Chapter 14
Towards a European eID Regulatory Framework

Challenges in Constructing a Legal Framework for the Protection and Management of Electronic Identities

Norberto Nuno Gomes de Andrade

14.1 Introduction

The difficulties, barriers and challenges in implementing a regulatory framework for a pan-European electronic identity (eID)1 have been analyzed before in a number of studies. Deliverables pertaining to research projects funded by the European Union (EU), as well as study reports prepared for the European Commission in the areas of eID and eGovernment,2 have focused on the legal complexities that currently hinder the realization of a pan-European eID scheme. In this respect, researchers and scholars have devoted more attention to legal barriers than to possible legal solutions. This paper attempts to fill this gap, and also to contribute to research on both these analytical dimensions. The article first summarizes the main legal obstacles and challenges to the implementation of a pan-European eID scheme and then suggests a conceptual framework of principles to address these challenges and overcome the obstacles. In summary, this paper contributes to the ongoing debate on the benefits of a regulatory framework for an electronic identity scheme for Europe by presenting a number of legal proposals that could facilitate the realization of such a scheme.

The views expressed in this article are purely those of the author and may not in any circumstances be regarded as stating an official position of the European Commission.

1 See Appendix Terminology for the definition of the most relevant concepts and terms regarding electronic identity (eID) and electronic identity management (IDM) systems.

2 This has been the case of studies done in the ambit of research initiatives such as the ones led by the Porvoo e-ID Group, Stork, MODINIS, and the IDABC program, as well as studies such as the European Commission (2005), prepared by the eGovernment subgroup of the eEurope Advisory Group.

N. N. G. de Andrade
Institute for Prospective Technological Studies (IPTS), European Commission, Joint Research Center (JRC), Seville, Spain,
e-mail: norberto.andrade@ec.europa.eu

The article is structured as follows. Section 14.2 describes the relevance of eID for the general development of the information society. I will assess the importance of electronic identity for administration (public), business (private) and, above all, citizens. I will also highlight the role of eID as a key enabler of the economy.

Section 14.3 identifies the various legal gaps and barriers in the current EU legal framework that are hindering the creation of a fully-fledged pan-European eID. I will examine the following issues: the legal blurriness of EU competences in the field of eID; the divergence (and, sometimes, incompatibility) of approaches pursued by different Member States in the regulation of eID; the lack of a harmonized EU legal taxonomy in this area; and the uncertainties about the legal treatment and control of identity-related data used in eID transactions. This examination clearly shows that appropriate regulation regarding eID at European level is still lacking, as the current EU law does not provide a specific legal framework for eID. At the moment, legal regulation of eID is composed of principles, rules, and concepts “borrowed” from different EU legal instruments and national laws that could be better articulated to address the current state of legal fragmentation.

Section 14.4 presents a number of legal proposals which aim to embed electronic identity into the EU regulatory framework. A series of new principles that should underpin a future eID legal scheme are elaborated: the principles of user-centricity, anonymity and pseudonymity and the principle of multiple identities, identity portability, un-linkability and negotiation, among others.

14.1.1 Nota Bene

Before moving on, one important remark regarding the focus and scope of this paper must be made. This paper is devoted to the legal aspects of eID. Hence, I will be looking at the main barriers to the construction of a pan-European electronic identity scheme and the possible solutions from a strictly juridical point of view. Nevertheless, technological and organizational aspects of eID will also be taken into consideration.

---

3 It is also important to bear in mind that the scope of this article is limited to the management of the digital identities of individuals or natural persons. I am fully aware that issues concerning the management of online identities for entities or objects (namely through RFID tags) are growing in importance, but these are outside the scope of this paper.

4 The analysis of the “specific barriers”, or better, the analysis of the legal gaps which derive from particular legal instruments in EU law vis-à-vis the need to effectively and comprehensively regulate eID—namely from the three most relevant European directives in such area (the Data Protection, the eSignatures, and the Services directives)—go beyond the scope of this article. Nevertheless, and just for cataloguing purposes, one could mention the shortcomings of the current identifiability model of the data protection legal framework and the need to regulate the processing of certain instances of non-personal data as legal gaps of the data protection directive regarding the need to regulate eID. For further details, see (Andrade 2011a). In terms of specific issues missing from the eSignature directive that need to be solved in order to attain a successful implementation of a pan-European eID scheme, one could mention the lack of issuance procedures and the lack of a definition concerning the content and verification of eID. In this sense, see (Myhr 2008).
Towards a European eID Regulatory Framework

(EEuropean Commission 2003). In fact, the technical and infrastructural elements of eID contribute directly to the formulation of the legal solutions proposed here. As we shall see later on, many of the new legal principles proposed are in fact derived from technological design principles, having already been tested in numerous research projects and technical prototypes. I will thus present a set of legal principles with a strong technical ascendancy.

In view of the intricate relationship between legal and technical aspects that this article will establish and address, I consider that the main challenge to European eID is not only technological but also legal. It is important to note that the technology necessary to enable an interoperable eID across Europe already exists (Modinis-IDM-Consortium 2006, 7). What is missing, in reality, is legal interoperability. It is the lack of legal harmonization that most inhibits cross border deployment of services based on electronic identity. Having said this, the article will focus on the legal framework that must be constructed in order to accompany and enforce the existing technological answers, transposing some of the latter into operating full-fledged legal principles. In brief, the scope of the article is to identify the legal gaps and propose a number of principles that, ideally, could form the basis of a common EU legal framework for the protection and management of digital identities.

14.2 Relevance of eID

This section emphasizes the increasing socio-economic relevance and importance of electronic identities and examines how eID has been targeted by international organizations and by EU political agendas, declarations, action plans, and research funded projects.

In reality, the need for a balanced mix between law and technology is not new. This alliance has been widely advocated under the label of “privacy by design.” In this regard, the European Commission noted in 2003 that “... the use of appropriate technological measures is an essential complement to legal means and should be an integral part in any efforts to achieve a sufficient level of privacy protection.” In the context of eID and taking into account the need to achieve a sufficient level of identity protection, I believe that technology should also contribute to an “identity by design.”

Microsoft, Shibboleth, Liberty Alliance, Passel, Sxip and other technology companies and consortia have devoted efforts to building digital IDM systems and tools.

In effect, as the Modinis Interim Report observed: “A commonly heard remark is that for any given technical difficulty in the IDM sector the problem is not the unavailability of technical solutions, but rather an overabundance of possible solutions. Overlooking legal, cultural and socio-political perspectives, from a strictly technical point of view most hurdles to interoperate IDM systems would be fairly easy to overcome”. One may therefore conclude that the most difficult obstacles posed to the creation of a pan-European eID are not technical, but are derived from the different legal approaches and socio-political sensitivities of EU Member States.

In other words, the article does not focus directly on interoperable technical mechanisms and infrastructures enabling EU citizens to identify and authenticate themselves. The article, instead, focuses primarily on the legal framework that must be put into place in order to allow identification and authentication procedures to be carried out.
There is undoubtedly an increasing need today for identification and identity management. The development of ubiquitous networks of electronic communications and the general trends of globalization and increasing human mobility give rise to the need to ascertain “who is who” on the internet, in the street, in the usage of services, and in commercial transactions. Large investments made by governments and companies are becoming essential for the provision of eGovernment services and interaction with the public administration—and also for the provision of commercial services and the deployment of marketing strategies—which aim to learn as much as possible about a potential customer’s needs, habits, and preferences.

eID also brings various societal and economic benefits to European citizens. The ability to interact and transact remotely with various institutions and entities allows users to benefit from the provision of a wider number of services, most of which were previously only available through a physical visit. Moreover, eID based services will also increase the efficiency and convenience of use. Citizens will be able to access these services at any point of the day (24/7 availability) and from any geographical location (e.g., services that can be accessed through a mobile phone). The increased availability, efficiency, and convenience brought by services that rely on eID will also result in monetary gains for the users and have a positive impact on the environment.

