, etc. Article 4, however, states an exception to this rule, when the equipment is used only for the purposes of transit of personal data through the territory, such as cables or routing equipment. Moreover, the Directive regulates that if the means for processing personal data are located on the territory of a Member State, a representative established in the aforementioned Member State should be designated by the controller.

The Data Protection Directive, mainly in Article 6, introduces a set of crucial principles for data processing. Most of these conditions refer to the quality of data. These principles set out the core regulation regarding the processing of personal data and therefore they are often characterised as the constitutional law of data protection [Blu02, p.30]. They will be discussed in Section 5.3.

5.2.2 The ePrivacy Directive

The Directive 2002/58/EC, commonly known as ePrivacy Directive, complements the principles introduced in the general Data Protection Directive and converts them into specific rules for the electronic communications sector. The Preamble of the Directive highlights that the advent of new advanced digital technologies in public communications networks in the Community, raises a need for specific requirements concerning the protection of personal data and privacy of the user. The development of the information society automatically leads to the introduction of new electronic communications services and increased access to digital mobile networks by an increasing public. As the capabilities of such digital networks to process personal data are significant, the confidence of users that their privacy will not be at risk is essential for the successful cross-border development of these services. The ePrivacy Directive was modified by Directive 2009/136/EC, commonly known as Citizens' Rights Directive. This Directive introduced the data breach notification and, among others, amended the provisions of the ePrivacy Directive relating to security and confidentiality of personal data, as well as those relating to unsolicited communications. Given that the Citizens' Right Directive was adopted long after the end of the PRIME project, its provisions did not influence the results of the project and will therefore not be analysed at this point.

These risks are especially clear in the area of Location Based Services (LBS). It is clear that in order to enable the transmission of communications, the processing of location data which gives the geographic position of the terminal equipment of the mobile user is required. However, digital mobile networks have the capacity to locate the equipment more precisely than is

necessary for the purpose of transmission of communications. Such accurate data can be used for the provision of value added services such as, for example, providing individualised traffic information and guidance to drivers. In such cases, the Directive states that the consent of the subscriber is indispensable for the processing of such data for value added services to be allowed. Moreover, even after giving their consent, subscribers should be permitted, in a way that would be easy and free of charge, to temporarily or permanently object to the processing of location data. It is also worth mentioning that the Directive emphasises the fact that the protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the technology used.

5.2.3 Other Relevant Directives

The main goal of the Directive on Electronic Commerce 2000/31/EC is to regulate the liability of Internet Service Providers (ISPs). All types of illegal activities performed on-line by third parties are covered by the Directive, which adopts a horizontal approach to the issue. This means that it applies to all areas of law, including civil and criminal law. Hence, the liability regulation covers all types of illegal online activities (copyright infringement, unfair competition, misleading advertising, defamation, child pornography, etc.).

Finally, the Directive 1999/93/EC on Community framework for electronic signatures introduced a rule that indicating a pseudonym instead of the signatory's name cannot be prevented by certification service providers who issue certificates or provide other services related to electronic signatures.

5.3 Principles of Data Processing

In this section we will discuss the core principles embedded in Directive 95/46/EC. We will discuss them in the light of defining legal requirements for privacy-enhancing identity management. These requirements can be used as a main guiding tool for the developers of identity management systems and privacy enhancing tools, as was done in the PRIME project. The principles are grouped into three categories: principles on processing of personal data, rights of the data subject and specific requirements for electronic communications systems or applications. Apart from these requirements, we have also defined a set of requirements that are rooted in both law (regulation and legal theory) and in sociology. These latter requirements, i.e., the principle of user consent, principle of security, right to information, right of access and right to rectify, erase or block the data are described in Chapter 6.

5.3.1 Principles on Processing of Personal Data

5.3.1.1 Principle of Fair and Lawful Processing

A fundamental principle laid out in Art. 6(1)(a) Data Protection Directive requires the processing of the data to be fair and lawful. It has been named a primary requirement due to the fact that it 'both embraces and generates the other core principles of data protection laws' [Byg01, p.1]. To assess whether personal data were processed in a fair and lawful way, the method used to obtain the data should be taken into account. Because it is the starting point of processing, it can, to a large extent, influence the fulfillment of other conditions in later stages of processing. In order to have the requirement satisfied, the relevant data subject has to be provided with certain information, mentioned in Article 10 of the Data Protection Directive (on the identity of the controller and of his representative, the purpose of data processing and further information, like who is the recipient of the data, if replies to the question are obligatory or voluntary, and whether there is a right to access and to rectify the data) at the time of the obtaining of the data, or very soon afterwards [Car02, p.54]. Moreover, lawful processing requires the data controllers to comply with all types of their legal obligations, general and specific, statutory and contractual, concerning the processing of the personal data. For example the processing should be performed with respect to Article 8 of the European Convention on Human Rights, which calls for respect for the private life of the individual.

