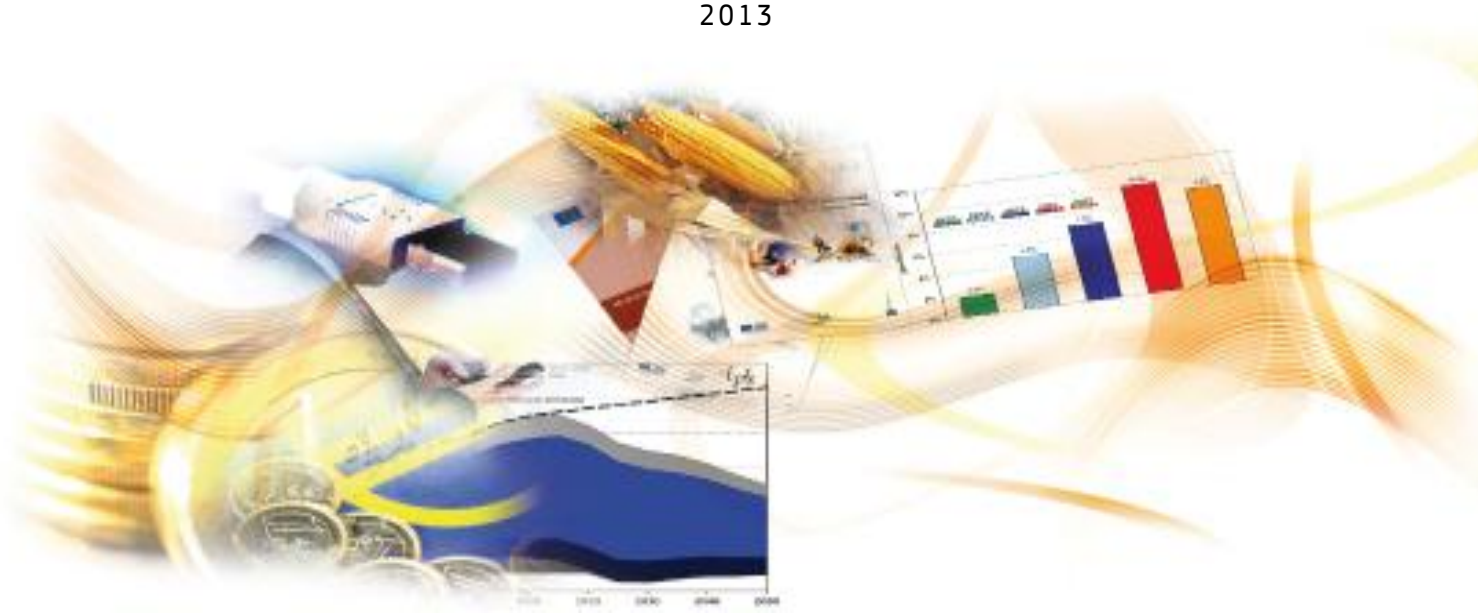
European Commission

JRC SCIENTIFIC AND POLICY REPORTS

Electronic Identity in Europe: Legal Challenges and Future Perspectives (e-ID 2020)

Norberto Nuno Gomes de Andrade, Shara Monteleone, Aaron Martin

2013



Report EUR 25834 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for Prospective Technological Studies

Contact information
Address: Edificio Expo. c/ Inca Garcilaso, 3. E-41092 Seville (Spain)
E-mail: jrc-ipts-secretariat@ec.europa.eu
Tel.: +34 954488318
Fax: +34 954488300

http://ipts.jrc.ec.europa.eu
http://www.jrc.ec.europa.eu

JRC78200

EUR 25834 EN

ISBN 978-92-79-28778-7 (pdf)

ISSN 1831-9424 (online)

doi:10.2791/78739

Luxembourg: Publications Office of the European Union, 2013

Printed in Spain

Table of Contents

This report contains content that:

- **has been published in the following book chapters:**

  Andrade, NNG 2012, "Towards a European eID regulatory framework. Challenges in constructing a legal framework for the protection and management of electronic identities", in "European Data Protection: In Good Health?", Serge Gutwirth, Paul De Hert, Ronald Leenes and Yves Poullet (Eds.), Springer (2012), pp. 285-314 (with kind permission from Springer Science+Business Media B.V.).
  The original publication is available at www.springerlink.com

  Andrade, NNG & Monteleone, S 2013 "Digital Natives and the Metamorphosis of European Society: The emerging behavioural trends regarding privacy and their legal implications", in "European Data Protection: Coming of Age", Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet (Eds.), Springer (2013), pp. 119-144 (with kind permission from Springer Science+Business Media B.V.).
  The original publication is available at www.springerlink.com

- **has been presented as a conference paper in the following conference:**

  Martin, AK & Andrade, NNG 2012, 'On the use of social networking services for government identity management purposes: A European policy analysis', 40th Research Conference on Communication, Information and Internet Policy, Arlington, VA, 21-23 September 2012.

- **corresponds to a prior version of a peer-reviewed article, later published in the following journal:**

  Andrade, NNG; Martin, AK & Monteleone, S; 2013, '"All the Better to See You with, My Dear": Facial Recognition and Privacy in Online Social Networks', IEEE Security & Privacy (May / June 2013), pp. 21-28.

Executive Summary

This deliverable presents the work developed by the IPTS eID Team in 2012 and 2013 on the wide topic of electronic identity. It has four parts: 1) eID: relevance, legal state-of-the-art and future perspectives; 2) Digital natives and the analysis of the emerging behavioural trends regarding privacy and identity and their legal implications; 3) The "prospective" use of social networking services for government eID in Europe; and 4) Facial recognition, privacy and identity in online social networks. In the following paragraphs, the main findings and arguments related to each of these parts are summarized.

Part 1 - eID: Relevance, Legal State-of-the-Art and Future Perspectives

The difficulties, barriers and challenges in implementing a regulatory framework for a pan-European electronic identity (eID)[1] have been analysed before in a number of studies. Deliverables pertaining to research projects funded by the EU, as well as study reports prepared for the European Commission in the areas of eID and eGovernment, 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 deliverable attempts to fill this gap, and also to contribute to research on both these analytical dimensions. Part 1 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 view of the intricate relationship between legal and technical aspects that this part establishes and addresses, the main challenge to European eID is considered to be not only technological, but also legal. It is important to note that the technology necessary to enable an interoperable eID across Europe already exists. 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. This part thus focuses 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 fully-fledged legal principles.

Section 1 of Part 1 describes the relevance of eID for the general development of the information society. It assesses the importance of electronic identity for administration (public), business (private) and, above all, citizens. It also highlights the role of eID as a key enabler of the economy.

Section 2 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. It examines 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 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 3 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

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

elaborated: the principles of user-centricity, anonymity and pseudonimity and the principle of multiple identities, identity portability, un-linkability and negotiation, among others.

In brief, this part identifies the legal gaps and proposes a number of principles that, ideally, could form the basis of a common EU legal framework for the protection and management of digital identities.

Part 2 – Digital Natives and the Analysis of the Emerging Behavioural Trends Regarding Privacy, Identity and Their Legal Implications

The new generation of young people, or *'digital natives'* (hereafter, DN), who have grown up immersed in information and communication technologies, reveal interesting attitudinal and behavioural patterns regarding the disclosure of personal information, profiling and protection of personal data. How do these emerging attitudes, expectations and behaviours shape society and how does the current set of normative rules and principles enshrined in the existing European legal framework of data protection influence them? The objective of this part is to analyse how observed behavioural trends of digital natives regarding the protection of personal data should be taken into account in future revisions of the legal regulatory framework. For this purpose, this second part of the deliverable looks at the better / smart regulation strategy of the European Commission (EC), and proposes the incorporation of data collection on the behaviour and the attitudes of DN into impact assessment (IA) procedures.

It considers the main different behavioural patterns of DN, detected by Eurobarometer 359, "Attitudes on Data Protection and Electronic Identity in the European Union" (published by the European Commission in June 2011), focusing on their attitudes to and perceptions of the disclosure of personal data via digital technologies. Moreover, it takes into account the results of specialized studies and projects that looked at the perceptions of privacy by DN, such as the PRACTIS project, the EU Kids Online project and other surveys conducted outside Europe.

Based on the results of the literature mentioned above, this part identifies not only a generational gap between adults and younger people, but also an important discrepancy between the legal dictates of the Data Protection Directive (according to which the processing of data is subject to rigorous legitimate criteria and principles) and the actual behaviour and privacy perceptions of the EU's youngest citizens. Taking into account the behaviours and attitudes of digital natives vis-à-vis the disclosure of personal data, this part argues that European Data Protection law is running the risk of becoming legally paternalistic, rigidly protecting citizens from the consequences of their own actions and losing touch with the reality of data subjects' expectations and behaviours.

The law should bear in mind that DN will have grown up in a couple of years and that they should, as such, not only be shaped by what the law says but also influence how the law is. Law-makers should thus learn to look at the future, to foresee and to anticipate the needs and the changing perceptions of those who are DN of today and the adult citizens of tomorrow. In effect, the current framework should strive not only to adapt itself but also to anticipate both the forthcoming technological landscape and technology's future users.

As a consequence, this part argues that future revisions of the legal framework should take into account the characteristics of the emerging digital natives, recommending the introduction of specific DN behavioural data collection into Impact Assessment procedures in the field of ICT law-making processes.

Part 3 – The "Prospective" Use of Social Networking Services for Government eID in Europe

The issue of identity policies for online environments continues to attract interest from academics, policy makers, and advocates. Today, the primary questions are not only whether and how to identify or authenticate users online, but also who (i.e., which entity) should be entitled to do so. In this context, this article addresses the ongoing tension between the traditional way of managing identities (that is, through unilateral actions endorsed by governments and public administration organizations) and recent trends in the provision and authentication of identities by private parties (or through cooperative private-public partnerships). Some European Union (EU) Member States have already opted for business models in which the private sector provides electronic identities (eIDs) that may also be used to access online public services, such as Sweden's BankID (which is e-government-enabled) and the proposed identity assurance model in the UK. The U.S. has its National Strategy for Trusted Identities in Cyberspace, which calls for the creation and facilitation of a "vibrant marketplace" for identity provision, with multiple accredited identity providers—both private and public—offering identity services.

In the context of private sector organizations emerging as identity providers, this part of the deliverable focuses on the possible role of social networking services (SNS) in government identity management (IdM). The widespread diffusion of SNS provides an opportunity to use these platforms for IdM purposes. Third-party sites have already started partnering with these services to simplify and streamline their registration processes. It appears that governments will be next to do so.

This deliverable thus explores the potential merits and drawbacks of these developments from a European policy perspective. This part discusses the following reasons why European governments may be interested in using pre-existing SNS for IdM: a) large installed base; b) critical mass of users; c) relatively mature infrastructure; d) high social acceptance of 'social' technologies; e) cost-effectiveness; f) real-name policies (which could render these identities more trustworthy and adequate for official uses); g) mutual recognition and cross-border (EU-wide) interoperability of eIDs; and h) the potential use of biometrics (particularly with the integration of facial recognition).

However, there are several drawbacks. The following are considered: a) citizen discomfort with using SNS credentials for official interactions; b) unreliable registration processes; c) reduced possibilities for anonymity and pseudonymity (and the attendant threats to freedom of speech and other political participatory values due to the emphasis on using real names); d) potential exclusionary effects for citizens unable or unwilling to use these eIDs; e) problems of neutrality (i.e., which platforms do governments endorse?); f) problems of data ownership; g) security concerns; h) the potential for SNS to track users on government sites; i) jurisdictional issues (i.e., most popular platforms are US-based); j) task complexity; and k) liability issues (assuming that one's SNS-endorsed eID is recognized and used for e-government services across different Member States, which party is liable for misuse, theft or impersonation?).