As a result, electronic identity has become a key driver for the growth of the EU economy and the completion of the Single Digital Market. eID constitutes not only a fundamental enabler for the deployment of cross-border services within the EU27, but also an indispensable element for the increase of entrepreneurial activities in Europe. As observed in the Digital Agenda, “[e]lectronic identity (eID) technologies and authentication services are essential for transactions on the internet both in the private and public sectors” (European Commission 2010b, 11).

In view of this, “it is clear that divergent rules with respect to legal recognition of eID and electronic signatures create barriers to the use of electronic communications and electronic commerce, and hinder the free movement of goods and services in the internal market” (Myhr 2008, 77). Therefore, the lack of a harmonized regulatory framework may not only create privacy and security issues affecting the construction of trustworthy online environments but may also compromise the development and the productivity of the increasingly interconnected and globalized economy in which we live, hampering the ability of entities to provide users with suitable services and applications.

Thus, interoperable electronic identities, at the European level, have been deemed essential for achieving the freedom of establishment and circulation of goods, capital

---

9 Many EU Member States such as Germany have in the recent times deployed large scale eID projects (see Graux et al. 2009, 120), many of which are presently underway.

10 Such strategic document envisages, moreover, specific and concrete actions in the field of eID. This is the case of Key Action 16, according to which the Commission will “[p]ropose by 2012 a Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online ‘authentication services’ to be offered in all Member States (which may use the most appropriate official citizen documents—issued by the public or the private sector)”.
and services (Leenes et al. 2009). eID is also considered to be indispensable for the completion of the digital internal market, reducing administrative burden throughout Europe and allowing the EU-zone as a whole to attain a better competitive position (Leenes et al. 2009)

Consequently, the relevance of eID and the need for interoperable eIDs has been recognized in EU agendas and strategies (European Commission 2010c), action plans (European Commission 2010a),11 declarations,12 communications (European Commission 2010d),13 studies (European Commission 2007),14 and programs.15

The EU has also financed and supported a vast amount of research and practical implementation projects focusing on electronic identity and interoperability (see Table 14.1).

In addition to these projects, there are many other international networks and research centers in Europe carrying out important projects in this area, such as the PETWEB II16 and the Porvoo Group.17 Though they entail different approaches, methods, case-analysis and technologies, all these research initiatives have contributed to the development of generalized frameworks for trust and privacy-protective identity management (IDM) systems across Europe.

---

11 In such Action Plan, the Commission has proposed a European Strategy on IDM to be attained by 2012, which includes legislative proposals on criminalization of identity theft and on electronic identity (eID) and secure authentication systems.
12 Such as the Manchester Ministerial Declaration (2005) and the Lisbon Ministerial Declaration (2007).
13 Such as the recent Communication from the European Commission (2010d).
14 Namely the following studies: Commission, “Signposts Towards e-Government 2010.”
15 Such as the Stockholm Program, which defines the framework for EU police and customs operation, rescue services, criminal and civil law cooperation, asylum, migration and visa policy for the period 2010–2014.
16 http://petweb2.projects.nislab.no/index.php/Main_Page
17 http://www.vaestorekisterikeskus.fi/vrk/fineid/home.nsf/pages/6F4EF70B48806C41C225708B004A2BE5
Furthermore, the need to develop an eID operational framework also stems from EU legal texts and instruments. Several single market initiatives and legal frameworks presuppose and rely on cross-border interactions between administrations, businesses, and citizens across Europe. Thus, the need to deploy a pan-European eID scheme also derives from EU-enacted legislation itself.¹⁸

Nevertheless, despite the various political declarations and initiatives in this area, the plethora of research projects, the proliferation of IDM systems and the wide array of advanced eID technologies, the creation of an encompassing, interoperable, pan-European eID scheme has not yet been accomplished. The fundamental reason for this, other than the organizational and technical challenges to interoperability that need to be addressed, is the presence of legal gaps and barriers in the EU legal framework. The main legal gaps and obstacles that hinder the creation of a full-fledged pan European eID are identified in Sect. 14.3.

14.3 Legal and Technical Barriers

This section describes the main barriers (encompassing both technical and legal difficulties) to the creation of a pan-European identity management infrastructure, which would allow existing national IDM systems to interoperate. In the analysis and description of these obstacles, I shall examine what one could call the ‘general’ barriers to a pan-European eID, that is, the obstacles that are not necessarily attached to any specific piece of legislation.

Although the article is mainly focused on legal barriers, I shall start with a fundamental technical barrier that is the Internet’s lack of a proper identity infrastructure. As explained in the PRIME research project White paper

The internet, by design, lacks unified provisions for identifying who communicates with whom; it lacks a well-designed identity infrastructure (Leenes et al. 2008, 1).¹⁹ Instead, technology designers, enterprises, governments and individuals have over time developed a bricolage of isolated, incompatible, partial solutions to meet their needs in communications and transactions. The overall result of these unguided developments is that enterprises and governments cannot easily identify their communication partners at the individual level (Leenes et al. 2008, 1).

In certain contexts, the lack of an Internet identity infrastructure may not constitute a problem, promoting for instance freedom of expression (allowing people to freely express their ideas and opinions anonymously or through pseudonyms in online forums, for instance). In other contexts, the lack of an Internet identity infrastructure

¹⁸ This is the case of the Directive on Services in the Internal Market (2006/123/EC), which article 8 constitutes an example of the necessity of interoperable eID, stating that “[…] all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means […]”

¹⁹ In effect, “[t]he Internet has an ID infrastructure often identifying only the endpoint of a communication: IP addresses. These are often unreliable to identify users” (Leenes et al. 2008, 1).
may hinder individuals, forcing them to ‘over-identify’ themselves, and disclose more personal data than is strictly necessary. Unlike real-world transactions, which can often be conducted in an anonymous fashion (by paying with cash without leaving any identity traces, for example), most online dealings require excessive disclosure of identifying data (this normally happens with online shopping, where detailed personal data is usually required to perform the transaction). At a more systemic level, the absence of an Internet identity layer also hampers commercial transactions and official government interactions, which rely on the proper identification of customers and citizens to provide their services.

14.4 The Diversity of Technical and Legal Approaches to eID, the Proliferation of Identity Management Systems and the Emergence of New Actors

One of the major factors blocking the development of interoperable IDM systems across Europe is the diversity (and, often, incompatibility) of technical and mainly legal approaches to the protection and management of electronic identities by EU Member States. As observed in previous studies and surveys (Graux et al. 2009, 106; Leenes et al. 2009, 25), EU Member States take different approaches to eID management systems, varying from the use of specific Public Key Infrastructures (PKI) and the inclusion of eID in non-electronic identity tokens (such as identity cards, driver licenses) to reliance on electronic signatures and two-factor authentication systems.

In addition to the variety of technical approaches, there is also a legal diversity of regulatory options and rationales. In this respect, while some EU Member States have developed national eID cards (such as Austria and Germany, among many others), others do not have an operational national identity card scheme (United Kingdom and Ireland). Furthermore, EU Member States also differ regarding the choice or not of unique identifiers, with some countries using national identification numbers for a wide variety of purposes and contexts, while others use several identification numbers with each one serving a single purpose within a specific context. It is worth noting that the use of unique personal identification numbers for multiple purposes and contexts has been considered unconstitutional in a number of countries (such as Germany, Hungary, and Portugal, among others).

---

20 This does not necessarily mean that unique identification numbers cannot be used in these countries, but that their use should be restricted to a specific context. In this way, countries tend to decree the use of separate sectoral identifiers (namely for tax and social security purposes). The use of sector based identifiers is, in effect, finding increasing adoption, partly as a consequence of the above mentioned constitutional restrictions.
Due to divergent legal regulation and organization in EU Member States, there is a proliferation of different IDM systems, which render the eID process more and more complex. Furthermore, new actors and institutions are emerging in the data processing and eID fields.