5.3.1.2 Principle of Finality

Article 6(1)(b) of the Data Protection Directive sets the second data processing principle. It is usually addressed under the names of principle of finality, purpose limitation, purpose specification or principle of secondary use. According to this requirement, data controllers must collect data only as far as it is necessary in order to achieve the specified and legitimate purpose. Furthermore, data controllers cannot carry out any further processing which is incompatible with the original purpose. This means that the data subject must be specifically informed about the purpose of the data collection and that subsequent use of collected data is restricted. In particular, the finality principle requires that, without a legitimate reason, personal data may not be used and the concerned individual must remain anonymous. The goal of the principle is to promote transparency and, additionally, to enhance the control of the user over the use of the data. This requirement is seen as the most controversial one in the data protection law [Blu02, p.32]. The indication of the purpose of data collection has to be clear and accurate, using a precise and distinct wording in order to satisfy the principle. This, of course, may lead to a constant dispute over the practical application of the requirement [Blu02, p.32].

5.3.1.3 Principle of Data Minimisation

Article 6(1)(c) of the Data Protection Directive embodies the principle of data minimisation, stating that the processing of personal data should be limited to data that are adequate, relevant and not excessive. The basis for the assessment whether this condition has been fulfilled is the purpose of data collection. Furthermore, Articles 7 and 8 of the Data Protection Directive implicitly repeat the requirement of data minimisation prohibiting the processing of data unless it is indispensable for achieving specific goals. Data controllers are obliged to store only a minimum of data sufficient to run their services. Particularly, data accumulation, a practice often exhibited by public authorities who gather more personal data than required, should be avoided. The storage of large amounts of data can easily be considered as privacy violation, and the argument that the data is not used is insufficient to justify its preservation [Blu02, p.34]. In the context of restrictions on the amount of collected data, issues of 'data avoidance' [HS03] and 'privacy by design' [DG04, p.193] are relevant. The former requires that the technical devices and designs use either no personal data or as limited a amount as possible. The latter suggests that the privacy issues and specifically the processing of personal data (including identity management related implications) should be taken into account from the earliest stage of the organisation of the network infrastructure. Technical tools and Privacy-Enhancing Technologies in particular, should be available to contribute to the effective implementation of the data minimisation requirement.

5.3.1.4 Principle of Data Quality

Another principle, deriving from Article 6(1)(d) of the Data Protection Directive, provides that all personal data shall be accurate and, where necessary, kept up to date. Data controllers are obliged to take every reasonable step to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected are either erased or rectified. This principle is particularly important for the protection of personal integrity. It is often suggested that data controllers should create an appropriate mechanism which would enable the data subjects to update their personal data or notify the data controller about the inaccuracies of the present information. Such solution would prevent, in case of detriment caused by the incorrect data, possible data subjects' complaints of breach of this principle. In practice, these measures are hardly ever implemented.

5.3.1.5 Principle of Conservation

The principle of conservation, also known as the time limitation principle, is described in Article 6(1)(e) of the Data Protection Directive. It stipulates that personal data shall not be kept for longer than is necessary for the purposes

for which these data were collected. It implies that after achieving the purpose for which the data were gathered, they should be rendered anonymous or destroyed, which means that the principle is targeted against the aforementioned practice of data accumulation. It should be emphasised that the processing of personal data for the purpose of anonymisation falls within the scope of the Directive, since the definition of the term 'processing' is so broad that it includes the process of anonymisation as well. However, having in mind the aim of the Directive, imposing compliance obligations with regard to the process of anonymisation could be considered as counter to the achievement of its purpose, especially in light of Recital 26 of the Directive, which says that the principles of data protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

5.3.1.6 Principle of Confidentiality

The Directive 2002/58/EC on privacy and electronic communications (ePrivacy) aims to protect the confidentiality of communications. Member States must ensure the confidentiality of communications (and the relevant traffic data) by means of public communications network and publicly available electronic communication services through national legislation. In particular, listening in on, tapping, storing or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned and except when legally authorised to do so, is prohibited. The Directive provides for an important exception from this principle: legal authorisation for the monitoring of electronic communications is possible when it constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the communications system (Article 5(1) in conjunction with Article 15(1) of the ePrivacy Directive).

