6

User-Centric Privacy-Enhancing Identity Management

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

[1] Tilburg University
[2] KU Leuven

6.1 Introduction

Online identities are associated to individuals and improper handling of these identities may therefore affect these individuals. Placing the individual at the center of identity management and empowering them with tools to actively manage their identity may help limit the privacy risks provoked by the information society. As we have argued in the previous chapters, embedding privacy into the design of identity management systems is important. What the actual embodiment of privacy features into IdM encompasses is less clear. The previous chapter has shown a number of data protection principles that have to be observed by any system that handles personal data. These principles are part of the legal requirements for the development of any application that handles personal data, including identity management systems. There are also other sources of requirements. Human computer interaction research, sociological research and economics/business studies can also contribute to defining requirements for privacy-enhancing identity management systems. In the current chapter we focus on results obtained in PRIME research in the fields of law and sociology and human computer interaction that resulted in a set of concrete set of requirements for user-centric privacy-enhancing IdM. A more detailed description of user-focused privacy requirements can be found in PRIME's Deliverables Framework V3 [PRI08] and Requirements V3 [KDR+08].

Section 6.2 briefly discusses the sources of the requirements described in the current chapter. Section 6.2.1 deals with the importance of *audience segregation* in Identity Management, and its direct link with privacy. One

J. Camenisch, R. Leenes, and D. Sommer (Eds.): Digital Privacy, LNCS 6545, pp. 91–106, 2011.

important aspect of audience segregation is *user control*. User control, a complex and ambiguous concept that gives rise to a set of subrequirements, is addressed in detail in Section 6.2.2. These requirements stem from legal and sociological/psychological grounds. Section 6.2.3 concludes the chapter by discussing a number of *adoption* requirements that should guarantee the user adoption of privacy-enhanced identity management developed along the lines of the previous requirements.

6.2 Sources of the User-Perspective Requirements

Legal and sociological research within the PRIME project has contributed to the conception of a set of requirements for privacy-enhancing identity management from a user-perspective. Identity management systems must comply with data protection legislation. The legal data protection principles outlined in the previous chapter are obvious starting points for developing requirements that do justice to the user-perspective of identity management systems. The current legal privacy-framework was therefore analysed in chapter 5 from the perspective of the individual as a user of identity management systems. The relevant Directives are:

- Directive 95/46/EC (Data Protection Directive),
- Directive 2002/58/EC (ePrivacy Directive) and,
- Directive 2006/24/EC (Data Retention Directive).

Apart from those, also the European Directive 1999/93/EC (Electronic Signature Directive) and the European Directive 2000/31/EC (eCommerce Directive).

The legal framework provides some general requirements for privacy-enhanced IdM systems. Another source for user-perspective requirements is literature on social aspects of interaction and technology use and privacy literature in general, when viewed through the lens of the individual. The input to the 'social' requirements comes from sociology, HCI, eCommerce, marketing, law, and philosophy research (e.g., [JB05, PK03]). Also survey data relating to privacy and identity management was was incorporated in the process of deriving requirements.[1]

6.2.1 Audience Segregation

Audience segregation is an essential aspect of Identity Management for the individual (see also Chapter 4). Every individual has different characters, which are used in different settings in society, such as 'citizen', 'daughter', 'friend',

[1] The survey results obtained in a large scale survey conducted within the PRIME project under Dutch, Flemish and UK students can be found as an annex to PRIME deliverable Requirements V3 [KDR+08](version 2.0 May, 2008), which is available from the PRIME website `http://www.prime-project.eu`.

and 'employee'. In playing their characters (which are sometimes roles), people explicitly and implicitly disclose information about themselves. This information people give, and give off [Gof59], is determinative for their character. While deploying or combining information, individuals are to some extent able to construct and manage their different characters in life, facilitating them to have various relations with different levels of intimacy. However, to be able to play different characters, one needs to be able to control the attributes of these characters and the settings in which they appear.