We have thus surpassed the simple phase of having the same entity acting as both identity certifier and service provider. Today, there is a tendency to separate identity providers from service providers. Identity providers, on the one hand, act as trusted third parties, authenticating a user’s identity. These entities, in addition, store user account and profile information. Service providers, also called ‘relying parties,’ on the other hand, accept assertions or claims about users’ identities from the identity providers in order to offer them their services. Under a user-centric identity system, for instance, “[u]sers are allowed to choose identity providers independently of service providers and do not need to provide personal information to service providers in order to receive services” (OECD 2009, 17). In this model, users not only select what information to disclose when dealing with service providers, they also use several identity providers as well. They thus avoid storing all their information in one place (OECD 2009, 17).

We are thus confronted with an increasingly complex scenario, encompassing a wide set of actors such as identity holders, identity providers, registration authorities, and authenticating authorities. Hence, in a typical eID management system, identity-related data is not simply sent or provided by a subject to a controller; rather the data is, in the process, authenticated by a third party. This new actor corroborates the authenticity of the citizen’s/customer’s identity, and then gives the trusted information to the public or private entity providing the service. We thus have identity providers and relying third parties. It is important to note that in these cases there is no explicit legal framework (Graux et al. 2009, 119).

In addition, and given the wide variety of technical and legal approaches followed by Member States, a fully-functional pan-European eID needs to articulate flows of data between eID holders, receiving parties, and certifying authorities from different countries. This can be quite a challenge (not only technically but also legally) when the receiving party has to handle eIDs from several certifying authorities, based in different countries and following different eID schemes, and the same challenge applies to certifying authorities, which “will have to relate to many receiving parties in different countries if they want eID holders to be able to make generic use of their eIDs” (Myhr 2008, 81). It is thus perfectly possible and probable that a relying party is situated in a different Member State from the one that has assigned the electronic identity. In these cases, the relying party will need to verify the eID at the authentication party in another Member State. Hence, cross border flows of eID

---

21 Four main models of IDM systems can be identified within the massive proliferation of eID systems: the “silod”, the centralized, the federated and the “user-centric” IDM systems. For a detailed explanation of each of them, see OECD (2009, 16–17).

22 One should bear in mind, though, that, in some circumstances, these different actors can coincide in the same entity. For example, an identity provider can also be an authentication authority, and a registration authority might also be an identity provider.
information can take place between the eID holder and the relying party, as well as between the relying party and the authenticating authority.

Another problem likely to emerge from this increasingly complex scenario is related to compliance with the Data Protection Directive rules. These require unambiguous consent from the data subject (the identity holder, also denominated the claimant), which may become complex when the data is not provided by the claimant directly (in an online form, for instance), or when data cannot be obtained from a certificate presented by the claimant (when taken from a certificate on a smart card inserted into a reader the claimant uses in the interaction) (Leenes et al. 2009, 32).

This is the case “when the service provider (relying party) needs to obtain additional data, such as (certified) attributes and these can be, or even have to be obtained, from other sources than the user.” (Leenes et al. 2009, 32).

As noted by specific eID research programs, these new generations of IDM systems “do not provide adequate safeguards for personal data and give individuals a limited control over their personal data” (Leenes et al. 2008).

The increase in different IDM systems and models poses also problems of accountability and transparency for how they are managed and operated, namely in terms of ascertaining responsibilities in case of an incident. The dilution of accountability and transparency of these systems will mainly affect the citizens and the consumers. Given the myriad of different digital identification systems and techniques, the registration and transfer processes for identity data will probably be less transparent. As a consequence, citizens and consumers will certainly have more difficulties in making informed choices as to which IDM systems to use.

14.4.1 EU Legal Competences

The problem of the distribution of competences between the EU and its Member States regarding a potential legislative action in the field of electronic identity is at the root of the increasingly diverse legal and regulatory approaches pursued by EU Member States.

Any proposal for EU legal intervention and regulation in the field of eID must analyze two important elements: competence and legal basis.

Firstly, an EU Institution adopting a legislative act in the area of eID must have the competence or the legal power to do so. Secondly, the legislative act (a Directive, for instance) must have a legal basis, and reference must normally be made in the recitals to the concrete enabling power, generally to be found in the Treaty itself.

---

23 The basic principle underpinning legal basis was expressed in Case 45/86, Commission v. Council (Generalized Tariff Preferences) where the ECJ expressed the opinion that: “the choice of a legal basis for a measure may not depend simply on an institution’s conviction as to the objective pursued but must be based on objective factors which are amenable to judicial review.”

24 In the case of delegated legislation, those references are located in an enabling legislative act.
In this manner, the main task is to find a way to legally anchor an eventual eID regulatory initiative to EU Law (both through Treaties and EU secondary legislation), that is, to identify specific area of EU competence and to specify a legal basis for a regulation regarding the implementation of a European eID system.

The relevant Treaty provisions concerning the issue of competences can be found in articles 2–6 of the Treaty on the Functioning of the European Union (TFEU). Three different categories of competence can be identified: exclusive, shared or complementary, and supporting or supplementary (Craig 2008, 8). A brief survey of the different areas and categories of competence immediately confronts one with the considerable difficulty of assigning an eID regulatory initiative to a specific area of competence. This has to do with the fact that the regulation of (personal) identity covers a very wide field, cutting across a broad range of different EU areas and policies. Looking, on the one hand, at the distribution of competences between the Union and the Member States and, on the other hand, at regulating eID at the EU level, it is easy to see that the latter may involve different categories of competence at the same time (such as shared competences and competence to support, co-ordinate, or supplement) or different areas within the same category of competence. Therefore boundary problems may arise between the categories of competence to support and shared competences when inserting eID into the EU legal framework. For example, eID could come under the internal market, which is shared power, or it could be regarded as falling within administrative co-operation, where only supporting action is allowed. Furthermore, the regulation of eID may also affect distinct areas within the same category of competence, such as the internal market, consumer protection, and the area of freedom, security, and justice (among others).

Thus, the EU does not seem to have a direct mandate to regulate eID. Furthermore, regarding the distribution of competences in eID between the EU and Member States, it is worth mentioning paragraph 7 of article 8 of the DPD:

Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

In other words, the requirements for processing these identifiers are to be defined by the Member States.

Moving from the topic of competences to the issue of legal basis, a legal disposition that could be invoked to sustain an EU legal regulation of eID is Article 25 In more detail, such three categories are the following: Exclusive competence, according to which only the EU can legislate and adopt legally binding acts, the Member States being able to do so only if empowered by the EU or for the implementation of EU acts; Shared competence, which constitutes a 'general residual category,' (Craig 2008, 8), as it provides that the EU shall share competence with Member States where the Treaties confer on it a competence which does not relate to the areas referred in articles 3 and 6 TFEU (such dispositions deal, respectively, with the category of exclusive competence and with the category of which the EU is restricted to taking action to support, co-ordinate, or supplement the action of the Member States); Competence to support, co-ordinate, or supplement, which allows the EU to take action to support, co-ordinate or supplement the actions of the Member States, without thereby superseding their competence in these areas, and without entailing harmonization of Member State law (article 2(5) TFEU).
77(3) TFEU. This article, contrary to the former EU Treaty, now allows for the adoption of measures and provisions on identity cards. Despite this innovation, the possibility of adopting such measures is still somewhat restricted, and requires a special legislative procedure (unanimity in the Council and a merely consultative role for the European Parliament). Furthermore, article 77 TFEU comes under the heading of border checks and immigration policies, and deals with identity cards. For these reasons, article 77 does not seem to be a suitable legal basis for eID, which encompasses electronic communications, covering a much wider spectrum of EU policies and areas. Nevertheless, Article 77(3) TFEU stands as a very important first step in legally framing identity in the EU Treaty, placing eID within the EU legal framework.

14.4.2 Control over Personal Data

The issue of control over personal data is not new, but it is intensified by the emergence of different IDM technical models for processing personal data.

Despite not being new, this issue is certainly exacerbated by the massive deployment of eID systems. This is particularly the case when personal data is re-used outside of the context in which it was initially granted, which, in principle, contravenes the provisions of the Data Protection Directive. Another related problem is the disclosure of more information than is actually needed for the purpose of the application. These situations contravene the provisions and the principles of the above mentioned Directive, namely the principles of fair collection and proportionality.