5.3.1.7 Principle of Notification to the Supervisory Authority

The data controller must notify the respective national data protection authority before any data processing operation is carried out (Article 18 of the Data Protection Directive). The Directive leaves to the Member States the possibility to simplify the notification procedure or to waive it altogether in certain situations. However, for the vast majority of entities engaged in any form of automated processing of personal data, the notification remains obligatory. According to Article 19 of the Data Protection Directive notification to a national data protection authority must include at least: the name and address of the controller and of his representative; the purpose of the processing; description of the categories of data subjects and of the data or categories of data relating to them; the recipients or categories of recipients to whom

the data might be disclosed; proposed transfers of data to third countries; a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

5.3.1.8 Data Processed in Line with the Rights of the Data Subject

Data controller are obliged to respect the rights of the data subjects when they process personal data. Article 12 of the Data Protection Directive, in particular, grants data subjects the right to be provided, by the data controller, with basic information about the processing of their personal data. It is generally accepted that all the rights mentioned in Article 12 (Subparagraphs (a), (b), and (c)), and not only those from subparagraph (a) as it is explicitly stated in the Directive, should be exercised without constraint at reasonable intervals and without excessive delay or expense [DS97, p.199]. The Directive also provides the data subject with a right to object to the processing of data relating to her (Article 14), as will be elaborated below.

5.3.2 Rights of the Data Subject

The Data Protection Directive grants several rights to the data subjects, although some of them are recognised in an implicit way. Providing the data subjects with those rights intends to guarantee that the data subject remain the ultimate controllers of their personal data. This should also reinforce the fundamental right to privacy described in Article 8 of ECHR. The right to information, the right of access and the right to rectify, erase or block the data will be analysed in detail in the following chapter, as they can be understood as requirements with a social as well as legal basis.

5.3.2.1 Right to Object

Pursuant to Article 14(a) of the Data Protection Directive, Member States shall grant the data subject the right to object to the processing of data relating to him, on compelling legitimate grounds relating to his particular situation. This right to object must at least cover the cases where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority and where processing is necessary for the purposes of the legitimate interests pursued by the controller (Article 7(e) and (f)).

Article 14(b) of the Directive concerns the processing of personal data for the purposes of direct marketing. The Directive gives the Member States a choice between two formulas. They can grant the data subject the right: (i) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes

of direct marketing, or (ii) to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses. The exact procedure and time limitations to be observed in such cases is the matter of the transposition of the Directive's provisions into national laws.

The right to object is aimed at giving the data subject a possibility to prevent the processing of his data, in case where it violates his personal integrity and where it would be otherwise legitimate. The principle originated from the idea that individuals own their personal data, therefore they should be in a position to control it and oppose to its processing. It is an evident recognition of the right to self-determination.

5.3.2.2 Right Not to Be a Subject to an Automated Decision

Article 15 of the Data Protection Directive grants the data subject a right not to be subjected to an automated decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to data subject, such as his performance at work, creditworthiness, reliability, conduct, etc. This right was introduced to overcome the effect of development of information technology which very often leads to decisions being made mechanically. Frequently, such decisions are of essential importance or have legal effects; hence they should be taken by other people who can take into account specific circumstances of the individual. There are statutory exceptions provided to this right in cases where the decision is either taken in the course of the entering into or performance of a contract, provided that the request (for the entering or the performance of the contract) has been lodged by the data subject and there are suitable measures to safeguard the data subjects legitimate interests; or is authorised by a law that also lays down measures to safeguard the data subject's legitimate interests.

5.3.2.3 Right to Seek Legal Relief

Article 22 of the Data Protection Directive provides for a right of every person to a judicial remedy for any breach of the rights guaranteed to him by the national law applicable to the processing in question. Further, the Directive provides that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the aforementioned Directive is entitled to receive compensation from the controller for the damage suffered (Article 23 of Data Protection Directive).