The final part of the deliverable describes the most recent EU policy and legal initiatives in the field of electronic identities and the proposed schemes for their identification and authentication. At the EU level, it focuses on the legislative measures currently being proposed in Europe to facilitate the Identification, Authentication and Signatures (IAS) policy, namely within the scope of the ongoing Electronic Signatures Directive revision process and the launch of the draft Electronic Trust Services Regulation. At the national level, it analyses the recent UK proposal for an Identity Assurance scheme. The possibility and feasibility of adopting SNS for government IdM purposes will then be analysed in light of these two proposed models.

The deliverable draws attention to the need to keep efforts to achieve mutual recognition and interoperability of eIDs open to evolution, technological progress, and new business models. The paradigm of state monopolies over the provision of identities is outdated. Alternatives to this model should be sought in the private sector.

Part 4 – Facial Recognition, Privacy and Identity in Online Social Networks

Online social networks (OSNs) are increasingly introducing biometric technologies such as facial recognition in their services. Facebook, for example, has incorporated a facial recognition system to facilitate the tagging on photos uploaded by users. Mobile phone-based OSNs, such as SceneTap, offer facial detection technologies to determine the average age and gender ratio of people at bars, in order to help bar-hoppers find the 'right' place to drink.

While biometrics have been traditionally employed in security contexts (e.g., for law enforcement purposes, authentication systems for access control, etc.), the introduction of this technique into social networking contexts is quite recent. However, the use of biometrics within OSNs is not uncontroversial. These technological developments have raised public concerns about automated identification and unwanted tracking. So much so that policy makers in the United States (i.e., the Federal Trade Commission) and European Union (i.e., the Article 29 Data Protection Working Party and Irish Data Protection Commissioner) have begun to monitor these developments and to offer their opinions on the use of biometrics within OSNs.

With these developments in mind, this deliverable analyses the social and legal implications of the use of these technologies in OSNs and explores ways of governing the privacy implications associated with their use. Among the important privacy and security issues, this part of the deliverable explores the following:

- How facial recognition technologies introduce novel problems for 'non-registered' members of OSNs by providing an increasingly reliable technological means of identifying and tracking people who have chosen not to participate as users of the network, but who are nevertheless subject to these identification technologies. For example, when an OSN member uploads multiple photos of a friend who does not have a profile on the site, the facial recognition system will nonetheless generate a biometric profile for this person;
- How, through the social graph (which describes the relationships between individuals of a network), OSNs reduce the severity of false matches (traditionally a major problem for biometrics) by prioritizing candidates who happen to be in close proximity to the person who has uploaded a photo. In other words, information from the social graph can help to limit the scope of the search and thus reduce the opportunity for false matches. A related issue involves the unintentional honing of the facial recognition algorithms being developed by OSNs, by users through popular 'tagging' features;
- How different contexts (public and private) for the use of biometrics are becoming increasingly blurred (e.g., the combination and integration of data collected through OSNs and detection technologies for security purposes), and how this mix impacts on the regulation of these technologies;
- How law enforcement authorities (and other third parties) access these images ought to be regulated, including the possibility that the police could cooperate with companies to process mug shots against an OSN's database of facial photos. Similarly, certain police forces are developing mobile phone applications to crowd-source the analysis of facial images of suspects. In this respect, compliance issues emerge, namely how to honour the principles of consent and purpose specification found in the European Data Protection regime.

In particular, this analysis notes how the use of automated facial recognition techniques on OSNs complicates the important data protection principle of consent (i.e., that the processing of photos for biometric purposes should be based on the free, informed and active consent of the users concerned and that biometric templates created without proper consent must be deleted). One challenge is how OSNs can ensure, both legally and technically, that biometric profiles of non-registered people are not created and/or maintained.

Finally, the deliverable reflects on the adequacy, efficacy, and limits of the current legal instruments to cope with these privacy risks. It also discusses how the forthcoming EU Data Protection Regulation impacts on the use of biometrics in OSNs, providing recommendations applicable to facial recognition technologies used in these networks.

Part I - eID: Relevance, Legal State-of-the-Art and Future Perspectives

1.1 Introduction and structure

The difficulties, barriers and challenges in implementing a regulatory framework for a pan-European electronic identity (eID)[2] have been analysed before in a number of studies. Deliverables pertaining to research projects funded by the EU, as well as study reports prepared for the European Commission in the areas of eID and eGovernment,[3] 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. Part 1 attempts to fill this gap, and also to contribute to research on both these analytical dimensions. This part of the deliverable 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. To sum up, this part 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.

This part of the deliverable is structured as follows. Section 1 describes the relevance of eID for the general development of the information society. It assesses the importance of electronic identity for administration (public), business (private) and, above all, citizens. It also highlights the role of eID as a key enabler of the economy.

Section 2 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. It examines 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 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 3 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 pseudonimity and the principle of multiple identities, identity portability, un-linkability and negotiation, among others.

Before moving on, one important remark regarding the focus and scope of the first part of this deliverable must be made. This Part is devoted to the legal aspects of eID.[4] Hence, it looks at the

---

[2] See Annex 1 for the definition of the most relevant concepts and terms regarding electronic identity (eID) and electronic identity management systems (IDM).

[3] 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 programme, as well as studies such as the European Commission's "Signposts towards eGovernment 2010," (2005), 6., prepared by the eGovernment subgroup of the eEurope Advisory Group.

[4] It is also important to bear in mind that the scope of this deliverable is limited to the management of the digital identities of individuals or natural persons. We are 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 document.

main barriers[5] 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.[6] 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 derive, in actual fact, from technological design principles, having already been tested in numerous research projects and technical prototypes. We 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 deliverable will establish and address, we consider that the main challenge to European eID is not only technological, but also legal. It is important to note that the technology[7] necessary to enable an interoperable eID across Europe already exists.[8] 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, this section will focus on the legal framework that must be constructed in order to accompany and enforce the existing technological answers,[9] transposing some of the latter into operating fully-fledged legal principles. In brief, the scope of the section 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.

---

5 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 deliverable. 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 Norberto Nuno Gomes de Andrade, "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights," in Privacy and Identity Management for Life: 6th Ifip Wg 9.2, 9.6/11.7, 11.4, 11.6/Primelife International Summer School, Helsingborg, Sweden, August 2-6, 2010, Revised Selected Papers, ed. S. Fischer-Hübner, et al. (Berlin ; Heidelberg: Springer, 2011). 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 Thomas Myhr, "Legal and Organizational Challenges and Solutions for Achieving a Pan-European Electronic Id Solution or I Am 621216-1318, but I Am Also 161262-43774. Do You Know Who I Am?" Information Security Technical report 13, no. 2 (2008).

6 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, we believe that technology should also contribute to an "identity by design." European Commission, "First Report on the Implementation of the Data Protection Directive (95/46/Ec)," (Brussels2003).

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

8 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", Modinis-IDM-Consortium, "Modinis Study on Identity Management in Egovernment, Identity Management Issue Interim Report Ii1," (2006), 7. One may therefore conclude that the most difficult obstacles posed to the creation of a pan-European eID are not technical, but the ones deriving from the different legal approaches and socio-political sensitivities of EU Member States.

9 In other words, this section does not focus directly on interoperable technical mechanisms and infrastructures enabling EU citizens to identify and authenticate themselves. This section, 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.

1.2 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.

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[10] 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."[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.”[12] 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 freedoms of establishment and circulation of goods, capital and services.[13] eID is also

---

[10] Many EU Member States have in the recent times deployed large scale eID projects (such as Germany, see Graux, Majava, and Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 120.), much of which are presently underway.

[11] European Commission, "A Digital Agenda for Europe," (2010), 11. 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).

[12] Myhr, "Legal and Organizational Challenges and Solutions for Achieving a Pan-European Electronic Id Solution: Or I Am 621216-1318, but I Am Also 161262-43774. Do You Know Who I Am?," 77.

[13] Leenes et al., "Stork - Towards Pan-European Recognition of Electronic Ids (Eids) - D2.2 - Report on Legal Interoperability," 22.Stork D.2.2 Report on Legal Interoperability, p.22

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.[14]

Consequently, the relevance of eID and the need for interoperable eIDs has been recognized in EU agendas and strategies,[15] action plans,[16] declarations,[17] communications,[18] studies,[19] and programmes.[20]

The EU has also financed and supported a vast number of research and practical implementation projects focusing on electronic identity and interoperability (see table below).

In addition to these, there are many other international networks and research centres in Europe carrying out important projects in this area, such as the PETWEB II[21] and the Porvoo Group.[22] 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 systems across Europe.

STORK	https://www.eid-stork.eu/
CROBIES	http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm
PRIME	https://www.prime-project.eu/
PrimeLife	http://www.primelife.eu/
Modinis IDM	https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome
TURBINE	http://www.turbine-project.eu/
BEST	http://www.best-nw.eu/
PICOS	http://www.picos-project.eu/
ABC4Trust	https://abc4trust.eu/
SEMIRAMIS	http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=250453
FIDIS	http://www.fidis.net/

Table 1: List of research and practical implementation projects devoted to eID and interoperability

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-

14 Ibid.

15 European Commission, "Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth," (Brussels2010).

16 ———, "Delivering an Area of Freedom, Security and Justice for Europe's Citizens: Action Plan Implementing the Stockholm Programme," (Brussels 2010). In such Action Plan, the Commission has proposed a European Strategy on identity management to be attained by 2012, which includes legislative proposals on criminalisation of identity theft and on electronic identity (eID) and secure authentication systems.

17 Such as the Manchester Ministerial Declaration (2005) and the Lisbon Ministerial Declaration (2007).

18 Such as the recent Communication from the European Commission, "Towards Interoperability for European Public Services," (2010).

19 Namely the following studies: European Commission, "Signposts Towards Egovernment 2010"; European Commission, "A Roadmap for a Pan-European Eidm Framework by 2010 - V.1.0," (2007).

20 Such as the Stockholm Programme, 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.

21 http://petweb2.projects.nislab.no/index.php/Main_Page

22 http://www.vaestorekisterikeskus.fi/vrk/fineid/home.nsf/pages/6F4EF70B48806C41C225708B004A2BE5

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.[23]

Nevertheless, despite the various political declarations and initiatives in this area, the plethora of research projects, the proliferation of identity management 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 the next section.

1.3 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, we 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 this section is mainly focused on legal barriers, we shall start with a fundamental technical barrier: 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.[24] 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."[25]

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 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.

---

[23] 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 […]."

[24] In effect, "[t]he Internet has a ID infrastructure often identifying only the endpoint of a communication: IP addresses. These are often unreliable to identify users." Leenes, Schallaböck, and Hansen, "Prime (Privacy and Identity Management for Europe) White Paper," 1.

[25] Ibid.

1.3.1. 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 identity management 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,[26]/[27] 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, drivers licences) 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 multi-purposes and contexts has been considered unconstitutional in a number of countries (such as Germany, Hungary and Portugal, among others).[28]

Due to divergent legal regulation and organization in EU Member States, there is a proliferation of different identity management systems,[29] 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 the 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."[30] 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.[31]

---

[26] Graux, Majava, and Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 106.

[27] Leenes et al., "Stork - Towards Pan-European Recognition of Electronic Ids (Eids) - D2.2 - Report on Legal Interoperability," 25.

[28] 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.

[29] Four main models of identity management systems can be identified within the massive proliferation of eID systems: the "siloed", the centralized, the federated and the "user-centric" identity management systems. For a detailed explanation of each of them, see OECD, "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers," 16-17.

[30] OECD, "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers," 17.

[31] Ibid.

We are thus confronted with an increasingly complex scenario, encompassing a wide set of actors: identity holders, identity providers, registration authorities and authenticating authorities.[32] Hence, in a typical eID management system, identity-related data is not simply sent or provided by a subject to a controller: 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.[33]

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 certificate 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 certificate authorities, based in different countries and following different eID schemes. And the same challenge applies to certificate 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."[34] 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 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 concerns 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).[35] 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."[36]

As noted by specific eID research programmes, these new generations of identity management systems "do not provide adequate safeguards for personal data and give individuals limited control over their personal data."[37]

The increase in different identity management 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.