Depending upon the architectural model for the IDM system chosen, identity information may be stored in a myriad of different places and entities. In the case of Siloed IDM systems, identity information is stored in separate service provider accounts; in centralized IDM systems, however, it is stored in one main account. In addition, while in federated systems, the identity information is kept in separate accounts and in different locations by different service providers; in user-centric systems, identity information is stored by identity providers chosen by the user. These last two systems, despite their advantages over the former ones, offer no way of safeguarding data after it has been shared (OECD 2009, 18). In federated systems, users have little input into the business-partner agreements, and lose track of their data once it has been shared amidst the federation members. In user-centric systems, there is instead the risk of concentration in the market for identity providers, which would then undermine users’ control over their own information.

---

26 Article 77(3) TFEU: “If action by the Union should prove necessary to facilitate the exercise of the right referred to in Article 20(2)(a), and if the Treaties have not provided the necessary powers, the Council, acting in accordance with a special legislative procedure, may adopt provisions concerning passports, identity cards, residence permits, or any other such document. The Council shall act unanimously after consulting the European Parliament.”
14.4.3 Lack of Common Taxonomy

The lack of a suitable, homogenous, unambiguous, and consistent terminology applied to the eID field has been identified by a series of studies and project deliverables.\(^{27}\)

A legal taxonomy for eID\(^{28}\) is not only lacking at the level of European legislation but also at the national level. The eID Interoperability for PEGS Analysis and Assessment Report interestingly noted that, in the countries surveyed, there is no legal definition of the concept of identity, and more importantly, of how an identity can be established in an electronic environment (Graux et al. 2009, 118). Austria comes closest to a legal definition in its eGovernment Act:

Unique identity: designation of a specific person by means of one or more features enabling that data subject to be unmistakably distinguished from all other data subjects (Graux et al. 2009, 118).

Despite the general absence of regulatory frameworks detailing and defining what elements legally constitute an entity’s identity, what authentication is and what specific requirements it entails, IDM systems do exist and operate. This is so because technology has stepped in and moved forward, regardless of law. The absence of law and legislation has not prevented technology from being developed, implemented, and applied in the field of eID.

An example of ‘technology implementing law,’ namely with regards to complying with the requirement for user consent, can be found in Italy where personal data is actually encrypted and cannot be accessed directly without the user’s consent (Graux et al. 2009, 128). In this way, technology reinforces the principle of user control over personal data in electronic authentication processes.

As a result, technology seems to be providing the values of certainty and predictability in the regulation of relationships that law should provide. This point is well illustrated by the PEGS study, which remarks on the absence of legislation applicable to authentication processes and the role of PKI signature technology as an entity authentication mechanism.

The mains reason for this is that, even if the legal framework does not strictly speaking address all relevant issues, the technology/technique behind PKI-based electronic signatures can still offer a large degree of certainty with regard to the entity using an electronic signature (especially when qualified certificates or qualified signatures are used), so that the use of electronic signatures is de facto an adequate tool for authentication, even if the legal basis for it is non-existent (Graux et al. 2009, 119).

As such, most of the current eIDM systems are working not on a ‘legal basis,’ but on a de facto ‘technical basis.’ There is thus a need to reintroduce law in this area in a way

\(^{27}\)This is the case of the Modinis-IDM-Consortium (2006) Modinis Deliverable: D.3.9 IDM Issue Interim Report III. In addition, the Modinis project developed a specific Terminology Paper (Modinis-IDM-Consortium 2005).

\(^{28}\)See Appendix Terminology for an overview of the terminology use in the field of eID.
that assumes its regulatory functions accompanied by technology, and not replaced by it. It is exactly in this context, in order to re-articulate the relationship between law and technology that I will propose the principle of technological assistance.

### 14.4.4 Legal Barriers and Challenges: Conclusions

As a conclusion to our brief analysis of the legal barriers and challenges to a European eID—and reinforcing what has already been stated in similar studies—it is evident that an explicit legal framework for eID does not exist. As Myhr observed, “[e]ven though existing laws that regulate a paper-based environment and physical ID-cards to a large extent can also be applied to electronic communication and the use of eIDs, an appropriate regulation regarding eID on a European level is lacking” (Myhr 2008, 77) Furthermore, the application of the current EU legal framework (namely of the Data Protection, eSignatures and Services Directives) to eID is not sufficient to cover all the aspects involved in the protection and management of electronic identities. What could be described as the current legal framework applicable to eID is deeply fragmented, borrowing some elements from the Privacy Directive, the eSignatures Directive, national regulatory approaches and legislation, and others from technically-implemented solutions. In brief, there is no global view or overview of what is to be regulated and how.

### 14.5 Legal Solutions

As van Rooy and Bus observe, Europe needs a legal framework that “[e]nsures interoperability for trustworthy authentication across service domains of Member State public authorities, business and citizens” (van Rooy and Bus 2010, 403), allowing for “EU-wide trustworthy service provisioning in domains such as e-government, e-health, e-commerce, finances and social networks, and hence should support the provisioning of multiple identity instances from government-accredited to commercially accepted, ranging from strong identification to anonymity (van Rooy and Bus 2010, 403).

In order to render different national and regional IDM systems interoperable within the EU, there is not only a need for technical interoperability, but also a fundamental need for legal interoperability. This section attempts to contribute to the latter by providing a series of common principles that are currently lacking from EU law and that could be contemplated in order to foster the vision of a pan-European eID scheme.

From the 1980’s onwards, various international arrangements have formulated a number of key principles for the protection of personal data. This is the case of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted by the Organization for Economic Cooperation and Development (OECD)
in 1980, and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the Council of Europe in 1981. In the 1990s, the EU’s Data Protection Directive (DPD) made a substantial contribution to this legislative effort with a list of principles stipulating the conditions in which personal data should be processed. These initiatives have enshrined an extensive list of principles regarding data collection, storage, and processing. These principles include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.29

As an addition to these existing principles, this section presents a series of legal principles and rules that, added to the current EU legal framework, fill some of the gaps in EU law and contribute to a more comprehensive and specific regulation of eID. These principles could also be seen as the foundations for a new shared European eID regulatory framework.

Relying upon the work done by initiatives and studies carried out in this area,30 I will present a conceptual legal framework that groups the most salient findings gathered in these studies, clustering them into a number of general principles and overall rules that, together, complement the existing data protection principles. The objective is thus to present a conceptual framework of principles and guidelines able to orient and frame further specific legal provisions needed in the area of protection and management of eIDs. Formulating legal principles from the new dynamics brought by IDM systems can also help us in testing new solutions for present and upcoming legal problems. Dumortier rightly notes that “[t]he field of privacy and identity management will be an important laboratory where we can experiment how the law will function in our future global information society” (Dumortier 2003, 69).

The principles presented here are derived from the overarching principle of user-centricity. Under the umbrella of such guiding principle, we will then find a group of key principles and a group of procedural principles. The key principles reflect the application of the fundamental values of individual autonomy to the management of one’s electronic identity, allowing users to act through multiple identities,

29 The basic principles are listed in article 6 of the Data Protection Directive (DPD), and include the requirements that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical, or scientific use.

30 Apart from these basic principles, article 7 of the DPD delineates the conditions under which personal data may be processed, amidst which we stress the requisite that “the data subject has unambiguously given his consent”.

Such as the EU/EC programs, commissioned studies, action plans, agendas, and research projects promoted in the eID area and mentioned in sect. 2.
pseudonyms, or otherwise anonymously. The procedural principles operate at a more technical level, allowing users to keep their multiple identities separate (principle of unlinkability) and under their effective control (principles of negotiation, portability, and authentication source principle). These procedural principles, moreover, are derived from the principle of technological assistance, which underlines the important complementary role of technology in regulating eID (see Fig. 14.1).

In addition, it is important to note that the principles proposed here need to be complemented and implemented with concrete rules, schemes, policy initiatives, and technological infrastructures in order to implement a fully-operational eID legal framework.