5.3.3 Specific Requirements for Electronic Communications Systems or Applications

5.3.3.1 Processing of Traffic Data

According to Article 2(b) of the ePrivacy Directive, the term 'traffic data' refers to any data processed for the purpose of the conveyance of a communication on an electronic communications network or for its billing. Traffic data may only be processed to the extent needed for the purpose of the transmission of a communication. When no longer needed for that purpose, the data must be erased or made anonymous (Article 6(1)). Traffic data necessary for subscriber billing and interconnection payments may be processed up to the end of the period during which the bill may lawfully be challenged or payment pursuit (Article 6(2)).

5.3.3.2 Processing of Location Data for the Provision of a Location Based Service

Pursuant to Article 9 ePrivacy Directive, location data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, about the type of data to be processed, the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing a value added service. The users/subscribers must also be given the possibility to withdraw their consent for the processing of location data at any time (Article 9(1) of the ePrivacy Directive). It should be emphasised, that location data may only be processed by persons acting under the authority of the provider of the public communication network or publicly available communication services (i.e., the telecommunication operator) or of a third party providing the value added service who obtained the data for the purpose of provision of this service (Article 9(3) of the ePrivacy Directive).

5.3.3.3 Automatic Data Collection Procedures

The data subject has the right to information in case of automatic data collection procedures, as well. Typical examples of such invisible processing include 'browser chattering', automatic hyperlinks to third parties, so-called 'Web-Bugs', active content (e.g., Java) and cookies. Again, the necessary information about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using must be given before any personal data are collected. In particular, the use of cookies (or other tools for storing information on the user's terminal equipment) is only allowed if the user has the opportunity to refuse the cookie to be installed. However, this condition does not apply if the use of the cookie is

"strictly necessary in order to provide an information society service explicitly requested by the subscriber or user" (Article 5(3) of the ePrivacy Directive).

5.3.3.4 Unsolicited Commercial Communications (Spam)

The ePrivacy Directive is also an important step forward in the protection of the users of electronic communications against unsolicited messages. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent (opt-in). As an exception to this general rule, it remains possible for merchants to send electronic mail to their own customers for the purpose of direct marketing of similar products or services, provided that customers clearly and distinctly are given the opportunity to object (opt-out). Other types of unsolicited communications for purposes of direct marketing are not allowed either without the consent of the subscribers' concerned (opt-in), or in respect of the subscribers who do not wish to receive these communications (opt-out). In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, has to be prohibited by Member States' legislation.

5.4 Applicability Issues of the Current Legal Framework

5.4.1 An Old Directive for New Technologies

The principles included in the general Data Protection Directive, as well as their specific interpretation in the ePrivacy Directive in cases where data protection issues arise in connection to publicly available electronic communications services and networks, delineate a solid data protection framework at the European level. At first and overall glance, the European legal framework on data protection contains the core principles that can ensure the protection of individuals with regard to the processing of personal data on one hand and the free movement of such data on the other. These were the main objectives of the Data Protection Directive back in 1995 and it can not be contested that they actually still ensure a satisfactory level of protection of the individuals when the processing of their personal data takes place in a conventional way, for instance when data are collected and processed by a company, with whom the individual signs a contract.

Objections regarding the effectiveness of the Directive arise with regard to new technologies. As already illustrated in Chapter 3, the notion of personal data is not always clear when new technologies are involved. IP addresses,

cookies, RFID technology are only but a few examples that show that the application of the Data Protection Directive is not free of problems. There is just too much information, created and exchanged in too many different ways. A piece of information, which relates to an identifiable natural person under one circumstance, does not qualify as personal data in another situation. Although the Directive was written up in a technologically neutral way, some new developments reveal the vulnerability of the Directive to deal with them efficiently. The European Commission actually admitted in its Communication on the follow-up of the Work Programme for better implementation of the Data Protection Directive that "the extensive development of new information and communication technologies necessitates specific guidance on how to apply [the] principles [laid down in the data protection directive] in practice" [otEC07, p.10].

Does this mean that a completely new piece of European legislation is needed? As the European Data Protection Supervisor has articulated, "there is no need for new principles, but there is a clear need for other administrative arrangements, which are on the one hand effective and appropriate to a networked society and on the other hand minimize administrative costs" [EDP07, p.4]. In simple words, this would mean that the most important principles for data protection are laid down in the Directive, so there is no pressing need for a new piece of legislation. Although new developing technologies reveal the vulnerabilities of the current legal framework, it is technology that can give the solution to this problem, when "used effectively and [is] relied upon in a privacy enhancing way" [EDP07, p.6]. It is the relation between technology and law that needs to be redefined: law enabling technologies and technologies enabling the law are the only solution that can ensure adequate protection of the individuals, when processing of their personal data is involved (see also extensively on the interplay between law and technology in this respect [Han08, Lee08, KL05]).