Audience segregation is an issue in the online environment, because 'simple' partial identities (or digital personae [Cla94]) can be aggregated into rich compound identities from data linked to identifiers, such as names and IP-addresses. Digital personae are easily copied, merged and manipulated. Hence, digital personae can be exposed to 'audiences' that should not be able to see them and be able to obtain personal data. This is even possible without the individual being aware of its occurrence. The merging of data and use of data out of context can easily result in practices such as social sorting and discrimination. A lack in the ability to segregate audiences also increases the risks of reputation damage because critique, comments, and worse online bullying, or blackmailing, for example, easily cross audiences.[2]

Having different partial identities is a social necessity. It allows the individual to fit into different social spaces, like work and family. Characters are furthermore often required to 'team play' in relations with others, like family and colleagues. Having consistent characters and segregating audiences positively affects the relation with relations present in a specific social context. In addition, characters are important in the sense that being confronted with the individual out of character may lead to wrong interpretations of behaviour, confusion, and decisions based on 'wrong' (out of context) information. For instance, bringing up certain hobbies in a job interview, may turn out not to be a good idea. The fact that one keeps snakes and feeds them mice, may not have a positive impression on the person conducting the job interview, while the hobby may well not at all affect the professional performance of the candidate.

The necessity to segregate audiences and play characters is an essential aspect of informational privacy. Having a variety of relations, or being able to develop oneself, is not only determined by the information we share in relations, but also by the information that is (mutually) concealed [Sch68]. In addition, not knowing something about a character or not needing to know information directly relates to the notions of trust, autonomy, cohesion, efficiency, and accountability (see, e.g., [Int97, Fri68])

If identities become 'mixed up' segregating performances played in different relations and relations is no longer possible and relations run the risk of becoming one-dimensional, confusing, and shallow. Lack of audience

[2] As Solove's [Sol07] 'Dog poop girl' example shows. See Chapter 5 for the details.

segregation would make an individual the same to his employer, spouse, dentist, best friend, and parents: everyone would become one-dimensional and colourless.

Some privacy concerns voiced by users in privacy studies clearly relate to this dimension. Many students in the PRIME survey, for instance, state that they use different and anonymous e-mail addresses to separate contexts (business, social) (see [KDR+08] May 2008 version). One of the key requirements that can be derived from the need for being able to segregate audiences is user control.

6.2.2 User Control

Even though there are many privacy conceptions, user control in many is a core requirement [Fri68, Rac75, Wes67]. User control ranges from some influence on what gets disclosed to whom, up to very strong positions such as the German right to informational self-determination. Both user control and self determination are part of the European notion of privacy [Sta02, OMS+07, PRI06a], and acknowledged in national and European data protection regulation. User control is therefore also a key requirement for privacy-enhanced IdM systems. Control, however, is an ambiguous concept [Gav80] which therefore needs to be explored into more detail. The following sections decompose user control into manageable concepts and preconditions for ex-ante and ex-post user control. We do this, from a social and legal point of view. We distinguish five sub-requirements: *information to the user*, *consent of the user*, *user access*, *correction, erasure, and objection*, and *security and trust*.

6.2.2.1 Information to the User

In order to be compliant with Article 10 of the Data Protection Directive (95/46/EC), a data controller should provide a data subject some minimum information regarding the processing and the controller doing the processing (cf. Chapter 5). A privacy-enhanced Identity Management system needs to take this obligation into account. Providing information to the user is an interpretation of the legal principle of fair and lawful processing because only when a user is informed beforehand about data collection, he or she can assess a service and decide whether or not to participate. In addition, providing information prior to the disclosure increases the willingness of people to enter into a relationship, a step in creating the social contract between data subject and data controller. It is therefore also a precondition for users to know when they can exercise their rights. Providing information to a user therefore is the first and crucial step to empower the individual to construct and maintain their identity and guard their privacy.

According to the Data Protection Directive, the minimum information that needs to be provided to the user, concerns:

1. The identity of the controller or his representative;
2. The purposes of the processing for which the data are intended;
3. Any further information if this is necessary to guarantee fair processing in respect of the data subject, such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of the failure to reply and the existence of the right of access to and the right to rectify the data concerning her.