### 14.6 Principle of User-centricity

In order to “create the knowledge society by empowering the individual,” (Reflection group on the Future of the EU 2030, 2010, 43) an eID legal framework should give the individual control over their own identity information. While respecting the interests of enterprises and society, the legal framework should place the individual at the core of the IDM system.

---

31 In terms of concrete proposals for the achievement of a pan-European eID scheme, Thomas Myhr presents two concrete action proposals that the European Commission could take into consideration in order to achieve cross-border interoperability: (i) setting up requirements for Validation Authorities and self-declaratory schemes and (ii) setting up a quality classification system, where different national security levels can be mapped against neutral requirements adopted by the European Commission. See Myhr (2008).
At the technological level, this principle has been implemented in ‘user-centric’ IDM systems. This particular IDM model, unlike the federated one, is composed of service providers and various identity providers. Identity providers, in this model, act as trusted third parties and are in charge of authenticating users, storing user accounts and profile information. Service providers, also called ‘relying parties’, perform their activities after receiving the authenticated identity claims about their users from the identity providers. This system not only allows users to choose identity providers independently of service providers, it also excludes them from providing personal information to service providers in order to receive their services (OECD 2009, 17). The user-centric system gives users greater control over their personal information by enabling them to select what information they want to disclose when transacting with service providers (although service providers may still require certain information for the transaction to take place) (OECD 2009, 17); and by enabling users to use various identity providers as well, so that their information is not stored at just one place (OECD 2009, 17). By endowing the data subject with an effective control over his/her own personal information, the principle of user-centricity reinforces the existing set of principles of data protection, i.e., specification, fair collection and accuracy, minimization, adequacy, and proportionality, contributing also to the effective enforcement of a ‘right to be forgotten’ (European Commission 2010e, 8).32

It is important to stress that the principle of user-centricity, which protects users’ interests in the control and management of their personal data, should be articulated with the interests of other relevant actors, namely governments and the private sector. Governments may also have a legitimate interest in accessing and sharing personal data. Be it for preventing terrorist actions, fighting cybercrime, or taxation purposes, the governments may be entitled to have access to users’ personal data (Rundle 2006).33 This is, in fact, one of the greatest challenges of building a coherent and operational eID legal framework: to conciliate the interests of individual citizens with those of the private sector and governments.

14.6.1 Principle of Multiple Identities

As Jones and Martin observed, “[t]he issue of what we consider to be the identity of a person has become increasingly complex as we have made ever greater use of

32 That is, “the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes”.

33 As examples of governments’ legitimate interest in accessing and sharing personal data, Mary Rundle lists the following: “For example, in fighting cybercrime, governments want authority to require Internet service providers to hand over subscriber information, among other data. To facilitate travel, governments have agreed to certain standards for a global system of electronic identity information. For taxation of international e-commerce, OECD members are seeking reliable ways to identify taxpayers. To counter the financing of terrorists or other criminals, governments seek to ensure that information on originators of wire transfer is available”.

the facilities and services that have been made available by developing technologies and the Internet. In the past, people normally had one identity, while in the current environment it is acceptable to maintain separate ‘identities’ for different aspects of our online interactions” (Jones and Martin 2010, 1).

Hence, any given person can have different partial identities which they use in different contexts. In the offline world, an individual person can be a citizen of a specific country, an employee or an employer of a given company, a mother and/or a daughter in her family context, etc. In this way, and

... as individuals take on many different roles in the course of their life, different set of characteristics, corresponding to these different roles, are used to represent their identity. Each of these ‘partial identities’ includes both inherited ‘timeless’ characteristics (such as nationality, gender, etc) and characteristics that they have acquired during their life (such as diplomas, competences, etc.), or that they have been assigned or issued to fulfil this role (such as a position, some sort of authority, etc.) (Nabeth 2009, 38).

In the online world, and in addition to the different partial identities of the “physical world”, an individual may have different accounts on various social networking sites (or within the same one), or he/she may hold different avatars in online games and virtual realities. An individual may also use pseudonyms for other kinds of interactions and present his/her civil identity for certain business transactions. In the digital world, a person may reveal and register selected information about his/her identity (disclosing certain attributes and not others) to a wide array of different institutions and service providers. These entities will then, based upon that information, assemble the (digital) identity of that person which can then vary quite considerably from one institution to another. In this manner, “[d]igital identities (and identifiers) can be constructed and issued by different organizations like the telephone company, the Internet provider, a social networking site, or an insurance company” (Leenes et al. 2009, 15).

Unlike the physical world and face-to-face interaction, where it is hard to avoid the disclosure of certain identity features (namely the physical and observable ones), in the digital world it is possible to reveal specific identity attributes while concealing others. It is even possible to create new attributes and features of ourselves, crafting and maintaining one or many new identities.

This new world of possibilities carries, nevertheless, problems and risks. The first problem is that citizens will tend to accumulate many “digital personae.” As it will be difficult to keep track of what each of these digital personae has done online, the privacy of that “multifaceted” person will become more difficult to protect. The second problem relates to the loss of control over information concerning those partial identities once they are released. As observed elsewhere, “[u]nlike goods, data cannot be reclaimed without the possibility that a copy is left behind in several possible places” (Leenes et al. 2008, 9).

In this way, the principle of multiple identities should ensure that IDM systems provide its users with the necessary tools to keep their multiple identities under con-
In this way, the principle of multiple identities also reinforces the principle of data minimization, as more user control over data disclosure (dispersed throughout its various digital personae) will lead to less disclosure of personal data.

The principle of multiple identities also aims to address the risks of using the same digital identity in the online world. As Poullet observes, “[i]t is clear that, most often, the same identification method or access key is used in different databases with as a result that our identity can be cross-referenced more easily” (Poullet 2010, 11). Taking into account that certain countries store the national registration number in all governmental databases, this “increases the possibility of cross-referencing the information and thus, enhances the power of the state (…) vis-à-vis the citizen (Poullet 2010, 11).” From this point of view, the principle of multiple identities contributes to the prevention of identity cross-referencing, thus equilibrating the balance of power between the state and the citizen. The principle of multiple identities has already been contemplated and developed at the technological level. The PRIME project, in providing privacy-enhancing identity management tools for individuals, conceived the PRIME Console as an instrument to manage users’ personal data. Among its various features, the PRIME Console—as the interface to the user’s IDM systems—would allow users to create partial identities (pseudonyms) and to associate personal data to these identities (Leenes et al. 2008, 5). Another example of a technical implementation of the principle of multiple identities (and of the principle of unlinkability, as we shall see next) can be found in the TURBINE project.35 This research program planned to enable an individual “to create different ‘pseudo-identities’ for different applications with the same fingerprint, whilst ensuring that these different identities (and hence the related personal data) cannot be linked to each other.”36

14.7 Principle of Anonymity and Pseudonymity

As a general principle, identity systems should facilitate anonymity and pseudonymity. They should also provide detailed rules regulating the use of anonymous and pseudonymous data. Thus, an IDM legal framework should explicitly regulate the cases in which people have the right to conceal their identity data (anonymization) or to present a different identity (pseudonymization), and the circumstances under which their identities can be unveiled. In this way, IDM systems should by default al-

---

34 The PRIME research project, in its technical proposals and prototypes for privacy-identity management tools, envisaged three central means of controlling multiple partial identities: tracking one’s data trail, support for rights enforcement and policy enforcement. See Ibid.
35 The TURBINE project aims to develop innovative digital identity solutions, combining the secure, automatic user identification thanks to electronic fingerprint authentication; and reliable protection of biometric data through advanced cryptography technology. For further information, see http://www.turbine-project.eu/
36 Ibid.
Towards a European eID Regulatory Framework

low for anonymous and pseudonymous interactions. This would be the case for most commercial transactions. Commercial service providers only need to know a limited number of specific attributes of a given client (such as age, address and payment information) to be able to successfully transact with them. For this kind of transaction, customers and citizens could interact through anonymous or pseudonymous identities. The principles of anonymity and pseudonymity, in this sense, are clearly related to the existing principle of data minimization. Exceptions to these principles would be established for certain and specific interactions with the public administration, in which it would be necessary to identify and/or authenticate the civil identity of a citizen (as a tax payer, a pension or benefits receiver). Apart from this exception, the principles of anonymity and pseudonymity applied to IDM systems acknowledge a known truth in today’s commercial transactions: it is not the identity of the user that matters but rather a specific attribute. Once again, technology is one step ahead of law, as the privacy and identity management tools conceived by the PRIME research project duly document:

... anonymous, or pseudonymous interactions are the default within PRIME ... PRIME supports different forms of pseudonymous with different characteristics with respect to linkability (Leenes et al. 2008, 8).