---

[32] 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.

[33] Graux, Majava, and Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 119. PEGS, 119.

[34] Myhr, "Legal and Organizational Challenges and Solutions for Achieving a Pan-European Electronic Id Solution: Or I Am 621216-1318, but I Am Also 161262-43774. Do You Know Who I Am?," 81.

[35] Leenes et al., "Stork - Towards Pan-European Recognition of Electronic Ids (Eids) - D2.2 - Report on Legal Interoperability," 32.

[36] Ibid.

[37] Leenes, Schallaböck, and Hansen, "Prime (Privacy and Identity Management for Europe) White Paper."

1.3.2. EU legal competences[38]

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 analyse 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,[39] and reference must normally be made in the recitals to the concrete enabling power, generally to be found in the Treaty itself.[40]

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.[41] 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

---

[38] For a detailed analysis of Lisbon Treaty's competences and legal basis for eID, see N. Andrade – "Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID." Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 28, No. 2 (2012), pp. 152 – 163

[39] The basic principle underpinning legal basis was expressed in Case 45/86, Commission v. Council (Generalised 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."

[40] In the case of delegated legislation, those references are located in an enabling legislative act.

[41] In more detail, such three categories are the following ones:

- Exclusive competence, according to which only the European Union can legislate and adopt legally binding acts, the Member States being able to do so only if empowered by the European Union or for the implementation of EU acts;
- Shared competence, which constitutes a 'general residual category,' (Paul Craig, "The Treaty of Lisbon, Process, Architecture and Substance," European Law Review 33, no. 2 (2008): 8.),Craig, "The Treaty of Lisbon, Process, Architecture and Substance." as it provides that the European Union 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 competence according to which the European Union is restricted to taking action to support, co-ordinate or supplement the action of the Member States.
- Competence to support, co-ordinate or supplement. This category of competence allows the European Union 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 harmonisation of Member State law (article 2 (5) TFEU).

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 77 (3) TFEU.[42] 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, Art 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.

1.3.3. 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 concerns the disclosure of more information than is actually needed for the purposes 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 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.[43] 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

---

[42] 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."

[43] OECD, "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers," 18.

systems there is, instead, the risk of concentration in the market for identity providers, which would then undermine users' control over their own information.

1.3.4. 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.[44]

A legal taxonomy for eID[45] 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.[46] 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."[47]

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.[48] 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 main reason for this is that, even if the legal framework does not 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."[49]

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 that assumes its regulatory functions accompanied by technology, and not replaced by it. It is exactly in this context,

---

[44] This is the case of the Modinis-IDM-Consortium, "Modinis Study on Identity Management in Egovernment, Identity Management Issue Interim Report Ii1." Modinis Deliverable: D.3.9 Identity Management Issue Interim Report II1. In addition, the Modinis project developed a specific Terminology Paper, ———, "Modinis Study on Identity Management in Egovernment. Common Terminological Framework for Interoperable Electronic Identity Management - Consultation Paper V.2.01," (2005).

[45] See annex 1 for an overview of the terminology use in the field of eID.

[46] Graux, Majava, and Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 118. PEGS, p.118

[47] Ibid.

[48] Ibid., 128.

[49] Ibid., 119.

in order to re-articulate the relationship between law and technology, that we propose the principle of technological assistance.

1.3.5. Legal barriers and challenges: conclusions

As a preliminary 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."[50] 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 and overview of what is to be regulated and how.

1.4 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",[51] 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."[52]

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.[53]

---

[50] Myhr, "Legal and Organizational Challenges and Solutions for Achieving a Pan-European Electronic Id Solution: Or I Am 621216-1318, but I Am Also 161262-43774. Do You Know Who I Am?," 77.

[51] Dirk van Rooy and Jacques Bus, "Trust and Privacy in the Future Internet – a Research Perspective," *IDIS - Identity in the Information Society* 3, no. 2 (2010): 403.

[52] Ibid.

[53] 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

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,[54] we 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 identity management 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."[55]

The principles here presented all derive 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, 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, derive from the principle of technological assistance, which underlines the important complementary role of technology in regulating eID (see figure below).

---

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 is 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.
A part 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".

54 Such as the EU/EC programmes, commissioned studies, action plans, agendas and research projects promoted in the eID area and mentioned in Section 2.

55 Jos Dumortier, "Legal Considerations with Regard to Privacy Protection and Identity Management in the Information Society," *112e rapport annuel, Hochschüle für Technik und Architektur Biel, Tilt*, no. 15 (2003): 69.

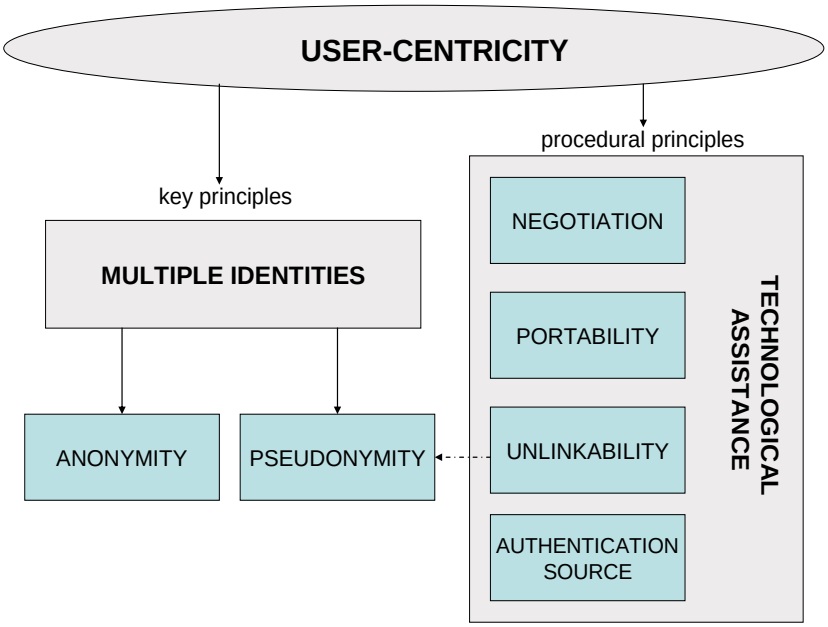


Figure 1: eID Legal Framework Principles

In addition, it is important to note that the principles here proposed need to be complemented and implemented with concrete rules,[56] schemes, policy initiatives and technological infra-structures in order to implement a fully-operational eID legal framework.

1.4.1 Principle of user-centricity

In order to "create the knowledge society by empowering the individual,"[57] an eID legal framework should give control of identity information to the corresponding individual. While respecting the interests of enterprises and society, the legal framework should place the individual at the core of the IDM system.

At the technological level, this principle has been implemented "user-centric" identity management 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.[58] 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);[59] and by enabling users to use various

[56] In terms of concrete proposals for the achievement of a pan-European electronic ID 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 classificatory system, where different national security levels can be mapped against neutral requirements adopted by the European Commission. See Myhr, "Legal and Organizational Challenges and Solutions for Achieving a Pan-European Electronic Id Solution: Or I Am 621216-1318, but I Am Also 161262-43774. Do You Know Who I Am?."

[57] Reflection group on the Future of the EU 2030, "Project Europe 2030. Challenges and Opportunities - a Report to the European Council by the Reflection Group on the Future of the Eu 2030," (2010), 43.

[58] OECD, "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers," 17.

[59] Ibid.

identity providers as well, so that their information is not stored in only one place.[60] 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".[61]

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. One should bear in mind that governments may also have a legitimate interest in accessing and sharing personal data. Be it for preventing terrorist actions, fighting cybercrime or taxation purposes, governments may be entitled to have access to users' personal data.[62] 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.

1.4.2 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 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."[63]

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.)."[64]

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

---

60 Ibid.

61 That is, "the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes", European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union," in *European Commission* (Brussels2010), 8.

62 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" Mary Rundle, "International Personal Data Protection and Digital Identity Management Tools " *Berkman Center Research Publication No. 2006-06* (2006).

63 Andy Jones and T. Martin, "Digital Forensics and the Issues of Identity " *Information Security Technical Report* (2010): 1.

64 Thierry Nabeth, "Identity of Identity," in *The Future of Identity in the Information Society : Challenges and Opportunities*, ed. Kai Rannenberg, Denis Royer, and André Deuker (Berlin ; London: Springer, 2009), 38.

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."[65]

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 certain 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."[66]

In this way, the principle of multiple identities should ensure that identity management systems provide its users with the necessary tools to keep their multiple identities under control, even after data is disclosed.[67] 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."[68] Taking into account that certain countries store the national registration numbers 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."[69] 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 identity management system – would allow users to create partial identities (pseudonyms) and to associate personal data to these identities.[70] Another example of a technical implementation of the principle of multiple identities (and of the principle of

---

65 Leenes et al., "Stork - Towards Pan-European Recognition of Electronic Ids (Eids) - D2.2 - Report on Legal Interoperability," 15.

66 Leenes, Schallaböck, and Hansen, "Prime (Privacy and Identity Management for Europe) White Paper," 9.

67 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.

68 Yves Poullet, "About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?," in *Data Protection in a Profiled World*, ed. S. Gutwirth, Y. Poullet, and P. de Hert (Dordrecht: Springer Science+Business Media B.V, 2010), 11.

69 Ibid.

70 Leenes, Schallaböck, and Hansen, "Prime (Privacy and Identity Management for Europe) White Paper," 5.

unlinkability, as we shall see next) can be found in the TURBINE project.[71] This research programme 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."[72]

1.4.3 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 allow 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 identity management 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."[73]

The principle of pseudonymity, once applied and embedded in IDM systems, would entail – for instance – the creation of transaction pseudonyms for customers.[74]

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.[75]

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.

---

[71] The TURBINE project aims to develop innovative digital identity solutions, combining: 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/

[72] http://www.turbine-project.eu/

[73] Leenes, Schallaböck, and Hansen, "Prime (Privacy and Identity Management for Europe) White Paper," 8.

[74] 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.

[75] 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." ———, "Prime (Privacy and Identity Management for Europe) White Paper," 11.

1.4.4 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 customers with tailored-made products, services and offers. Users, on the other hand, can have a legitimate interest in remaining un-identified to some service providers and identified to others. Users should have the freedom to make the 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.

The principle of unlinkability is an important complement to the principles of multiple identities and of anonymity and pseudonymity. Regarding the former, the aim of the principle of unlinkability is to prevent linkages between users' different digital identities, leaving the user in control. This principle is particularly suited for the upcoming trend of "pseudonymization." It serves to keep the various pseudonyms isolated from one another, so that "full" (or "exact") identities are not linked to these partial ones, and that one partial identity (in the form of a pseudonym) is not associated and clustered with another partial identity. Thus, the principle of unlinkability prevents both *de-pseudonymization* and *de-anonymization* of data,[76] that is, their re-identification.

The principle of unlinkability should thus secure the same degree of protection to different pseudonyms and to anonymised 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."[77]

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 derived. Another "technical" implementation of the principle of unlinkability can be found in the case of the Austrian sourcePin, which works as an "obfuscated identifier."[78] 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."[79]

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.

---

[76] *De-anonymization* of data is becoming a recurrent phenomenon, posing new risks to privacy. In this respect, see Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization " *University of Colorado Law Legal Studies Research Paper No. 09-12* (2009).

[77] OECD, "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers," 14.

[78] Graux, Majava, and Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 115.

[79] 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.

Touching upon a number of proposals here advanced (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. 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".[80]

1.4.5 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 previous 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.[81] 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 identity management 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 authorisations, 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."[82]

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

1.4.6 Principle of portability

This is a principle that does not derive 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 point of 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

---

80 Dumortier, "Legal Considerations with Regard to Privacy Protection and Identity Management in the Information Society," 69.