The information has to be provided to the user at the time — or before — their personal data are collected. If disclosure to a third party is foreseen, Article 11 of the DPD provides that the information must be provided at the latest when the personal data will be disclosed to this third party. The Directive excludes the right of information in cases where the disclosure to a third party is made for statistical purposes, or for the purposes of historical or scientific research, and when 'the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by [national] law' (Article 11(2) of the Data Protection Directive).

Information is a key prerequisite to providing the user control over their personal data. Data subjects need to know what will happen to their data and indirectly to themselves. This promotes their autonomy and fosters human dignity. Having information at their disposal also raises the 'consciousness' of the data subject, which is essential to enable them to make informed choices concerning the dissemination of their personal data. Moreover, when information regarding data collection is provided, the process of data collection is made transparent beforehand, which contributes to fairness and trust. In addition, information about processes of data collection reduces the chances of instituting 'panoptic surveillance', in which human behaviour becomes normalised and influenced by the sense of omnipresent surveillance [Fou77].

Being aware which data will be collected and for which purposes may reduce the risks that the data controller can collect data to serve as a basis for many — potentially undesirable — processes and decisions, like profiling, discrimination and exclusion. The transparency this creates is an instruments that helps level out the immanent power-imbalance between data subject and data controller.

The information that is given to the user is seen both as a right of the data subject and as an obligation of the data controller to inform the data subject. In practice, the obligation to inform the data subject is seen as a major duty of the data controller, as the data subject very often is ignorant of the fact that processing of some of her data takes place, let alone knows the details regarding the processing. Only providing the user a minimal right to information will probably not guarantee the actual consciousness of a data subject to the data processing and its effects. It is therefore necessary to go beyond providing the minimal information and also raise awareness regarding the essential events, stakeholders, and attributes of the collection and use of personal data. This requires that information is presented in a comprehensive format. This is a

difficult task because of the different information needs of people and their capacity to understand the information. 'Comprehension' of the information provided is essential because only then can misguided disclosure of information, false information sharing, and user regret be minimized. This makes the provision of clear information not only an the interest of the user, but also of the data controller because it avoids future conflicts or unsatisfied customers.

Following from the requirement to provide information in a way that creates *consciousness* and *comprehension* is that information needs to give users a glance into the future. Privacy-enhanced Identity Management systems therefore need to be *consistent*. Many to all actions following from the collection of data lie in the future, and so there is always a risk of future misrepresentation of partial identities or unforeseen and unwanted decisions. People, preferences, and situations change and data may be used differently in the future. By providing the user a consistent application, however, a level of trust is integrated, and can people anticipate to the future use of their personal data. If consistency is not taken into consideration, there is a risk that things 'go weird' which can damage the percepted trustworthiness of an application. Showing the normal line of operation to a data subject makes it possible for users to estimate the future consequences of their actions. In addition, providing the user complementary information, e.g., in the form of markers, warranties, and seals can contribute to the trust of a data subject in data transaction parties.

6.2.2.2 User Consent

Legitimacy of data processing according to the principle of legitimate data processing, requires the unambiguous consent of the data subject. Consent is of major importance, because it changes an unlawful act info a lawful one. In this sense, consenting to data processing makes the difference between an infringement on privacy or an allowed use of personal data [Wes04].

Consent should be voluntary and in most of the cases shall be revocable. Moreover, influences of force, fraud, incompetence, and paternalism need to be rejected. In this respect, hierarchical relations deserve special attention. Because consent of a data subject can be influenced and manipulated by many factors, the Data Protection Directive (95/46/EC) stipulates that the data subject's consent shall mean any 'freely given specific and informed indication of her wishes by which the data subject signifies her agreement to personal data relating to her being processed' (Article 2(h) data protection directive).

It is very important for the data controllers to interpret the aforementioned legal provision correctly in order to avoid violations of the data protection legislation. An important issue is what 'freely given, specific and informed' means. Freely given consent shouldn't be conditional on an advantage or subject to negotiations on behalf of the data controller. The consent needs to be specific, meaning that it should be given for a specific and identified scope. Finally, it needs to be informed; the user shall get the appropriate and sufficient

information before the collection of the data and such information shall be in clear language and of course in a language that the data subject understands. In this last demand, we can see the relation with the requirement of consent with the previous requirement, 'information to the user'.