The principle of pseudonym, once applied and embedded in IDM systems, would entail—for instance—the creation of transaction pseudonyms for customers.37 However, it is important to bear in mind that the principles of anonymity and pseudonymity are not absolute and should have their limits explicitly defined. Therefore, the principle of anonymity and pseudonymity should not prevent strictly and legally contemplated possibilities and mechanisms of revealing users’ civil identities when the latter have breached their legal obligations or duties (Leenes et al. 2008, 11).38

The introduction of the principles of anonymity and pseudonymity should encompass both the regulation of the cases in which anonymous and pseudonymous identities are permitted, and the circumstances in which these identities can be revealed.

### 14.7.1 Principle of Unlinkability

In today’s world, online service providers—on the one hand—tend to exchange information regarding users’ habits, tastes, and preferences in order to address potential

---

37 As remarked in the PRIME project White paper: “If I know your name, I can try to get data about you through all sort of channels, which is much more difficult if I only know your transaction pseudonym ghT55897” (Ibid).

38 There are mechanisms to reveal the identity of users when warranted and under strict conditions. As a concrete proposal, it is suggested that “[o]ne of these conditions would be the use of a trusted third party that is contractually bound to reveal the civil identity of the user under certain circumstances.”
customers with tailored-made products, services and offers. Users, on the other hand, can have a legitimate interest in remaining unidentified to some service providers and identified to others. Users should have the freedom to make a choice. To help them do so, the principle of multiple identities and the principle of pseudonymity have been proposed. However, in order to effectively implement these principles, a further principle should be put forward: the principle of unlinkability. It is not enough to be able to create and maintain multiple identities and pseudonyms, it is also necessary to keep them apart from each other, that is, unlinkable.

Unlinkability is necessary in the context of ‘pseudonymization.’ The different pseudonyms used by an individual should be isolated from each other to prevent ‘full’ (or ‘exact’) identities to be linked to these partial ones and to prevent one partial identity (in the form of a pseudonym) to be associated and clustered with another partial identity. Thus, the principle of unlinkability prevents both de-pseudonymization and de-anonymization of data (Ohm 2009), that is, their re-identification.

The principle of unlinkability should thus secure the same degree of protection to different pseudonyms and to anonymized information. Otherwise, “[l]inking identities that do not share the same degree of anonymity, or that contain different sets of attributes may allow others to overcome pseudonyms and discover the user’s identity” (OECD 2009, 14).

The concern about the risk of possible linkage between different identity representations has already been addressed by technology designers. For example, the PRIME project conceived the creation of multiple private credentials from a single master certificate. These credentials, which could correspond to different pseudonyms belonging to the same person, would not be linkable to each other or to the master certificate from which they are derived. Another ‘technical’ implementation of the principle of unlinkability can be found in the Austrian sourcePin, which works as an ‘obfuscated identifier’ (Graux et al. 2009, 115). This number is never used to directly authenticate the user in eGovernment applications; it is used instead to generate sector-specific personal identification numbers (PINs). The unlinkability principle comes into play through the use of cryptographic one-way functions, according to which “sector-specific identifiers are calculated so that the citizen is uniquely identified in one sector, but identifiers in different sectors cannot be lawfully cross-related.”

Touching upon a number of proposals advanced here (and as a way to recapitulate the principles presented so far), Dumortier argues that:

Future solutions will have to give data subjects maximum possibilities to control and steer the use of their personal data. They should be flexible enough to offer possibilities for the data subject to reveal only the identification data that are necessary for particular circumstances.

39 De-anonymization of data is becoming a recurrent phenomenon, posing new risks to privacy.
40 In also observing the principle of unlinkability, the same study points out that the Czech republic plans to implement a similar system to the Austrian one, “based on the introduction of a ‘basic personal identifier’, which will be used to derive a set of personal identifiers for specific contexts, so that each individual will be identified by a different identifier in each context” (Ibid.), avoiding thus for different eIDs to be cross-related and linked.
Anonymous use of network services should be guaranteed where it is reasonably admissible. If unconditional anonymity—whereby the identity of the user is irreversibly lost—is not feasible, privacy-protecting schemes for conditional anonymity have to be established. Consequently the use of multiple ‘virtual identities’ will have to be regulated (Dumortier 2003, 69).

To sum up, the principle of unlinkability should orient IDM systems to considerably reduce the risk of cross-referencing between the different kinds of pseudonyms and multiple identities used by the same person.

### 14.7.2 Principle of Negotiation

The principle of negotiation aims to introduce a greater degree of flexibility in the current regulatory model of data protection. The implementation of this principle would allow users to negotiate the terms and conditions of disclosure of their identity information with service providers as a prior step to the already contemplated legal possibilities of accessing, correcting, and deleting personal data. This would also strengthen the requisite consent, which today is deprived of any real meaning and force. In fact, today, users have to comply with the demands of service providers if they want to gain access to their services. There is a clear imbalance between the bargaining positions of these two actors. The user has to provide the data asked for and has no choice but to accept the privacy conditions stipulated by the service provider. As a counterbalance to this currently pursued ‘take it or leave it’ approach, which undermines the idea of user consent, the principle of negotiation would endow users with more control over the processing of their own personal identity data. It derives from the principle of user-centricity and aims to reinforce and go beyond consent as a requirement for the lawful processing of personal data. The principle of negotiation thus serves to help the coming generation of IDM systems to empower users with tools that allow them to negotiate the conditions of the protection and management of their identities with service and identity providers. The PRIME project has already experimented with this idea. As stated in its White Paper:

PRIME replaces the ‘take it or leave it’ approach to privacy policies by a system of policy negotiation. Both parties can express different kinds of policies relating to authorizations, data handling, and preferences. The user is assisted by the PRIME Console which helps in setting personal preferences and requirements, in converting preferences from machine readable form to human readable form and vice versa, and in automatically negotiating the user’s preferences with the other party.

The principle of negotiation entails that users express their preferences and negotiate the terms of their identity data disclosure with service providers.

---

41 See (Leenes et al. 2008, 3).
42 Ibid., 7.
14.7.3 Principle of Portability

This is a principle that is not derived from a privacy ‘raison d’être’, but from a strict and specific identity rationale. Privacy, seen from a more classical and negative perspective as a right to opacity or to seclusion, deals mostly with the concealment of certain private aspects from public knowledge and the protection of disclosed information from the public sphere. Identity, on the other hand, deals with the transmission of information to the public sphere, namely with its correct expression and representation to the public eye. According to this view, an important principle related to the protection and management of one’s identity is the possibility of carrying one’s identity information with oneself, that is, the principle of portability. This principle underlines the fact that preventing someone from taking his/her constructed identity information to another place constitutes an unjustified hindrance to the protection and management of one’s identity.

The principle of portability is particularly relevant for reputations associated to eIDs, that is, for valuations and ratings of someone’s identity attributes or skills expressed within a given online community or network. The construction of reputations in the online world is a growing trend. It is increasingly common for citizens and users to acquire reputations in the form of financial credibility, work recommendations issued by colleagues or other skills rating made by peers. However, and despite the development of these reputation circles, it is difficult—in the online world—to transfer reputations from one context to another. The move from one social network to another usually implies the need to build one’s reputation from scratch. It is even more difficult to transfer one’s reputation without revealing one’s identity (be it the civil or a pseudonymous one). As noted in the PRIME project, “[t]ransferring reputations from one context to the next, without linkability of the underlying partial identities, is a feature that will prove valuable in online interactions.”