81 Leenes, Schallaböck, and Hansen, "Prime (Privacy and Identity Management for Europe) White Paper," 3.

82 Ibid., 7.

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 eID reputations, 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 and phenomenon. It is increasingly common for citizens and users to build 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."[83] 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.

To sum up, 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, this principle is innovative.[84] 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.

1.4.7 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."[85] In other words, this principle ensures that one and only one authentic source should be correlated with a specific identity attribute, rendering all other sources for that attribute 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."[86]

---

[83] Ibid., 10.

[84] In this sense, see Norberto Nuno Gomes de Andrade, "The Right to Privacy and the Right to Identity in the Age of Ubiquitous Computing: Friends or Foes? A Proposal Towards a Legal Articulation," in *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, ed. C. Akrivopoulou and A. Psygkas (Hershey, PA: Information Science Publishing, 2011). Andrade, "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights."

[85] Graux, Majava, and Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 112.

[86] Ibid., 81. 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 ———, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 81-84.

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.[87] Thus, this principle reinforces the existing principle of data accuracy.

1.4.8 Principle of technological assistance

Law and legal solutions can only go so far. This is the case, for example, of 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 makes 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."[88]

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.

Several steps have already been taken in this direction. Art. 29 Data Protection Working Party, in Recommendation 1/99,[89] 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 systems 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.[90]

---

87 Graux, Majava, and Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 112.

88 Leenes et al., "Stork - Towards Pan-European Recognition of Electronic Ids (Eids) - D2.2 - Report on Legal Interoperability," 32.

89 Article 29 Data Protection Working Party, "Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware," (1999).

90 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, "About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?," 27. Such right, as heavily based on technological components and technical requisites embedded into terminal equipment, constitutes what I would call a derivation of the principle of technological assistance.

Part 2 -Digital Natives and the Analysis of the Emerging Behavioural Trends regarding Privacy, Identity and their Legal Implications

2.1. Introduction

The objective of Part 2 is to analyse how observed behavioural trends of digital natives[91] regarding the protection of personal data should be taken into account in future revisions of the legal regulatory framework. For this purpose, Part 2 looks at the Better / Smart Regulation strategy of the European Commission (EC), proposing the incorporation of data collection on the behaviour and the attitudes of DN into the Impact Assessment (IA) procedures.

The research on digital natives is based on Eurobarometer 359, "Attitudes on Data Protection and Electronic Identity in the European Union" (published by the European Commission in June 2011),[92] which constitutes the largest survey ever conducted on citizens' behaviours and attitudes concerning identity management, data protection and privacy (the survey was conducted in 27 EU Member States via a national, random-stratified sample of ~1,000 interviews; overall, 26,574 Europeans aged 15 and over were interviewed face-to-face in their homes, between 25/11 and 17/12 of 2010). We considered the main different behavioural patterns of DN, detected through the related 2011 survey, focusing on their attitudes and perceptions in the disclosure of personal data via digital technologies. We based our claims also on a further analysis of the survey results developed by Joint Research Centre-IPTS of the European Commission,[93] illustrating views, emerging attitudes and expectations of European citizens concerning their personal data. Moreover, we took into account the results of specialized studies and projects that looked upon the perceptions of privacy by DN, such as the PRACTIS project,[94] the EU Kids Online project[95] and other surveys conducted outside Europe.[96]

Based on the results of the literature mentioned above, this part identifies not only a generational gap between adults and younger people,[97] but also an important discrepancy between the legal dictates of the Data Protection Directive (according to which the processing of data is subject to rigorous legitimate criteria and principles) and the actual behaviour and privacy perceptions of the EU's youngest citizens. This second part explores, among other topics, how one's experience of an invasion of privacy today may be different from the way it will be experienced in the future.

---

91 The authors acknowledge that, while the term 'digital natives' is widely used, its definitions vary; sometimes referring to teenagers, sometimes to adolescents and sometimes to all people under 35. For the purpose of this paper, we take into account the age categories used in the special Eurobarometer 359 "Attitudes on Data Protection and Electronic Identity in the European Union", in which DN are identified in the young people aged 15-24. For a wide research study conducted in Europe on the Internet use among children and youngsters (aged 9-16) see the EU Kids Online project.

92 This EB updates and integrates the Eurobarometer *Data Protection in the European Union: citizens' perceptions*, Analytical Report, February 2008, http://ec.europa.eu/public_opinion/flash/fl_225_sum_en.pdf.

93 Wainer Lusoli, et al. *Pan-European Survey of practices, attitudes & policy preferences as regard personal identity data management*. EC JRC Institute for Prospective Technological Studies EUR- Scientific and Technical Research series, Luxemburg: Luxemburg Publications Office (forthcoming-2012).

94 http://www.practis.org/. Though the purpose of the PRACTIS project is to assess "the potential impacts of emerging and future technologies on privacy and privacy perceptions", and "how the developments of new technologies may induce shifts in perceptions about privacy", we deem that some of its main findings are valid to the aim of our paper, in particular those related to the possible generational gap between adults and younger people.

95 http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx.

96 Hoofnagle et al., *How different are Young adults from older adults when it comes to information privacy attitudes and policies* Survey, April 14, 2010, http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf.

97 *Ibid*.

Departing from such observations, the part develops a series of underappreciated challenges between the legal and the social reality, the actual behaviour and privacy perception of the EU's youngest citizens. We advance the thesis that the current data protection legal framework may need to be stretched to adapt to future societal developments.

Taking into account the behaviours and attitudes of digital natives vis-à-vis the disclosure of personal data, this part argues that European Data Protection law is running the risk of falling into a legally paternalistic temptation, rigidly protecting citizens from the consequences of their actions and losing touch with the reality of data subjects' expectations and behaviours. As a consequence, this part argues that future revisions of the legal framework should take into account the image of the emerging digital natives, recommending the introduction of specific DN behavioural data collection into IA procedures in the field of ICT law making processes.

With this aim in mind, we developed our claims structuring the sections of this part as follows. Section 2.2 defines digital natives, providing a review of the essential literature on the topic. Section 2.3 is devoted to discuss the emerging attitudes of younger people with regard the protection of their personal data and privacy as confirmed by data collected through recent studies. It reflects on new "perceptions" of privacy and considers, consequently, the legal implications of these emerging practices. Section 2.4 analyses the adequacy of the current DP legal framework in order to cope with new challenges and needs of young generation. It elaborates specifically on three data protection paradigms that are increasingly being questioned by DN behavioural patterns: the principle of data minimization; the hierarchical mind set and the vertical architecture of the current DP model; and the requirement for systematic opt-in consent. Section 2.5 proposes a solution for the identified legal and social discrepancy by looking at the EU Better / Smart Regulation policy. In this ambit, the section recommends the integration of collected data from DN into IA procedures, highlighting the importance of incorporating DN in the EU law making process.

2.2. "Defining" digital natives

The concept of *digital natives* was first used in specialized literature on educational research by Marc Prensky,[98] who contrasted the new generation of students, born and grown up in a world of information and communication technologies (ICTs) in the late 1980s and 1990s, to that of "digital immigrants" (hereafter, DI), who were born before the digital age and thus have had to adapt to new technologies. As native speakers of the digital language of computers and the Internet, DN - according to Prensky - would think and process information fundamentally differently.

The literature about DN is quite conspicuous, and initiatives that aim to 'understand' young people as they grow up in the digital age have proliferated around the word.[99] For this part we reviewed selected studies that examine the nature, behavioural trends and technologies used by DN. These studies (which are not necessarily focused on privacy issues, but often related to the topic) discuss whether DN, through their exposure to new technologies, have developed radically new cognitive capacities and learned skills besides being tech-savvy. The debates pivot on questions such as: do DN really think differently and learn differently? Is one born digital or does one become a DN? What is the role of technology in defining social movements?[100] In some of this literature, the idea that this generation is tech-savvy is also debated and contested.[101]

---

[98] This definition is taken from Marc Prensky "Digital Natives, Digital Immigrants", in *On The Horizon. 6 MCB University Press* (2001).

[99] Further to the studies already mentioned, another focused research study on DN is the one developed by John Palfrey and Urs Grasser, *Born Digital*, New York: Basic Books, 2008. It is the result of an ongoing interdisciplinary project of the University of Harvard and University of St Gallen, available at: http://www.borndigitalbook.com/.

[100] See, *inter alia*, Nishant Shah and Fieke Jansen. *Digital AlterNatives With a Cause? Book One, To Be.* The Center for Internet and Society (CIS), 2011, http://www.scribd.com/nilofarh/d/65628308-Book-1-To-Be-Digital-Alternatives-With-a-Cause; See, moreover, David Buckingham. *Youth, Identity and Digital Media*,

Though there is not a consensus on the nature and features of DN,[102] there is a general acknowledgement of quantitative differences in the use of technologies between DN and DI, as well as in their attitudes towards technologies.[103] These differences, moreover, may imply changing needs, risks and opportunities for the new generation.

Aware of the existence of these current debates, our aim is not to add more knowledge to this literature base, nor to discuss the very nature of this discontinuity between generations. Rather, taking into account these discussions, we want to further stimulate debate on the legal issues at play.

2.3. New generations, new technologies and new privacy perceptions

Since topics such as privacy online are not immediate concerns for most of the DN, at least when they are not directly asked about them,[104] the simplistic inference from this statement would be that younger people are simply uninterested in these topics and that they do not care, as reported in most of the recent literature reflecting the digital natives discourse.[105] Thus, our question is the following: is it correct to simply say that DN do not care about the risks they run with regard to their privacy?

From the results of the EB 359 survey, some meaningful figures emerge on the attitudes of European citizens regarding personal identity data, concerning, for instance the general use of Social Networking Sites (SNS) like *Facebook, Linkedin, Flickr, Youtube,* etc. According to the survey, more than a third of EU27 citizens (34%) access SNS, and more than half of those (57%) also use websites to share pictures, videos, music, etc. As the main use of SNS is to enable online socialising, it necessarily means disclosing social (personal) information online. One meaningful outcome is that SNS users (both DN and DI) seem less cautious than the non-SNS users about sharing information on the social networks, although they generally consider it personal.[106]

A relevant concept in relation to personal data disclosure is that of control, namely the amount of control SNS users think they have on data they disclose. One practical tool in relation to control is the ability to change one's privacy setting on a SNS profile from default. Overall, 56% of SNS users surveyed affirmed that they have tried to change privacy settings of SNS personal profile from default options and 43% have not tried. Thus, if SNS providers have not set appropriately high

---

Cambridge: MIT Press, 2008; Rebecca Eynon and L. E. Malmberg (2011), A typology of young people's Internet use: Implications for education, 56 *Computers & Education*(2011): 585; Catrina Denvir, et al. "Surfing the web- Recreation or resource? Exploring how young people in the UK use the Internet as an advice portal for problems with a legal dimension", *Interacting with Computers* 23 (2011): 96-104; Yair Amichai-Hamburger, Gideon Vinitzky "Social network use and personality", 26 *Computers in Human Behavior*, 26 (2011) 1289.

[101] Sue Bennett et al. "The 'digital natives' debate: a critical review of the evidence" *British Journal of Educational Technology*, 39 (2008): 775. The difference between DN and older generation of users would be in the appropriation of technologies, not in their ability to use it. Moreover, some scholars sustain that young people with Internet literacy tend to cope with more risks, but the level of exposure to online risks remains high also for those with lower Internet literacy: self-confidence, in fact, would go with more exposure to online risks. See also Sofie Vandoninck et al. "Digital Literacy among Flemish adolescents: How do they handle online content risks?" *Communications* 35 (2010): 397.

[102] For an overview on the different concepts regarding Digital Natives see: Michael Thomas, *Deconstructing Digital Natives, Young people and new literacy*, Routledge 2001.