5.4.2 The Role of the ePrivacy Directive with Regard to the Challenges Posed by New Technologies

The general Data Protection Directive is complemented by the ePrivacy Directive, when processing of personal data in the electronic communications sector is involved. The ePrivacy Directive aimed at the protection of the users of publicly available electronic communications services that are offered via public communications networks regardless of the technologies used, seeking to implement the principle of technology neutrality into the regulation of data protection in the electronic communications sector (Recital 4 of the ePrivacy Directive). However, questions arise regarding the applicability of the ePrivacy directive to several emerging technologies, such as RFID, and to problems that arise from their use in the field of electronic communications.

Although the distinction between private and public networks seemed reasonable at the time of the drafting of the ePrivacy Directive, the fact that the

Directive only applies to publicly available electronic communications services in public communications networks is heavily criticised today. The Article 29 Working Party on Data Protection has expressed the opinion that "private networks are gaining an increasing importance in everyday life, with risks increasing accordingly [and there is a] tendency [that they] increasingly become a mixture of private and public ones" [Par06, p.3]. The same opinion is shared by the European Data Protection Supervisor, who "regrets that the proposal [for a Directive amending, among others, the ePrivacy Directive] has not tackled the issues of the increasingly blurred distinction between private and public networks"[EDP08, p.6].

Nevertheless, it seems that the ePrivacy Directive will still apply only on public networks and services, even after the review. It shall be clarified that the individuals enjoy the protection of the general Data Protection Directive, whenever processing of personal data takes place. It remains to be examined whether the specific provisions of the ePrivacy Directive that regulate issues, such as security, confidentiality, traffic and location data, are also applicable. Currently in order to decide upon the applicability of the ePrivacy Directive, three main issues need to be examined:

1. Whether there is an *electronic communications service*,
2. Whether this service is offered in a *communications network* and
3. Whether the aforementioned service and network are *public*.

According to Article 2(d) of the Framework Directive[5] "*public communications network* means an electronic communications network[6] used wholly or mainly for the provision of publicly available electronic communications services[7]". The term *communication* is defined in Article 2(d) of the ePrivacy

[5] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive), O.J. L 108, 24.04.2002, pp. 33 - 50.

[6] '*Electronic communications network* means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed' (Art. 2 (a) Framework Directive).

[7] '*Electronic communications service* means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of the Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks' (Article 2 (c) Framework Directive).

Directive as "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information".

The need for further clarification of these quite complicated definitions has already been recognised by the Article 29 Working Party: "The Working Party notes that both definitions 'electronic communications services', and 'to provide an electronic communications network' are still not very clear and both terms should be explained in more details in order to allow for a clear and unambiguous interpretation by data controllers and users alike" [Par06].

5.5 Conclusion

The European data protection framework tries to strike a balance between promoting the free movement of personal data within the European Union, and ensuring a high level of protection of the right to privacy, and of the fundamental rights and freedoms of the individuals with regard to the processing of personal data in all Member States. This means that the Directive promotes the free flow of information provided that a set of data protection principles is observed. The basic data protection principles for the processing of personal data contained in the Data Protection Directive provide a certain level of protection. The provisions in the Directive (through their implementation in the legislation of the member states) provide obligations for data controllers and rights for data subjects and should be observed in the implementation of any data processing system that deals with (potential) personal data. The principles outlined in this chapter are therefore also design requirements for privacy-enhancing identity management solutions.

The protection seemed adequate at the time the Directive was written. The tide, however, seems to shift. The development of new technologies and new services create new challenges with respect to privacy and data protection. The basic data protection principles need to be revisited in order to be able to tackle the challenges of today. This does not necessarily need to be done by a new legislation. The solution to upcoming challenges may be provided by what causes them in the first place: technology. Technology may provide solutions that will enable the privacy compliant processing of personal data. PETs can play an important role in implementing and enforcing the data protection principles. Data minimisation, anonymisation and purpose limitation are just three of the principles that can be realized in privacy-enhancing systems as we will see later on in this volume.