Technology, once again, anticipates law, as PRIME proposes a technical system to handle this kind of reputation transfer through the issue of anonymous credentials. Here we have an interesting combination of the principles of portability and anonymity.

In summary, the principle of portability argues that online identities (including their reputations) should be inherently portable and not irremediably anchored to any given service or identity provider. Taking into account that the current data protection model is overly privacy-oriented (Andrade 2011b), this principle is innovative. The existing data protection model “only” allows for the right to access, correct and delete private information because, from a privacy point of view (as a seclusion instrument of opacity), it does not make much sense to talk about the right to move private information from one place to another. However, and as mentioned before, a right to portability makes sense in terms of an identity rationale. From an identity management point of view, it is crucial to have the possibility to carry our identity information from one service provider (e.g., a social network) to another.

---

43 Ibid., 10.
14.7.4 The Authentication Source Principle

This principle derives from EU Member States’ national legislations (namely from National Registers Acts, eGovernment Acts, and other pieces of national and regional legislation). According to a study on eID interoperability, “this principle implies that for each given attribute (piece of identity data), one and only one source is considered to be authentic, i.e., correct” (Graux et al. 2009, 112). Other sources for that attribute are dispensable.

As observed in the mentioned study, this principle “is relevant from a cross border interoperability perspective, because a consistent application of the authentic source principle means that a single correct source exists for each bit of information, which can facilitate the access and exchange of this information (Graux et al. 2009, 81).”

This principle serves to help users manage and protect their digital identity, preventing them from having to provide the same information time and time again, ensuring that there is only one place in which information needs to be updated or corrected (Graux et al. 2009, 112). Thus, this principle reinforces the existing principle of data accuracy.

14.7.5 Principle of Technological Assistance

Law and legal solutions can only go so far. This is the case, for example, in the legal impossibility for the majority of EU Member States to allow (national) identity numbers to be used outside the Member State itself, along with the legal impossibility to establish a unique identifier to be used across every EU Member State. As the idea and project of a pan-European eID can only be implemented if citizens from one European country are able to use their eIDs to access services in a different EU country, Member States need to have some form of identifier when other EU national citizens make use of their services. This is the point where technical solutions must be devised and implemented. Given the legal impossibilities mentioned above, technology is the solution. In this way, and taking into account that one of the most problematic issues in cross-border IDM systems is the need for Member States to have some form of identifier when a foreign citizen makes use of their services, a “possibility to mediate this issue may be to use a one-way transformation function that unequivocally transforms a foreign ID number into one that may be locally stored” (Leenes et al. 2009, 32).

This example demonstrates that law can (and should) be complemented by technology so that they both form part of the regulatory framework. In other words, technology will fill the natural limits of law and assist the latter in enforcing its rules and dispositions.

---

44 For more information on which countries surveyed in the PEGS study subscribed to an authentication source principle and to what extent that this principle has impacted their identity management policies, see (Graux et al. 2009, 81–84).
Several steps have already been taken in this direction. Article 29 Data Protection Working Party (1999), in Recommendation 1/99, explicitly stated that software and hardware industry products should provide the necessary tools to comply with EU data protection rules. This statement is an important manifestation of the principle of technological assistance. Other important steps taken on the implementation of this principle can be found in the support and development of Privacy Enhancing Technologies (PETs) and the “Privacy by Design” approach, as well as in the increasing trend of imposing liability on terminal equipment manufacturers and information system designers by Data Protection Authorities.

The principle of technological assistance may, for example, lead to the imposition of technical standards on terminal equipment manufacturers in order to ensure compliance in terms of digital identities protection and management. It may also lead to the construction of new and fully fledged rights.45

14.8 Conclusion

In its “Europe 2020” Strategy, the Commission alerts us to the need to overcome “the fragmentation that currently blocks the flow of online content and access for consumers and companies” (European Commission 2010c, 19) within the envisaged digital single market. Often in the offline world today, business and citizens still need to deal with 27 different legal systems for the same transaction (European Commission 2010c, 18). As this article has attempted to demonstrate, there is no specific legal framework for eID. The protection and management of electronic identities is currently regulated by a patchwork of different pieces of EU and national legislation, along with implemented technological initiatives. Many solutions and innovations, both at the technical and legal levels, have been developed by Member States and introduced into their national regulations. As an example, and going beyond the applicability of their generic data protection regulations, a number of Member States have subjected some or all unique identifiers used in their administrations to additional protection mechanisms (Graux et al. 2009, 115).46

Nevertheless, the existing legal and technological solutions, current EU and national laws, along with the present technical arrangements seem insufficient to cover the limitations of the current and fragmented EU legal framework for the eID area.

This article, contributing to the discussion on the need for a shared eID legal framework for the EU, has suggested a number of new legal principles that take into account the new dynamics of and demands for the protection and management of electronic identities.

45 In this context, see Poullet’s construction of a “new privacy right: the right to a privacy compliant terminal with a transparent and mastered functioning by its users”, in (Poullet 2010, 27). Such right, as heavily based on technological components and technical requisites embedded into terminal equipments, constitutes what I would call a derivation of the principle of technological assistance.

46 Member States have also implicitly introduced in their legislation the already alluded authentic source principle.
The principles listed in this article constitute the backbone of an eID legal framework that puts users at the center and empowers them with the means, both legally and technically designed, to remain anonymous or to use pseudonyms, to manage multiple identities, to keep them separate and irretraceable, to negotiate the terms of their identity management preferences, to carry and freely move their identity information, among other possibilities. Furthermore, the listed principles would contribute to an even stronger protection of users’ privacy, strengthening trust, confidence and security in the online world of electronic communications and transactions.

More than technology, we need law. We need a shared encompassing legal framework, which guarantees that electronic identities can unobtrusively travel across different EU Member States, enabling access to services and transactions. The list of new principles described in this article aims to orient and contribute to this endeavor.

Acknowledgments Thanks to Ioannis Maghiros for very helpful comments.

Appendix: Terminology

This annex provides a general overview of the most relevant concepts, terms, and notions regarding electronic identity (eID) and electronic identity management systems (eIDM). It lays down the terminological grounds on which the legal analysis provided in the article is based.

The processing of electronic identities involves a wide array of technical terms that must be clarified in order to understand what the creation of a pan-European eID entails and implies. In fact, in order to discuss the creation of a European electronic identity and the legal challenges to such an endeavor, we need first to understand what electronic identity is. In order to comprehend the notion of electronic identity, we also need to understand other related and important concepts and processes, such as attributes, credentials, identification, authorization, and partial identities.

Starting with the basics, we should first distinguish between an entity and a quality. Any specific entity (a human being, for instance) has a number of qualities or attributes. The sum of these attributes make up one’s identity (namely one’s exact identity). The notion of “attribute” is of utmost importance because, depending on the context or on the attribute in question, it can refer to a “full identity” (when it is used to unequivocally identify a given individual) or to a “partial identity” (when it refers to an identity characteristic of a given person without revealing his/her full

---

47 This section relies upon various studies that have provided detailed “glossary-type” definitions of the various terms and notions employed in the area of eID. This is the case of the FIDIS project, the MODINIS, PrimeLife, STORK and specific studies, such as Pfitzmann and Hansen (2010).

48 In order to distinguish the concept of exact identity from the one of partial identity, I shall also use the term ‘full identity’.
or entire identity, (Pfitzmann and Hansen 2010, 31)\(^49\) that is, without identifying him/her in absolute terms.\(^50\)

Another important term is ‘identifier’. A unique identifier can be defined as “an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context” (Graux et al. 2009, 113).\(^51\) Two classes of identifiers can be distinguished which are primary digital identifiers, which are directly connected to a person (name, address, mobile phone number, password, or electronic signature) and secondary digital identifiers, which are not directly connected to an individual (cookies, IP addresses, or RFID tag numbers).