[103] Anoush Margaryan et al. "Are digital natives a myth or reality?" *Computers & Education* 56 (2011) 429.

[104] See the study of Hoofnagle et al., mentioned above.

[105] For an overview on the common discourse on DN in media, literature and education, built on the assumption that "youth do not care about privacy" see: Alice Marwick et al. "Youth, Privacy and Reputation", *Berkman Center Research Publication*, Harvard: Harvard University (2010).

[106] See EB 359, 45.

safeguards to protect people's personal data by default, just less that half of European SNS users may have left their personal data unprotected in these environments.[107]

The survey also contains significant data concerning DN: in particular, data on their behaviour regarding personal data and on the technologies they use in their daily activities that allow us to envisage the future trends in their personal data practice. These cannot be disregarded by policy makers. The survey, in fact, revealed a relevant generation split, as DN (the younger Europeans, still mostly studying, aged 15-24), are those who use the Internet more (94%, EU 66%), join SNS more (84%, EU 52%)[108] and use websites to share pictures, videos, movies more (73%, EU 44%).[109] In all Member States they use the Internet very little outside SNS, while older people who use SNS are practically the same as the percentage of Internet users. In addition, this is not the only discrepancy that emerges between DN and DI which contributes to strengthen our claim that policy and regulation of today will need overhauling in the next 10-20 years. For instance, DN perceive data disclosure as unavoidable (41%, EU 28%) and disclose more social information (48%, EU 28%). They also believe in strong uniform protection of their data and value their digital profile as much as older people; moreover, they feel more in control and perceive less risk in using the Internet.

Generational differences are confirmed also by the PRACTIS project's results that emphasize the contrast between the attention devoted by younger people to privacy concerns, when asked explicitly, and their behaviour.[110] From this contrast interesting considerations can be drawn: firstly, "adolescents perceive social network sites as part of their private sphere, where they exchange private information with their peers; secondly, they handle private data in a differentiated way trying to explicitly manage who gets which information. For the decision regarding which information is given to whom, the context seems to matter. Finally, they are ready to trade off privacy for benefits, like discounts or increased convenience".[111] Therefore, younger people do look for creating private spaces and do seek to manage who gets their information and in which context. Meanwhile, when they share information about themselves, increasing their exposure, they do so because they gain something: "when they are negotiating privacy [...] they are considering what they might gain from revealing themselves": this gain is not necessarily an economic gain (discount, free products or services), but could often be a reputational gain.[112]

---

[107] Lusoli et al. "Pan-European Survey", 71. Interesting figures emerging from the EB 359 are also those related to control perception and responsibility perception of EU citizens using SNS: people thinking that disclosure is unavoidable are more likely to think they are responsible for protecting their own data, rather than companies. People who are happy to disclose think it is authorities who are responsible, rather than companies. However, there is no relation between self-responsibility and identity protection behaviour. Even people feeling responsible do little to protect their personal data once they have been disclosed. This may be due to the lack of tools allowing people to take care, effectively if at all. But when tools are available, such as privacy notices, people do read them if they feel responsible. See Lusoli et al. "Pan-European Survey", 43.

[108] *Ibid.*, 39: "General pattern emerges from the socio-demographic analysis of the types of personal information disclosed on social networking or sharing sites. The younger the social or sharing site users are, the more likely they are to disclose their names (85%), their photos (65%), their nationality (54%), the things they do (50%), who their friends are (51%) etc".

[109] See EB 359, 4.

[110] See PRACTIS Deliverable D3.4 final, Report on changing perceptions of privacy and the changing role of the State, http://www.practis.org/UserFiles/File/D3%204_final_report_20110725.pdf. Though, the PRACTIS Report considers this behaviour "privacy-treating behaviour" pointing to the lower awareness of younger people for privacy.

[111] *Ibid.*

[112] danah boyd, Alice Marwick, Social Privacy in Network Publics: teens' Attitudes, Practices and Strategies, paper presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 22, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128, 10-13.

Nonetheless, peculiar behavioural patterns, emerge concerning young people. On the one hand, they appear more relaxed (in terms of personal data disclosure); on the other, they are more knowledgeable and alert. This aspect could seem paradoxical at a first glance, but it is not. This attitude could be understood as a product of the different perceptions and different needs of the new generation. Differences in privacy perception do not necessarily mean disregarding one's own personal data or ignoring the related risks connected with the data processing.

As DN are the citizens of tomorrow, it seems relevant to investigate what is (and will be) their perceptions of privacy. It is likely that the existing generational gap will expand and that in the future what it is perceived today as a privacy concern will not be the same for the DN, who are already coming of age.

2.3.1. Is it true that young people do not care about privacy?

Even scholars, like Ralph Gross and Alessandro Acquisti,[113] who have quantified individuals' willingness to provide large amounts of personal information in an online SNS (when they published, only a small number of members would have changed the default privacy preferences) and have inferred that the users are unconcerned about privacy risks, recognized the existence of different drivers influencing users' information revelation behaviour ("many simultaneous factors are likely to play a role"), the importance of which is still to be defined.[114]

According to the EB 359, DN feel sufficiently informed about the use of their data when joining a social networking, adapting their behaviour accordingly: they are likely to change their privacy settings and they are also likely to feel that they have control over the information disclosed on social networking In addition, they are more likely to appreciate the possibility of moving their data from one service provider to another.[115] As a general trend, today's young people use online spheres for peer socialization, relationship-building, information-sharing and mainly to talk with people they already know.[116] Young people, in the majority of cases, do want to put personal information online[117], but this behaviour does not have to be automatically interpreted as a disregard for privacy: the data shown in the EB seem to suggest that this occurs not necessarily because they do not understand or do not care about risks,[118] but more likely because their perception of what is (and will be) private changes. As Marwick stressed:

> "Many of the studies of privacy online focus on risk, rather than understanding the necessity of private spaces for young people where they can socialize away from the watching eyes of parents, teachers or marketers. These seeming contradictions demonstrate how understanding of risks, public space, information and the role of the Internet in day-to-day life differ between teenagers, parents [...] and scholars."[119]

---

[113] Ralph Gross and Alessandro Acquisti, "Information Revelation and Privacy in Online Social Network (The Facebook case)", *Proceedings of the ACM Workshop on Privacy in the Electronic Society (WPES)*, New York, 2005.

[114] In subsequent research findings, the same authors (Alessandro Acquisti and Ralph Ross "Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook", in *PET 2006*, ed. G. Danezis and P. Golle, Cambridge, LNCS 4258 (2006): 36) seemingly mitigated their assertions, acknowledging that members of communities do exhibit privacy concerns, though they are not deterred by them from joining the community.

[115] See EB 359, 160-167.

[116] Marwick et al. 4.

[117] As Marwick et al. highlight, the policy and technical solutions proposed until now are based on this assumption and presume that young people would not disclose their personal information if they understood the risks, consequently they focus predominantly on making DN aware of the consequences of disclosing information.

[118] James Grimmelman (2010), Privacy as Product Safety, 26 *Widener Law Journal*, 793, talks about these assumptions as "myths of privacy".

[119] Marwick et al. 4. In a recent lawsuit in U.S., a Minnesota middle school student claims a violation of her privacy rights by her school district, perpetrated through a search over her Facebook and emails account,

DN want private spheres and these are the spaces they have chosen for socialization, for free expression, for fun. These spaces are typically SNS or communities.[120] As Marwick et al. stress, young people, more than the adults, instead of viewing the public and private as two strictly separate realms, have a more flexible understanding of information disclosure and control. Consequently, "they want to be able to restrict personal data posted online in a *nuanced and granular way*" (emphasis added), "as posting personal information online is a way for youth to express themselves, connect with peers, increase popularity[...]".[121] They show an interest in controlling access to their personal information, for instance, selecting the set of information and the set of people to share this information with or finding particular practices to protect their privacy.

In boyd and Marwick' view, while the idea that teenagers do not care about privacy is a widespread myth, "the participation in such networked publics does not imply that today's teens have rejected privacy as value".[122] These authors sustain that young people do have a sense of privacy, though their definitions of privacy vary widely. Accordingly, young people's practices in SNS would be shaped by their interpretation of the social situation and by their ability to navigate the *technological* and *social* environment, so that they would develop peculiar strategies to approach privacy aims. The technological architecture of SNS, which augments the blurring between what is private and what is public, would affect young people practices: "As social constructs, privacy and publicity are affected by what is structurally feasible and socially appropriate. In recent history, privacy was given as granted, because structural conditions made it easier to not share than to share. Social media have changed the equation".[123] Finally, these scholars offer a vision of privacy as a social norm that is achieved through a wide harry of social practices configured by structured conditions. In this light, young people seem to have started developing innovative strategies for achieving privacy: segmenting friends' groups depending on the service used (e.g., some teens use Facebook and Twitter to talk to different "communities"); or deleting constantly their comments or those of their friends after have read them; or even deactivating and reactivating on a daily base their Facebook account.[124]

As a consequence of the aforementioned "nuanced and granular way" of young people in using personal data on line and restricting the access to them, Heather West notices: "Rather than all-or-

---

confirming these different perceptions of privacy, as reported by CNN U.S. "Minnesota girl alleges school privacy invasion, March 10, 2012, http://articles.cnn.com/2012-03-10/us/us_minnesota-student-privacy_1_school-counselor-school-house-gate-facebook?_s=PM:US

120 Maria Karyda, Spyros Kokolakis Privacy Perceptions among Members of online Communities, in *Digital Privacy, Theries, Technologies and Practices*, ed. A. Acquisti, S. Gritzalis et al., New York: Auerbach Pub. (2008) distinguish different types of privacy, which are considered important by community members: physical, interactional, psychological and informational privacy. Moreover they wonder how the concept of privacy protection may be affected by the fact that people online often have multiple (virtual) identities or profiles.

121 Marwick et al. 5.

122 danah boyd, Alice Marwick, Social Privacy in Network Publics: teens' Attitudes, Practices and Strategies, paper presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 22, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.

123 *Ibid*., 10.

124 danah boyd, Alice Marwick, Social Privacy in Network Publics, 18-20. See also Mimi Ito et al. Living and Learning with New Media: Summary of Findings from the Digital Youth Project. *The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning*, 52 (2008), http://www.itofisher.com/mito/weblog/2008/11/living_and_learning_with_new_m.html; and Emily Christofides, Amy Muise and Serge Desmarais, Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *CyberPsychology & Behavior*, 12(3), 341–345 2009.

nothing public or private paradigm, we expect to be able to choose levels of privacy and levels of exposure to the public".[125]

Subsequently, policy and lawmakers should not further postpone taking into account young people's privacy practices, or as boyd and Marwick describe it: "how teens approach privacy challenges and the ways in which privacy is currently conceptualized, discussed, regulated".[126]

2.3.2. Changing privacy practices and legal implications

One can assert that DN, though they are more inclined to disclose personal information, will still become privacy-sensitive adults in the future, because the contexts and the quality of their perceptions will be different as well as the practices and strategies used to protect their privacy.

This seems to be confirmed also by the findings of the PRACTIS study, from which emerges the conclusion that "adolescents' sensitivity for privacy seems to change towards a more flexible concept of privacy rather than diminish due to future technologies".[127]

A 2010 survey[128] on young American adults' attitudes (aged 18-24), reported by the Berkeley Center for Law & Technology, demonstrated that the picture is more nuanced than portrayed in the popular discourse on DN (*e.g.,* they are less concerned about privacy). In that survey, Hoofnagle et al. note that the statements of American young adults reflected a sensitivity towards privacy and policy options, as well as a knowledge of information privacy law, that only apparently contrasts with their behaviour on SNS and elsewhere online.[129] The data of such survey, mutatis mutandis, do not differ drastically from those emerging from the EB 359 or from the PRACTIS study. The latter, though, emphasizes the direct impact that new business models, new online practices (*e.g.,* selling personal data to third parties) exert on privacy threats and also on new privacy perceptions. We share, however, the PRACTIS's view that the main threats to privacy induced by Internet companies are related to the lack of transparency towards users.[130] We also share the policy implications of these findings, at least with regard to the claim for the role of Governments in regulating privacy by design for businesses, for instance "imposing minimal standards on services and products, or implementing other process-oriented privacy assessment for technologies".