A highly debated issue is whether consent can be expressed in an opt-in or in an opt-out way. It is necessary that 'there must be some form of communication whereby the individual knowingly indicates consent'. This can be expressed by ticking a box, or sending an e-mail or subscribing to a service. For the processing of sensitive data, i.e., data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life, the data subject shall give her explicit consent, although Member States may even prohibit the processing of sensitive data, even with the consent of the data subject.

It shall furthermore be noted that the definition of consent explicitly rules out consent being given as part of accepting the general terms and conditions for an offered electronic communications service. Many contemporary services disregard this requirement. In current practice consent is usually obtained through the general terms and conditions of a service offering (in which the processing of personal data will occur). The picture gets even blurrier when the consent of the user is given in an environment that allows no or minimal user interface, such as in the case of most emerging technologies, like RFID, Bluetooth, etc.. Ambient Intelligent environments are based on the processing of personal data, and obtaining the consent of the data subject is often not taken into account in the designing phase of these systems.

Related to the requirement of consent is *choice* as an important social condition for true privacy-enhanced Identity Management, because consent implies a possibility for the user to choose whether or not to engage in a service and subsequently to choose how her privacy requirements are addressed in different services. When service providers use a 'take-it-or-leave-it' approach (viz. without offering different privacy options), it is impossible for users to withhold specific information from the focused attention of others. Individuals need to be enabled to choose for themselves the way they are portrayed to others, instead of being bound to predetermined identities and predetermined judgments. However, for the sake of motivation and feasibility, choice should not be exaggerated, but moderated and limited [Hey02].

Next to choice and consent, individuals also need to be able to set the boundaries in which their data is being used. Such *'confinement'* [JB05] relates to the purpose of use of data, but also to security measures. Data controllers may define the purpose of use and access to data too broadly or incomprehensively for the user resulting in an undermining of their privacy position. The user should therefore be enabled to define purpose of use and access to data, to avoid data leakage to others and/or to circumvent the use of data for unintended purposes ('function creep').

6.2.2.3 The Users' Right to Access the Data

User control would be a useless concept if individuals are unable to inspect whether actions with regard to data collection observe their policies. Ex-ante control is insufficient to ensure privacy. Moreover, data can be interpreted or presented wrongfully, users can make mistakes, change their preferences, or regret earlier decisions. Access to disclosed data is therefore necessary to enable users to check whether data controllers observe the agreements with them, observe the legal requirements, and to assess whether the data collected and processed is correct. Users should also be able to inform data controllers about possible errors or harmful behaviour by them. Just like 'information to the user' contributes to ex-ante transparency, the right to access data contributes to ex-post transparency and helps level the asymmetric power relation between data subject and data controller. The requirement of access to data furthermore relates to the general legal principle of data quality, because it allows users to notice and correct wrong personal data.

The Data Protection Directive grants various rights to data subjects with regard to the processing of personal data. The right of access to collected personal data states that every individual of which personal data has been collected and processed has the right to obtain from the data controller:

- confirmation as to whether or not her personal data are being processed and information at least as to the purposes of the processing, the categories of the data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to her in an intelligent form of the data undergoing processing and of any available information to the resources and of any available information as to their source.

Where any automated decisions (as defined in Article 15 of the Data Protection Directive) are involved, the data subject has the additional right to be informed about the logic involved in any automatic processing of data concerning her. All the aforementioned information must be available to the data subject 'without constraint at reasonable intervals and without excessive delay or expense' (Article 12 (a) Data Protection Directive). In addition and as regards to how the right of access is exercised, an ideal situation would include both online and physical access — the latter realised at the physical address of the data controller. However, in cases where physical access would entail disproportionate efforts and costs on behalf of the data controller (or if the data collected is disproportionately little), it is arguably accepted that the right of access can be exercised only through online means. In such a case however, the controller shall ensure via strong authentication mechanisms that the person requesting some information about the processing of personal data is the one entitled to do so, in order to avoid cases of identity fraud, identity theft etc.