Also relevant is the notion of identity claims, which is intimately connected with credentials. In the offline world, claims that an individual is of certain age or lives at a given address are certified by third parties, namely by the State when it issues certificates supporting these claims (e.g., passport, ID card, or driver’s license). In the online world, there are entities specifically designated for the certification of identity claims. “[O]nline certifiers can, by means of cryptographic techniques (security tokens), vouch for certain claims in a secure manner that cannot be tampered with” (Leenes et al. 2008, 8). While paper-ID aims to identify physically present individuals, electronic ID provides credentials to enable citizens to remotely identify themselves. While conventional ID functions on the basis of personal appearance and paper-based proof of identity (certificates, identity cards, showing one’s signature or photograph), eID is based upon more complex processes and mechanisms.

Such processes of identity recognition are developed and carried out by identity management (IDM) systems. The overall objective of eIDM systems is to associate information with people, enabling transactions between different parties in an ecosystem of mutual confidence and trust. IDM, at a more general level, can be defined as “[s]ystems and processes that manage and control who has access to resources, and what each user is entitled to do with those resources, in compliance with the organization’s policies (Leenes et al. 2008, 1). On the administrators’ side, IDM systems allow organizations, businesses, companies, and institutions to grant, control, and manage user access to information, applications, and services over a wide range of network services. This access is conducted through authentication methods (passwords, digital certificates, hardware or software tokens) and authorization.

\(^{49}\) The distinction between full and partial identity I here propose presents a different *nuance* from the one advanced by Pfitzmann and Hansen regarding complete and partial identities: “A partial identity is a subset of attribute values of a complete identity, where a complete identity is the union of all attribute values of all identities of this person”, in (Pfitzmann and Hansen 2010, 31). While for these authors, partial identities may encompass attributes through which a person can be identified; I define partial identities as covering those attributes that do not necessarily identify a given person, classifying the ones that do as full identities. In sum, the difference between full and partial identities has to with identifiability, equating to the difference between information that relates to an identified or identifiable person, and information that does not.

\(^{50}\) As we have seen, this specific characteristic of the processing of eIDs enables the use of multiple identities by the same individual.

\(^{51}\) Though numbers (such as national register numbers, VAT numbers, certificate numbers, etc) are the most common (and, in fact, the default) form of unique identifier, “any sufficiently unique set of attributes pertaining to a specific entity can serve the exact same purpose” (Graux et al. 2009, 113).
rights. On the users’ side, IDM systems provide (or should provide) them with the necessary tools to manage their identities and control the use of their personal data. IDM systems can widely vary in terms of applications requiring different degrees of identification, access control, and credentials.

The functioning of IDM systems involves two main processes or components which are identification and authentication. While the purpose of identification is to “link a stream of data with a person,” (Myhr 2008, 77) the process of authentication can be defined as “the corroboration of the claimed identity of an entity or of a set of its observed attributes” (Graux et al. 2009, 113). In this respect, a distinction can be made between an authentication process that determines one’s exact identity and an authentication process that determines one’s specific quality or attribute (partial identity). In the latter situation, a given application authenticates the entity only to verify whether he or she has a specific required quality (such as being an adult, being a resident of a given region, city, etc). The process is thus carried out without revealing or knowing who exactly the person is. “The application determines the entity’s status, not his/her identity (Graux et al. 2009, 113).” In the other situation, the application authenticates one person by determining his/her exact identity. Here, authentication processes sufficient information to distinguish and select one individual from all others, one specific person out of all mankind.

In other words, the authentication process corresponds to the verification of the authenticity of an identity. Authentication must effectively prove that a person has indeed the identity that he/she claims to have. In this way, the authentication process requires elements/instruments such as identity cards, passports, or a key (proving to a technical infrastructure the right to access). In brief, authentication is the process of associating and permitting a specific identity or set of identity-related credentials to access specific services.

The authentication phase thus requires the presentation of a “credential”, i.e., “data that is used to authenticate the claimed digital identity or attributes of a person (OECD 2007, 12). Examples of digital credentials include an electronic signature, a password, a verified bank card number, a digital certificate, or a biometric template (OECD 2009, 6). Several actors can be identified in the authentication process of electronic identities. Within the eGovernment area, and as explained in one of the deliverables of the STORK project:

the eID process generally comprises five roles, which will be present in most Member States’ eID models. First of all, there is an (1) authority that registers the citizen that wants to obtain an eID. This authority is related to the (2) organization that provides an electronic token and the credentials (hence, the eID) that can be used in eGovernment authentication. In addition, the process of authentication comprises the role of (3) an authority that authenticates the token that is used by the citizen. Next to the authenticating party, there is (4) a relying party that depends on this electronic authentication for the purpose of interaction or transaction, e.g. in the eGovernment service. Of course, there is also (5) an entity that claims a particular identity (e.g., the citizen or a delegate) (Leenes et al. 2009, 25–26).

52 (Graux et al. 2009, 113) As we shall see, it is based on this type of authentication that I will argue in favor of a principle of multiple identities.
In a European context, the concept of **interoperability** is of paramount importance. Electronic identities will have little value for free movement of persons, goods, services and capital, and the stated objectives of constructing a fully operational single digital market, if they are not recognizable outside national borders and across different EU Member States. Interoperability is generally defined as “the ability of a system or a product to work with other systems or products without special effort on the part of the user, covering both the holder of the eID and the counterparty on the receiving end of electronic communication” (Myhr 2008, 77). It has both technical and legal/organizational dimensions.

A pan-European eID can be roughly defined as an “eID issued to persons, mainly natural persons but also legal persons (enterprises, etc.), which can be used in cross-border transactions, and is accepted by all states within the EU (Myhr 2008, 77).” A pan-European eID is closely connected to the notion of interoperability, which “mainly comprises the possibility of a citizen from one country to use the authentication system from this country to have access to an application in another country” (Leenes et al. 2009, 15).

To conclude, and in line with previously mentioned proposals for an eID terminology (Pfitzmann and Hansen 2010), the term eIdentity is used in this paper to indicate a set of personal information and data relevant to a human’s identity when stored and transmitted via electronic systems, including but not limited to computer networks (that is, digitized). Taking into account that, in the offline world, an identity is established from an extensive set of attributes associated with an individual (e.g., name, height, birth date, employer, home address, passport number), it is relevant to note that, in the online world, an individual identity can be established by combining both real world and digital attributes (OECD 2009, 6) (such as passwords or biometrics). Electronic identities are thus identities that are constructed out of the various identity-attributes related to a given person (which together compile his/her identity information), processed electronically by technically supported IDM systems, and that are then recognized by public and private entities (such as national governments and private companies) (Leenes et al. 2009, 16).

---

53 Typical use cases of an interoperable eID, which are currently being developed by Stork, “are when a citizen of country X can use the electronic identity and authentication scheme of his or her home country for a license application, or when a student from country Y can register for a scholarship in country X with her home authentication scheme, without a need to register herself in country Y” (Leenes et al. 2009, 16).

54 “Biometrics are measurable biological and behavioral characteristics and can be used for strong online authentication. A number of types of biometrics can be digitized and used for automated recognition. Subject to technical, legal, and other considerations, biometrics that might be suitable for IDM use include fingerprinting, facial recognition, voice recognition, finger and palm veins”, (OECD 2009, 7).

55 From a more technological perspective, the technical solution most commonly used in electronic communication identifying the person/holder of eID is PKI (public key infrastructure), which uses a pair of ‘keys’: a public key used for signing an electronic document and a private key linked to a certificate and used by the receiver to validate the signature. In this way, PKI can be used to detect
References


European Commission. 2010d. Towards interoperability for European public services.


if a document has been changed without authorization after it was sent. In addition, eIDs “may be stored on smart cards or other devices but may also be received from a central authority during an authentication process” (Leenes et al. 2009, 16).


Pfitzmann, Andreas, and Marit Hansen. 2010. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management (version V0.34).