That said, we argue that if the DN are too optimistic about the efficacy of the law to protect them, the solution, however, cannot be in more rigidity of the regulatory regime, *i.e.* in prohibiting/limiting what they consider normal to do with the new technologies. If work should be done in terms of adequate educational programmes (a topic that is beyond the scope of this deliverable), the same should be said from the legal point of view, as a different legal formula is also required. Higher degrees of flexibility (where needed) should go together with firm but renovated legal rules that finally take into account the changes that occurred in the (online) society.

---

[125] Heather West, Is Online Privacy a Generational Issue? *GeekDad, Wired.com*, 2009, http://www.wired.com/geekdad/2009/10/is-online-privacy-a-generational-issue/.

[126] *Ibid*.

[127] PRACTIS Deliverable D3.4 final, Report on changing perceptions of privacy and the changing role of the State, 7, http://www.practis.org/UserFiles/File/D3%204_final_report_20110725.pdf.

[128] Hoofnagle et al., *How different are Young adults from older adults when it comes to information privacy attitudes and policies* Survey, April 14, 2010, http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf.

[129] The Berkeley's report, though, shows data on a lack of knowledge of DN on the effective protection ensured by the law to their privacy, concluding that the young adults do have an aspiration for increased privacy, but the business environment and other factors encourage them to disclose data in order to enjoy social inclusion: the suggestion from Hoofnagle et al. is, thus, to search for forms of assistance in the educational and regulatory field.

[130] PRACTIS Deliverable D3.4 final, 6.

Our considerations on DNs' changing perception of privacy are also in line with the Nissenbaum's view of information privacy in terms of "contextual integrity" and its corollaries: 1) the personal information is always tagged with the context in which it is revealed, that is, all sectors of life are governed by context-specific norms of information flow; 2) depending on the nature of information, in some contexts it is "appropriate" and expected to reveal and share certain information while in others it is not (Nissenbaum talks about norms of appropriateness that guide the behaviour of people in the different contexts); 3) daily people move into and out of different contexts (from family to business to leisure); the movement or transfer of information from one party to other(s) requires different levels of "distribution" of information, that correspond to different norms of information sharing (she talks about norms of distribution).[131]

Our claims do not seem to contrast either with some developments of Nissenbaum's view in the context of social networking. For instance, Gordon Hull et al.[132] sustain that "contextual gaps" are endemic to Facebook and other SNS, that these gaps are at the root of the many privacy issues, but also that these issues are mainly design issues, ameliorable by an interface design that could increase transparency and control of information flow. The development of new technologies, especially for SNS applications, tends to change the expected distribution norms of the perceived context (e.g. Facebook), therefore, in order to allow the users to keep the control over the distribution of their information, SNS should make more transparent the flows of information on the site. In other words, as the perception of DN on Facebook would be influenced by the design of the site, these gaps could be addressed through a "good" programme design.

Moreover, as pointed out by boyd and Marwick, teenagers do not share a uniform set of values about privacy and publicity: in particular, variations in teens' practices seem, in boyd and Marwick view, to be "shaped by the social norms that surround them[...]Sharing is viewed differently in different friend groups, schools, communities".[133]

Supporting the insight of Marwick et al., about the DNs' need - which not necessarily correspond to that of their parents - to restrict personal data posted online in a *nuanced and granular* way (i.e., using SNS in a multifaceted way and highly differentiating set of data/set of people, according to the social contexts created online), we suggest that, the focus of DN privacy discourse regarding SNS and similar contexts should be on filling in the existing "contextual gaps" and that an adequate legal framework should seek to assure a more context-based privacy protection, possibly with the support of technology, such as better programme design for community sites.

Departing from the results of the survey and the analysis of the related literature and research conducted in this area, we shall argue in the following sections that there is not only a significant discrepancy between digital natives and non-digital natives, but also between the behaviours, practices and perceptions of DN regarding privacy and personal identity management and the data protection legal framework. In other words, we claim that there are a number of discrepancies between the legal dictates of the Data Protection Directive (DPD) and the actual behaviour and privacy perception of the EU's young citizens, i.e. a growing mismatch between the social reality of DN and the legal reality of data protection. In effect, the existing legal framework does not seem to take into full account the emerging (and shifting) attitudes, expectations and behavioural trends of DN, reflecting instead a somewhat outdated vision of reality. Hence, the current regulatory scheme does not seem to be in pace with the reality of DN, i.e., with their new ways of communicating,

---

131 Helen Nissenbaum, "Privacy as contextual integrity", *Washington Law Review*, 79 (2004): 101.

132 Gordon Hull, et al., Contextual Gaps: Privacy issues on Facebook, *Ethics and Information Technology*, 4, (2011): 289, http://ssrn.com/abstract=1427546.

133 danah boyd, Alice Marwick, Social Privacy in Network Publics: teens' Attitudes, Practices and Strategies, paper presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 22, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.

sharing information, forming relationships, understanding privacy and perceiving their own identities.

Taking into account the behaviour and attitudes of DN vis-à-vis the disclosure of personal data, we argue that European data protection law is running the risk of falling into a legal paternalistic temptation, rigidly protecting citizens from the consequences of their actions and losing touch with the reality of data subjects' expectations and behaviour.

It is in this context that we pose the question of whether and to what extent future legal revisions (namely the ones in the area of data protection) should take into account the new generation of users and their different attitudes and perceptions regarding the processing of their own personal data and the use of their electronic identities. In other words, the main question is to what extent the use of new technologies by DN and the behavioural trends that emerge from their utilization should be taken into account by the lawmakers in future legal revision processes.

2.4. Current legal framework

The current international legal framework for privacy and data protection is based upon a set of instruments that date from the 80s and 90s, such as the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the "OECD Guidelines"), the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"),[134] and the European Union Data Protection Directive 95/46/EC ("DPD"). The DPD - the main European legal instrument on the protection of individuals with regard to the processing of personal data and on the free movement of such data - entered into force more than 17 years ago. At that time, technologies such as biometrics, social networking, cloud computing, web 2.0 or the Internet itself, were either non-existent or only making their first steps, still far from today's massive adoption and pervasive use. As Tene argues, the current legislative framework has not been able to keep up with these technological environment and remains based on concepts developed practically over 30 years ago.

> "[T]he current Framework is in danger of being unravelled by a new generation of users utilizing a new generation of technologies. The fundamental concepts underlying the Current Framework, including basic terms such as 'personal data', 'data controller', 'data processor', and 'data transfer', have been disrupted by shifting technological realities".[135]

In this way, the current framework does not only refer to a completely different technological landscape from the one we have today, it still addresses the data subject of the 90s and their lifestyles, privacy conceptions and needs. The new data subjects are, today, individuals who openly disclose and exchange large amounts of personal, often intimate, information online. DN are also, for example, the ones that transfer more information using peer-to-peer (P2P) file sharing applications.[136] They are individuals used to having their location tracked, their profiles displayed, their photos posted, and their tastes and preferences revealed. Their daily lives are increasingly

---

[134] The OECD Guidelines and the Convention 108 were, in effect, put in place before the advent of the World Wide Web as a public network.

[135] Omer Tene, Privacy: The New Generations. *International Data Privacy Law* 1 (2011).

[136] In a recent empirical study that characterizes and quantifies the amount of content of various types that is transferred worldwide using BitTorrent, it was found that content that is popular among teenagers is more likely to be disproportionately represented in BitTorrent as compared to content that appeals to an older audience. See, MATEUS, A. M. & PEHA, J. M. 2011. Quantifying Global Transfers of Copyrighted Content Using BitTorrent *39th Telecommunications Policy Research Conference (TPRC) 2011* George Mason University School of Law, Arlington, VA.. This study has also concluded that BitTorrent Transfers result in hundreds of millions of copyright violations worldwide per day, and that copyright holders fail to realize significant revenues as a result. The analysis of this result in light of DN behavior practices lead us to discuss the adequacy and the (social) acceptance of current copyright laws (and the need to devise new alternative models to the existing one). Nevertheless, this discussion goes beyond the scope of this paper.

entrenched and dependent upon the information they constantly produce, seek and receive in the online and offline spheres.

Contrarily to what the existing data protection rules seem to imply, there are important benefits to withdraw from maximizing the disclosure and sharing of information. As Swire contends, and "[a]s illustrated by our eagerness to use social networks, access to the personal data of others is often a benefit to individuals, rather than the threat assumed by the data protection approach. These benefits notably include our right to associate, to reach out to people to effect political change and realize ourselves as individuals".[137]

Nevertheless, the current DPD still presents the same structure, the same set of basic principles and rules, and the same mind set of 1995 – when the "Internet" was still in an embryonic phase. The current data protection legal framework is thus based upon a set of unquestioned premises and paradigms that are, notwithstanding, being slowly disrupted by shifting technological developments and user's practices and perceptions.[138] In the following we take a closer look at three of these paradigms.

2.4.1. Minimization of information

The effective protection of personal data relies upon the robust application of principles such as purpose limitation and the minimization of personal data collection, as required by the EU Data Protection Directive. One of the key principles of the current data protection legal framework is thus the principle of data minimization.

This principle derives from Article 6.1 (b) and (c) of DPD, which states that personal data must be "collected for specified, explicit and legitimate purposes" and must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and / or further processed". According to this principle, a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. Moreover, data controllers should also retain the data only for as so long as is necessary to fulfil that purpose. Briefly, the data minimization principle requires data controllers to collect only the personal data they really need and to keep it only for as long as they need it.[139]

While the legal "rhetoric" of the current framework emphasizes the construction of an information ecosystem where individuals and organizations interact with one another on the supposed basis of minimized disclosure of personal information, the technological reality is completely different, not to say the exact opposite. In fact, we are living and participating in "an online reality that is optimized to increase the revelation of personal data".[140] The ongoing increases in processing power allow more information to be extracted about individuals, using data mining algorithms to discern and record patterns of behaviour,[141] and generating more and more information. In addition, and along the lines of the pervading Web 2.0 business model, users are encouraged to maximize their

---

[137] SWIRE, P. 2012 Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection *North Carolina Law Review, 2012; Ohio State Public Law Working Paper 165; 2011 TPRC Conference.*

[138] The inefficiencies and shortcomings of the current data protection model, such as the ones developed in this section, have led legal scholars and computer scientists to put forward alternative models, presenting different proposals of how to attain a more effective enforcement of one's privacy and data protection rights. This is the case of the proposal for introducing property rights in personal data (see Purtova, Nadezhda. *Property Rights in Personal Data. A European Perspective*, (Kluwer Law International 2012.) or the proposal of a data protection approach based on the assertion of different categories of privacy harms (see CALO, M. R. 2011. The Boundaries of Privacy Harm. *Indiana Law Journal,* 86.

[139] http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74

[140] Hoofnagle et al. "How Different are Young Adults from Older Adults", 20.