As already mentioned, access and inspection contribute to the fairness of data processing and decreases the power imbalance between the strong party

(data controller) and the weak party (data sharer) in a data collection process. Access and inspection are thus countervailing powers. These powers should not only be applicable to the initial data collector, but throughout the *chain* in which a service is being delivered to the user. Services are often provided by combining the efforts of several organisations. The telecommunications sector for instance, has multiple parties engaged in the provision of one single service (see for instance Chapter 25). Furthermore, business processes and the data processing involved can be outsourced to other (specialized) parties. Users should therefore not only have insight in the phase of initial data collection, but also in phases such as subscription, payment, and integration of a service.

6.2.2.4 Rectification, Erasure, and Blocking of Data and the Right to Object

People can make mistakes or regret their decision concerning the dissemination of personal information. Initially, one can be tempted to disseminate personal information, as the benefits of personal data disclosure are much clearer than their disadvantages [Sta02]. Negative effects of data disclosure may occur later in time when people encounter undesired use of their data or even downright abuse of personal data. Apart from this reason to grant a right to withdraw data, people need to have the ability to decide to continue or modify their behaviour when their lives change or when personal data turns out to be wrong or interpreted incorrectly. IdM systems need to provide a level of 'forgetfulness' which is not present by default in the online environment [BJ02].

The 'right of access' to one's own personal data in the broad sense includes a right to rectify, erase, or block the data that relate to the data subject in cases where the processing does not comply with the requirements of the Data Protection Directive. For example, the data controller's collection of personal data may turn out to be disproportionate to the purposes, or when the data at issue are incomplete or inaccurate (Article 12 (b) of the Data Protection Directive). A common instance where data subjects exercise their right to rectify data is when their name is misspelled and they ask for correction. Furthermore, in the course of ex-post control over their personal data, the data subject also has the right to object (Article 14 and Recital 45 of the Data Protection Directive) to the collection and processing of her personal data. These aforementioned rights can only be imposed upon the data controller when the data subject has a legitimate right to do so and at the data controller does not have an overriding right to process the data. It is important to note that consent of the data subject is only one of different reasons according to which the processing of personal data can take place, so the right to object can not for instance be exercised in front of a data controller who deems that the processing is necessary for the performance of a contract to which the data subject is party.

Nevertheless, Article 14 of the Data Protection Directive stipulates the cases where the right to object can be exerted. Firstly, when the processing is

necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed and when the processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights for fundamental rights and freedoms of the data subject, Member States are obliged to grant the data subject a right to object at any time on compelling legitimate grounds relating to her particular situation to the processing of data relating to her, save where otherwise provided by national legislation. When there is a justified objection, then the processing instigated by the controller may no longer involve those data. Secondly, the data subject can object, on request and free of charge, to the processing of personal data relating to her which the controller anticipates being processed for the purposes of direct marketing, or 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 ePrivacy directive perceives the right to object and the right of withdrawal of consent in various situations. Therefore, the specific right is implicitly mentioned as a right to object to the installation of cookies, to the processing of traffic data processed for the purpose of marketing electronic communications services or for the provision of value added services, the processing of location data other than traffic data, to have her data available in directories of subscribers and to the processing of her personal contact information in order to receive unsolicited communications. In all the aforementioned cases, the data subject is given the right to refuse the provision of services or in cases where she has already accepted them, to withdraw her consent.

The requirement of 'access to information' would lose its value if subsequent actions cannot follow from this inspection of information. Thus, ex post user control by erasing, blocking, and correcting information is closely related to, and follows from, access and inspection. This requirement can serve the social need for 'forgetfulness', when people feel the need to get a 'fresh start' or 'second chance' in life [BJ02]. Moreover, a world in which people cannot make mistakes and nothing is forgotten is not a world conducive to the development of democratic and autonomous individuals. There of course is also a need to hold users accountable for their behaviour and the information they share which has to be balanced with data erasure. Also we have to take into account that the responsibility for the quality of data lies at the data controller. Because of this, ex-post user control by blocking, erasing, and rectifying information, is a balancing act between what is (legally) necessary to achieve accountability of the user, correctness of data, and the (legal) possibility to provide the user a control tool which can complement the data controllers' obligation with regard to the quality of data.