[141] Ian Brown, Data Protection: The New Technical and Political Environment. *Computers & Law* 20 (2010).

personal data by producing digital content, sharing information, forming relationships and establishing networks,[142] which are then used and exploited by commercial companies and other entities. The internal logic of Web 2.0 is thus structured, on the one hand, on users who are converted into *superprocessors* of information and, on the other hand, on business companies that seek to record every user action, store the resulting data and mine it for profit.[143]

Rather than data minimization, one should emphasize the value and of benefits of data maximization (the increased production and access to personal data), as well as the need for data empowerment.[144] Contrarily to data protection, which relies on limits to sharing of information, data empowerment relies precisely on information sharing, allowing ordinary people (through the use, for instance, of social media tools) to do things with personal data that only large organizations used to be able to do.[145]

The current technological environment, where business models encourage users to disclose personal information and where the users (namely the DN) happily do so, not only questions the adequacy of the current legislative framework, but also its effectiveness.[146] Taking into account the avalanche of data that is being produced and the multifarious purposes to which they are used for, what is the actual use and effectiveness of the data minimization principle? Is it still possible to uphold it? Or better, does it still make sense? In this light, it is important to note that the sole focus on data minimization obfuscates the benefits of data sharing for consumers. Notwithstanding the control one should have over his or her data, the fact is that the maximization of this data may also bring relevant advantages to the user. In effect, behavioural ads are overwhelmingly appreciated by consumers.

In brief, the minimization of the processing of information required by the existent legal framework is becoming somewhat unrealistic, unattainable and, moreover, at odds with the current and forthcoming technological environment, business models and user practices regarding privacy, identity and data protection.

---

[142] This mode of computing has been called "affective processing", see Robert, W. Gehl, The Archive And The Processor: The Internal Logic Of Web 2.0 *New Media & Society* 13 (2011): 1228.

[143] *Ibid*. Surveys on privacy attitudes seem to suggest that some of today's SNS users are aware of (and comfortable with) this commercial environment, while others are not. It needs further monitoring to see to what extent these attitudes might change over time.

[144] *Ibid*.

[145] SWIRE, P. 2012 Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection *North Carolina Law Review, 2012; Ohio State Public Law Working Paper 165; 2011 TPRC Conference.* "I suggest the term "data empowerment" to describe how individuals use personal data in social networks and the other many horizontal relationships enabled by modern computing ... the 2008 Obama campaign and the Arab Spring symbolize the political dimension of this empowerment. The discussion of non-profit, religious and other expressive associations shows that the empowerment goes well beyond the realm of political power. More broadly, individuals are empowered to reach out to others on many dimensions, from the cultural (writing, photos, music), to the economic ... to the everyday social interactions of the social networks themselves".

[146] Furthermore, in a recent empirical study regarding how privacy laws affect the location decisions of Internet firms when faced with high legal standards of privacy protection, the ease of access to personal data proved to be a determinant factor. In effect, the study demonstrated that the more a jurisdiction makes collecting and using these data easy, the more attractive the country is. Such analysis highlighted a new privacy paradox according to which the more stringent certain online privacy laws are, the more they induce firms to locate their business in less stringent countries, and finally the weaker actual privacy protection on the internet is. See, ROCHELANDET, F. & TAI, S. H. T. 2012. Do Privacy Laws Affect the Location Decisions of Internet Firms? Evidence for Privacy Havens Available: http://ssrn.com/abstract=2022160.

2.4.2. Hierarchical mind set / vertical architecture

The DPD is aimed at protecting the privacy of individuals by bringing within its scope the information processing activities of companies and organizations that collect and extract information from these individuals. The European Data Protection Directive is thus structured in a hierarchical fashion according to which the information stream is depicted vertically,[147] flowing from the data subjects – usually perceived as individual physical persons - to the data controllers and processors – larger companies and institutions. In principle, the DPD does not cover horizontal relations, i.e, information flows among individual persons. The Directive, in effect, establishes in its Article 3/2 the so-called "household exemption", according to which its rules do not apply to individuals who process personal data for "purely personal purposes" or "in the course of a household activity". In other words, data protection principles and rules do not apply to individuals who make use of personal data just for their own domestic and recreational purposes.

Taking into consideration the ever-increasing merge between public and private spheres and caused by the various developments observed in the field of ICT, the understanding that the DPD had of "purely personal" back in 1995 is today open to discussion and interpretation. In inserting, in the mid-nineties, the so-called "household exemption", the DPD assumed that personal data processed for domestic purposes did not raise privacy risks or issues of responsibility on the side of the data controller, as he or she would only be processing the data for their own private purposes. The directive also departed from the assumption that the processing of data for personal purposes (horizontal relations) would only involve a restricted circle of intimate people and, as such, would not entail the expectation or the need to protect the privacy of the individuals identified. With the rise and consolidation of social networking sites (SNS), these assumptions are highly questionable today. In fact these assumptions are at odds with today's reality and, moreover, with the behavioral trends of DN. The publishing of personal information on SNS, even if for purely personal or recreational reasons, often involves the disclosure of information to large audiences.[148] And this contradicts the assumption that data will only circulate among a restricted circle of people and that its disclosure does not represent any privacy risk.[149] The sharing of information among SNS users also puts into question the definition of "data controller" within the Data Protection Directive. If this definition – a "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data" – is applied literally to SNS then not only organisations such as Facebook or Google Plus would be regarded as "data controllers" (through Art. 4 of the DPD), but also individuals who posted information about others would also be regarded as "data controllers" and thus would have to adhere to the DPD rules.[150]

---

[147] See also, in this respect, SWIRE, P. 2012 Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection *North Carolina Law Review, 2012; Ohio State Public Law Working Paper 165; 2011 TPRC Conference.* The author also depicts the shift from vertical to horizontal relationships in computing.

[148] The average Facebook user has 130 friends and is connected to 80 community pages, groups and events (http://www.facebook.com/press/info.php?statistics).

[149] Art. 29 WP has clarified a number of instances where the activity of an SNS may not be covered by the household exemption, namely "when the SNS is used as collaboration platform for an association or company" or "when access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS or the data is indexable by search engines." As noted in its Opinion, "a high number of contacts could be an indication that the household exception does not apply and therefore that the user would be considered a data controller", Article 29 Working Party, Opinion 5/2009 on online social networking, 2009b, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[150] Wong, Rebecca, "Social networking: a conceptual analysis of a data controller". *Communications Law* 14 (2009): 142-149.

There is thus an urgent need to review the adequacy of the hierarchical model and vertical focus of the current data protection legal framework (data controller – data subject),[151] as well as to clarify the rules applying to data processing by individuals for private purposes, that is, at a horizontal level.[152]

2.4.3. Consent

In the context of Data Protection legislation, consent is one of the requirements for the lawful processing of personal data. It corresponds to any freely, given, specific and informal indication of the wishes of a data subject, by which he or she agrees to the processing of personal data related to them.[153] The obtained consent, moreover, can only be used for the specific processing operation for which it was collected.

Despite the importance of consent to the protection of a data subject's privacy, it is important to bear in mind that an excessive dependence on consent may overload the user's online experience. Moreover, the constant requirement of opt-in consent for the collection and processing of data is not in line with DN's browsing and navigating habits.[154]

Proposals to solve the problem of the burdensome requirement for constant consent include software agents, as an effective way to achieve the protection of privacy, particularly challenged by new Information Technologies. The underlying idea is that a technological architecture based on 'Privacy Agents', which meets a series of legal requirements to ensure the validity of consent delivered through such agent, could be useful to avoid overwhelming the data subject with repeated requests of consent, while protecting his/her privacy. This option,[155] thought for the general Internet users, could also be applied to DN users.

---

[151] Despite recognizing the lack of safeguards that need to be addressed for individuals who upload their own personal data into the internet (social networks, cloud computing services, etc.), Art. 29 WP "does not recommend, however, revising the terminology used in the Data protection framework for data controller and data subject relationship in the context of Web 2.0 technologies or cloud computing, but rather, to continue using the "data controller – data subject" dichotomy and enhancing their responsibilities, which appears by some outmoded in Web 2.0 technologies" - Wong, Rebecca "Data protection: The future of privacy". *Computer Law & security Review* 27(2011): 53. See also Article 29 Working Party 2009a. The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.

[152] In this light, a number of questions may be posed: What is to be understood by "purely personal purposes"? Does the posting of information on an SNS equate to the disclosure of information for private purposes, that is, to our private (although admittedly large) group of selected contacts? Or – depending on the access to the information - does it equate to the disclosure of information to the public? How many people have to have access to that information for its diffusion to become processing of personal data for private purposes or, instead, disclosure to the public?

[153] See Article 2 (h) of DPD and article 2 (h) of Regulation (EC) No 45/2001.

[154] The systematic need for opt-in consent is also out of touch with the ubiquity of current and future mechanisms of data processing, rendering ineffective the existing notice and choice regime. In effect, with the forthcoming development of the Internet into an Ubiquitous Computing environment (also called Ambient Intelligence or Internet of Things), the current opt-in consent model is frankly not sustainable in the long run. The trend is to move towards a frictionless, mobile and ubiquitous technological environment in which continuous requests for consent will be extremely difficult to articulate. For an overview of the technological developments leading towards an Ambient Intelligence Scenario, see Andrade, Norberto, Technology and Metaphors: from Cyberspace to Ambient Intelligence". *Observatorio (OBS*) Journal* 4 (2010): 121-146. For an overview of the challenges posed by the vision of Ambient Intelligence, see Antoinette Rouvroy, Privacy, Data Protection, and The Unprecedented Challenges of Ambient Inteligence *Studies In Ethics, Law, And Technology,* Berkeley Electronic Press (2008).

[155] Daniel Le Metayer and Shara Monteleone, "Automated Consent through Privacy Agent: legal requirements and technical architecture", *Computer Law Security Review* 25 (2009)136-144.

2.5. Digital natives and the EU law making process

In order to increase the effectiveness and reduce the overall costs of regulation, the EU has been for more than a decade engaged in improving the quality of its law making processes, instruments and outcomes. These efforts can be grouped into what has been called "Better Regulation" (BR) policy, recently re-labelled as "Smart Regulation" strategy. Taking into account that, among its various objectives, BR "seeks to ensure that decision-making meets the needs and expectations of citizens",[156] we argue that a tighter connection should be established between DN (namely their expectations) and the EU law making process. The latter should, moreover, strive to understand the behavioural trends of these young citizens, adapting its rules in a way that fosters the desirable behaviour and prevents the non-desirable ones. In this section, we propose and explain how EU law making process could (and should) take into account collected data from DN (behavioural, cognitive, etc.), namely in the ambit of the so-called impact assessment (IA) procedures.

2.5.1 Better / smart regulation

As more and more laws applicable in the EU Member States (MS) have their origin in EU-decision-making processes, the need to simplify and improve the quality and effectiveness of the regulatory environment has progressively assumed greater importance, ranking high on the EU agenda. In order to achieve these goals, the European Commission (EC) has deployed a detailed strategy and policy of "Better Regulation",[157] devising a series of different processes, structures and tools to prepare new legislation (looking at new initiatives proposals still under negotiation) and to review the existing one (legislation already enacted).[158] In this light, the Better Regulation programme includes a mix of different actions:

- "introducing a system for assessing the impact and improving the design of major Commission proposals;
- implementing a programme of simplification of existing legislation; testing Commission proposals still being looked at by the Council of Ministers and the European Parliament, to see whether they should be withdrawn;
- factoring consultation into all Commission initiatives;
- looking at alternatives to laws and regulations (such as self-regulation, or co-regulation by the legislator and interested parties)."[159]

In its overall goal to prepare and apply the best regulatory tools at the EU level, the BR strategy is articulated in three key actions: simplification, reduction of administrative burdens and impact assessment. In the following, we look at the latter.

---

[156] ALLIO, L. 2007. Better regulation and impact assessment in the European Commission. *In:* KIRKPATRICK, C. & PARKER, D. (eds.) *Regulatory Impact Assessment. Towards Better Regulation?* Cheltenham, UK: Edward Elgar.

[157] See ec.europa.eu/governance/better_regulation/index_en.htm. The Better Regulation policy had its origin in 2001 with the Mandelkern report on Better Regulation. For an evolution of the "better / smart regulation" agenda at the level of the EU, see Ibid. MCCOLM, H. 2011. Smart Regulation: The European Commission's Updated Strategy. *European Journal of Risk Regulation***,** 9-11. ALLIO, L. 2011. On the Smartness of Smart Regulation - A Brief Comment on the Future Reform Agenda. *European Journal of Risk Regulation*.