6.2.2.5 Data Security and Trust

An important prerequisite for user control is a secure infrastructure because if, for instance, third parties have access to the communication between data subject and data controller or to the collected data, user control is relatively meaningless. Therefore the data controller needs to take appropriate security measures. From a social perspective, the need for security is also related to trust, which is a highly relevant aspect for the success of online transactions. Even though trustworthiness and security are not the same, many users will not be skilled to asses the security measures taken by a data controller and therefore have to rely on trust marks provided, for instance, by institutions they do trust. Which institutions are trusted by individuals depends among other factors on context and culture.

Data security requires data controllers to take 'appropriate technical and organizational measures' (Article 17 (1) of the Data Protection Directive) against unauthorised or unlawful processing, and accidental loss, destruction or damage to the data. To the extent that this principle covers the security requirements and robustness of the network itself, this principle overlaps with the security and confidentiality requirements laid down in Articles 4 and 5 of the ePrivacy Directive (Directive 2002/58/EC). Taken as a whole, this principle imposes a statutory obligation on data controllers to ensure that personal data are processed in a secure environment. This means that the data controllers must consider the state of technological development and the cost of the implementation of any security measures.

Bearing in mind these factors, the security measures that are adopted by the data controllers must ensure a level of security that is appropriate to both the nature of data to be protected and the likely harm that would result from a breach of this principle. It follows that, the more sensitive the data, the more adverse the consequences of a security breach would be for the data subject, and therefore more stringent security requirements should be put in place.[3] This is especially the case as regards the processing of health related data. In any case, the data controllers should implement appropriate security measures to ensure that non-authorised personnel are unable to gain access to personal data. In addition, security precautions would suggest making secure back-up copies.

Security measures are of importance to ensure that boundaries for data processing determined by the user, are not crossed. Without appropriate security measures, confinement of data processing is thus not possible. Another relevant aspect when discussing security is that infrastructure and transaction partners need to be trustworthy. Security and or security marks can play a role in increasing and signaling trustworthiness. Not only should an organisation thus handle a secure transaction of data, they should also make these risks and their measures transparent to the user. The user needs to recognize the security and reliability of a technology and the trustworthiness of an

[3] See on this aspect also Section 7.3.

organisation, which is difficult to achieve because many users are laymen in the field of technology and security, and online transactions lack face-to-face interaction.

Trust is commonly conceived of as the assumption that another person, organisation, and its technology will not take advantage of the vulnerable party. Turned around, a trustworthy data controller should be trusted to attend to the interests of the data subject. By its very nature and by the differences in social context, trust is defined differently amongst social groups and individuals. However, some generally regarded trust marks — like trust seals — can contribute to the trustworthiness of an application and the organisation that uses the application.[4] These markers may originate from well-reputed organisations, and should not only apply to the specific security measures (which for most users are difficult to comprehend), but also to information about sources, providers, affiliations, and certificates of the data processor. A broad use of markers is necessary, whereas there is a general problem with regard to trust in technology: the information about security and trustworthiness needs to be tailored to the context of the (non-expert) user.

Trust in technology will often be combined with the trust in the partners one engages with. This is also important considering the adoption and use of a privacy-enhanced service. For the sake of trust and the adoption of a technology, complementary markers about reputation and brand of a data controller/service provider can therefore also be of importance.

6.2.3 Adoption of Privacy-Enhanced IdM in Society

Privacy is pursued in a specific social environment and has social importance, which effects the adoption of privacy-enhanced technologies. In addition, the adoption of privacy enhancing technologies relies on general aspects of technology adoption, like product aspects and market factors. Some of these market factors will be described in the next chapter. Some social aspects regarding the adoption of PETs will be elaborated in this section.

There is a plethora of privacy-enhancing technologies available on the market (some freely available), but adoption of these technologies by the individual seems to be difficult, even though people generally are concerned about their privacy in online environments [Sta02, BGS05, Sho03]. This demonstrates that adoption of a privacy-enhanced IdM system is not obvious. Given the importance of privacy for collective, common, and public values, broad adoption of PETs is desirable. Broad adoption, instead of use by only a few users, is also necessary in order to prevent 'digital divides', or 'digital inequality' regarding privacy protection online [DH01] and to create a multiplier effect. Thus, the ability to access and use technologies needs to be guaranteed for every online user in order to limit digital inequality in societies. In this respect, two aspects are important: *affordability* and *skill level*.

[4] An initiative to provide comprehensive privacy trustmarks is the EuroPrise privcay seal, see `https://www.european-privacy-seal.eu/`.

6.2.3.1 Affordability and Skill Level

The first requirement is affordability of privacy enhancing IdM solutions to a large group of users. There is a widespread notion that people are, at the moment, unprepared to pay much for privacy [Sho03]. There is no consumer market for privacy, because the benefits of ensuring privacy on an individual level do not seem to be clear and are difficult to define economically, whereas the benefits for giving up privacy are clear and often bring direct advantages [Sta02]. In this sense, affordability is related to the perceived usefulness of a privacy-enhanced IdM system. Information about the product and comprehensibility of its features can therefore influence the perceived affordability of a service. Currently, there does not seem to be a high level of the necessity of PETs amongst individuals, although privacy-awareness will probably be increasing when technologies become a part of our everyday life.

In addition, users should be able to use an application with a minimal amount of training. Not only actual access to the technology, but also skills and motivation can determine equality in society. Groups with relative low skill levels, like children or the elderly also make use of the online environment, and should also be able to protect their privacy. There is no homogeneous user group, and skills can even change between social groups or nations. Because of this, it is necessary that IdM systems can be used by non-skilled users and provide satisfactory default privacy settings.

6.2.3.2 Context and Social Settings

People value privacy differently. Some of us are 'privacy fundamentalists', whilst others may share personal data without hesitation. On top of this, situational factors add complexity, because the use of identities and identity-related information is adjusted to the environment and the kind of interaction people engage in. Thus, information that is considered private changes throughout situations. One can for example relate to the difference between sharing information at a crowded helpdesk or at a birthday party, or to the difference between disseminating personal data to authorities or best friends. Moreover, sharing medical data with a doctor may not be considered privacy sensitive, but sharing the same data with a real estate agent may be completely different. These examples illustrate that it thus is difficult to point out beforehand the different kinds of sensitivity of data.

IdM systems must pay attention to the contextuality of privacy. They need to give individuals the possibility to change privacy settings according to context. This does not simply mean that there is a distinction between 'private' and 'public'. Privacy is not a button which can be switched on, or switched off. Even within the public and private spheres, different privacy perceptions exist. Hence, different privacy features need to make it possible to fine-tune preferences to contextual privacy settings.

Moreover, the individual is not the only actor that determines the privacy-sensitiveness of situations. Social settings have an influence on the use of IdM systems, because understandings of privacy and privacy perceptions vary across social groups, societies, age, and cultures. History and political regime can, for example, influence the perceptions on privacy, just as media coverage, general respect towards government, or recent social debate [Pro06]. In addition, language settings, symbols, and icons are different between societies. IdM systems that need to be adopted broadly, and which want to enhance privacy according to many social settings, need to be adjustable to these settings.

The other way around, the society and legislator can also impose 'norms' on the exercise of privacy that determine occasions in which a claim on complete privacy cannot be accepted. Society and the legislator may therefore impose requirements for accountability to the design of IdM systems. For the adoption of IdM systems, it is important that accountability can be assured in specific instances. Vice versa, society can also not afford that people give up their privacy completely as we have argued in chapter 4. This also means that society has to take the requirements outlined in the Data Protection Directive seriously and not allow people to freely contract away their privacy.

6.2.3.3 Accountability

The first requirement of this chapter, audience segregation, points towards instruments that allow people to create, maintain, and protects partial identities. However, society and legislator may impose restrictions on the identities used by individuals. In some occasions, anonymity, or a specific pseudonym may be undesirable. Hence, just as there are rationales for anonymity, or pseudonymity, there are rationales for identifiability or accountability. One can think here of governmental regulation but also of relationships in which accountability is required, like parent-child relations and employer-employee.

Norms for accountability can be imposed by legal means, but also by social groups. There are thus *de facto* and *de jure* regulatory powers, which may in turn have an extra-territorial effect. Examples here are for instance the regulation considering fraud prevention in multinational organisations, but one can also think of demand for accountability by interest groups, like the public outcry for transparency of the income of CEO's.

Not in all cases it is thus desirable to interact anonymously or with pseudonyms. IdM systems need to take this into account because otherwise they may become considered illegal or undesired. For accountability of an individual, IdM systems must sometimes reveal identities, or credentials must be assigned to ensure that an actor meets to some demands. However, an important condition to implement a mechanism of accountability into a privacy-enhanced IdM system, is that individuals can trust that accountability is only required in concrete and specific occasions.

6.2.3.4 Trust

We have already touched upon the aspect of trust in the requirement of data security. It needs to be stressed that trust and security are not the same. People trust people, not technology [FKH].[5] Therefore, technology can be proven to be trustworthy, but in order for user to actually trust the technology and the relationship with a service provider requires more than just reliable technology. As users will not be skilled to assess the reliability of a technology, this needs to be made transparent and accessible to the user. Furthermore, the look and feel of a technology and markers of quality and functionality are considered important factors in the creation of trust. Especially markers about the authority or credibility of the makers and providers of a service are of importance.

In the online environment, consumers perceive their transactions to be more riskier than transactions in traditional channels. This can be attributed to the fact that the transactions take place without face-to-face contact, but also because much more personal data is disclosed online than offline. Also experience with concrete online transactions is relatively low, the variance in online transaction procedures is much higher than in offline transactions; the steps in a transaction process are often not clear, even though service providers have an obligation to make them clear to the user. It appears that, with a lack of face-to-face contact, users need to rely more heavily on brand name, reputation, past performance, and other information. When designing privacy enhanced identity management solutions it is important to try to understand what the appropriate trust markers are that help people consider the technology trustworthy, provided that the technology is trustworthy of course, and that the data controller can be trusted too (see also [ACC+05]).

6.3 Conclusions

In this chapter we have given a brief high level overview of requirements for privacy-enhancing identity management systems from the perspective of the individual. An extensive and detailed account of these requirement, the legal requirement, and the business requirements can be found in PRIME Deliverable Requirements V3 [KDR+08].

An important aspect of identity management from the perspective of the individual pertains to how individuals present themselves to others. Individuals operate in different spheres and present different aspects of themselves to others in these different spheres because they play different roles and have different interests. The possibility to keep different spheres separated is an important characteristic of modern states. In an online environment this kind of audience segregation requires special attention and implies a number of requirements. A central requirement to facilitate audience segregation is user

[5] Even though this may turn out to be a wrong assumption.

control which can be decomposed in a number of more specific requirements. This chapter has briefly elaborated on the various requirements from a joint social/legal perspective, starting with audience segregation to be followed by the ten requirements that together constitute the control requirement: 'comprehension', 'consciousness', 'consent', 'choice', 'confinement', 'consistency', 'context', 'inspection', 'chain control', and 'ex-post user control'. After these, six adoption requirements were discussed: 'social settings flexibility', 'minimize skill level', 'accountability', 'trust in transaction partners', 'trust in communication infrastructure', and 'affordability'.

The requirements discussed are mostly complementary, but on several occasions, a balance between them needs to be struck by the developer and the provider of a service. Privacy, and thus also control and adoption, are dependant on the situation in which a service is implemented.

The requirements presented in this chapter are rather abstract and as such not immediately useful for developers. The PRIME Deliverable Requirements V3 [KDR+08] discusses them in much more detail and also provide measurable targets. For instance, the comprehension requirement (SR.A2 Comprehension) is formulated as: "The user should understand how personal data is handled by the service provider."

Whether the application satisfies this requirement can be examined by answering questions such as:

- Does the application provide sufficiently comprehensive explanations of the consequences of relevant events with respect to the collection and use of (personal) data?
- Does the application provide sufficient general information about (personal) data, its collection and use?
- Does the user understand the application itself?
- Is the user documentation sufficient in scope and understandability?
- Is the user not overloaded with information through too many or too detailed notifications and explanations?

Apart from the legal and user perspective there is also the business perspective to take into account when developing privacy-enhancing identity management applications. The requirements this perspective brings about will be addressed in the next chapter.