[158] Furthermore, by re-labeling the strategy "Smart Regulation", the EC has connected the two extremes of the policy cycle, enhancing the ex ante impact assessment of a given proposal, while devoting more attention to the ex post evaluation and outcomes of the produced legal instrument. See MCCOLM, H. 2011. Smart Regulation: The European Commission's Updated Strategy. *European Journal of Risk Regulation***,** 9-11.

[159] EUROPEAN COMMISSION 2006. Better Regulation - Simply Explained. Luxembourg: Office for Official Publications of the European Communities.

2.5.2 Impact Assessment (IA)

A crucial element in producing better laws is to anticipate and acknowledge their likely impacts. In this way, the Commission "has focussed on IA as the key element for its BR agenda",[160] rendering it compulsory for major policy proposals.

The IA[161] is a "tool that assists regulators in their efforts to structure decision-making and increase the effectiveness of regulatory outcomes".[162] It is a threefold system that assesses and analyses the economic, social and environmental impacts of a proposal. The IA is linked to the preparatory stage of policy-setting and decision-making on the one hand, and the revision of the *acquis communautaire*, on the other.[163] In effect, IA is progressively being understood as a "wide-ranging 'process'[164] structuring and closing the policy-making cycle, influencing and supporting the various different aspects of the Better Regulation policy".[165] Moreover, the IA consists of "a knowledge-based approach — aimed at ensuring that decisions on whether and how to proceed with an initiative are based on solid evidence and a thorough analysis of options".[166]

In more detail, IA is a set of logical steps to be followed when preparing policy proposals; it is a process that prepares evidence for political decision-makers on the advantages and disadvantages of possible policy options by assessing their potential impacts (the results of this process are then summarised and presented in the IA report).[167] At a more technical level, the carrying out of an IA is composed by the following key analytical steps: identifying the problem, defining the objectives, developing main policy options, analysing the impacts of the options, comparing the options, and outlining policy monitoring and evaluation.[168]

2.5.3 Integrating digital natives into the IA system

In the ambit of Smart Regulation consultation exercises, and regarding the effort to improve the transparency of the process, the Commission strives to hear the views of all interested parties, namely those of SME (small and medium-sized enterprises), non-governmental organizations representing vulnerable stakeholders and citizens. Nevertheless, and further to allowing (and incentivizing) stakeholders to comment on planned impact assessments (by publishing 'roadmaps' outlining its plans for the broad direction of proposals, the public consultation process and supporting analysis), the EC should also integrate DN (as an important and specific category of stakeholders) in the very process of impact assessment regarding legislative proposals in the field information and communication technologies (ICT) regulation. In other words, the process of

---

160 ALLIO, L. 2007. Better regulation and impact assessment in the European Commission. *In:* KIRKPATRICK, C. & PARKER, D. (eds.) *Regulatory Impact Assessment. Towards Better Regulation?* Cheltenham, UK: Edward Elgar.

161 See, in general, MEUWESE, A. C. M. 2008. *Impact Assessment in EU Lawmaking,* The Hague, Kluwer Law International.

162 ALLIO, L. 2010. Keeping the Centre of Gravity Work: Impact assessment, Scientific Advice and Regulatory Reform. *European Journal of Risk Regulation***,** 76-81.

163 ALLIO, L. 2007. Better regulation and impact assessment in the European Commission. *In:* KIRKPATRICK, C. & PARKER, D. (eds.) *Regulatory Impact Assessment. Towards Better Regulation?* Cheltenham, UK: Edward Elgar.

164 As a process, IA "naturally spills over into the development of other equally crucial elements of regulatory reform, such as enhanced planning and programming; systematic and timely consultation practices, a smoother implementation and enforcement of legislation, and enhanced transparency and accountability" ALLIO, L. 2010. Keeping the Centre of Gravity Work: Impact assessment, Scientific Advice and Regulatory Reform. *European Journal of Risk Regulation***,** 76-81.

165 Ibid.

166 EUROPEAN COMMISSION 2006. Better Regulation - Simply Explained. Luxembourg: Office for Official Publications of the European Communities.

167 EUROPEAN COMMISSION 2009. Impact Assessment Guidelines.

168 For a detailed description of these key analytical steps, along with practical examples of how they have been carried out in previous IAs, see Ibid.

gathering valuable input from stakeholders should not only restrict itself to consultation exercises (which are obviously welcome), but involve also the gathering of empirical collective data from specific legal addressees, such as the DN.

In this respect, and further to IA's focus on reducing the administrative burden and compliance costs imposed on economic operators by regulation, we argue that IAs should also address the likely impacts of (ICT) regulation by identifying and understanding the behavioural trends of the users of new technologies and the addresses of the legal instruments under scrutiny, The evidence gathered through the examination of DN behavioural trends may prove to be extremely useful in the development of possible policy options in the IA exercise, along with the analysis of the options' impacts.

Moreover, the collection of data regarding the behavioural, cognitive and attitudinal trends of DN (and the assessment of how the latter could impact on current legislation) is in line with the efforts that the Commission has put on reforming the way scientific advice is collected, validated and used throughout the decision-making process. This is particularly evident in the 2009 revised IA Guidelines, which "reinforce the requirement for desk-officers to rely on data that is of high quality".[169] The collection and use of DN reliable data requires the further integration of this particular category of stakeholders into the IA exercise in particular, and in the EU law making structure in general. Along this process, DN move from mere and passive addressees of laws to active contributors and shapers of the latter.

As a way to complement and support the diffusion of comprehensive IS processes, and as a reinforcement of the principle of evidence-based decision-making, we thus propose the incorporation of specific DN data collection and analysis into the impact assessment procedures of ICT legal proposals. This recommendation could also contribute to solving the increasing trend for law and regulation, namely with regard to computer and communications sector, to become increasingly detailed and overly complex.

Despite the alleged benefit of increasing their certainty as to compliance, and as noted by Reed, over-complex laws have their normative effort greatly weakened, becoming also contradictive and subject to frequent amendment processes.[170] As a solution, Reed proposes to abandon the search for certainty and to adopt a method of law making which seeks to influence behaviour by requiring the law's subjects to make their own qualitative assessments as to whether they were meeting the obligations imposed on them.[171] This proposal could be used in the specific case of DN, inviting the legislator to approach directly this specific category of legal subjects, assert if they were complying with the obligations established in law, and – in the case of a negative response - understand why they were not. Engaging into qualitative assessments of law's subjects "will not only make the law more easily understandable by those to whom it applies, but will also increase the normative effect of computer and communications law".[172] Reed's proposed law making approach, which concentrates on human actors rather than on the technological activities those actors engage in,[173] is in line with our own proposal of integrating DN collected data to the impact assessment procedures of ICT laws or legislative proposals. Using the scholar's methodology, and replacing the terms laws with the one of IA, the latter should thus:

- "Identify the behaviours which are likely to emerge from the innovation they want to regulate;

[169] ALLIO, L. 2010. Keeping the Centre of Gravity Work: Impact assessment, Scientific Advice and Regulatory Reform. *European Journal of Risk Regulation*, 76-81.

[170] REED, C. 2010. How to Make Bad Law: Lessons from the Computing and Communications Sector *Queen Mary School of Law Legal Studies Research Paper No. 40/2010*.

[171] Ibid.

[172] Ibid.

[173] Ibid.

- Decide which behaviours are to be fostered and which discouraged; and
- Devise mechanisms for persuading the human actors to behave in the desired manner".[174]

In this way, IAs would reinforce the regulators' capacity to meet the societal expectations of legal subjects. Moreover, IAs would also prepare laws designed according to the legal addressees' current and prospective behavioural, attitudinal and cognitive trends, reinforcing the overall effectiveness of the regulatory environment.

This remodelled IA proposal would allow lawmakers to better understand DN attitudes regarding personal data and identity protection and to shape future laws according to their corresponding needs and expectations. In specific, the legislator would be able to identify areas where a stricter regulation would be necessary (such as in the field of profiling and its unintended consequences); and identify other areas where a less stringent approach would be more opportune (such as in the field of the systematic opt-in consent).

[174] Ibid. As a concrete example of an existing law redrafted to fit such lawmaking approach, Reed proceeds to a partial redraft of data protection law which aims to comply with the principles of law-system quality. See, REED, C. 2010. How to Make Bad Law: Lessons from the Computing and Communications Sector *Queen Mary School of Law Legal Studies Research Paper No. 40/2010*.

Part 3 - The "Prospective" Use of Social Networking Services for Government eID in Europe

3.1 Introduction: the end of governmental monopolies on the provision and authentication of citizens' identities — the rise of new actors and stakeholders

The attribution and certification of citizens' identities was understood, for many centuries, as a function (or even a privilege) typically and exclusively assigned to governments and other public authorities. These processes were, moreover, centralized, highly regulated, and bureaucratic. The government's monopoly over the 'identity business' followed administrative imperatives such as the collection of tax, administration of justice, regulation of commerce, security, surveillance, access to territory, and control of immigration. Today, the provision of identities has evolved into a much more flexible, decentralized, and less bureaucratic processes, involving a myriad of other actors and stakeholders.

In recent years and especially within the online world, an important shift from government-issued electronic identities (eIDs) to other sources and means of identity attribution and authentication has taken place. The issuance of digital identities, such as the ones derived from social networks, social media based on user-generated content, browser eIDs or virtual worlds, nowadays constitutes additional (if not alternative) models to the ones established by states for identification and authentication. While the identification and authentication processes controlled by states and public authorities were inherently political, following governmental needs and administrative tasks, today these processes have become more and more socially oriented. Thanks to the development of digital technologies, the global expansion of the internet, and the rise of social networking sites, non-state entities and organizations are — more and more — providing identity elements (tokens, credentials, etc.) to a growing base of users for social interaction, communication, and transaction purposes.

These 'new' digital identities, which form a very heterogeneous group with different levels of security, integrity, and trust, enable citizens to hold and use a set of identity elements outside the public authorities' sphere and in parallel to the official ones validated by the state. These alternative eIDs, moreover, play an increasingly important role in the online sphere. In effect, they now represent the gateways to the digital environment and to the use of the various services it provides. The growing importance assumed by these novel identification and authentication systems is linked, to a large extent, to the transformation of the internet's initial anonymous infrastructure (where, to quote a famous New Yorker cartoon from 1993, nobody knew you're a dog) into a complex internet identity layer — that is, a set of sophisticated architectural models and processes that identify and authenticate users' identities.

We are thus witnessing an ongoing competition (and even tension) between the traditional way of issuing and managing identities and recent trends in the provision and authentication of identities. While the former consists mainly of unilateral actions endorsed by governments and public administrative organizations, the latter is carried out through private parties or cooperative private-public partnerships.

In this deliverable, we focus not on the policy and legal aspects related to the competition between public and private entities dealing with identification and authentication processes, but on the analysis of the benefits and drawbacks of an eventual cooperation between these two different actors: governments and other public organizations on one side, and private companies and entities on the other.

The remainder of this deliverable is structured as follows: In Section 2 we provide background on social networking technologies, their current status in Europe, and online IdM application for eGovernment. Then, in Section 3, we move to explore the potential merits of government use of SNS-based eIDs. Among the reasons why European governments may be interested in using pre-existing SNS for IdM, we discuss the following: a) large installed base; b) critical mass of users; c) relatively reliable infrastructure; d) high social acceptance of 'social' technologies; e) cost-effectiveness; f) real-name policies (which could render these identities more trustworthy and adequate for official uses); g) mutual recognition and cross-border (EU-wide) interoperability of eIDs; and h) the potential use of biometrics (particularly with the integration of facial recognition). Still, there are several drawbacks, which we review in Section 4. Among these, we consider the following: a) citizen discomfort with using SNS credentials for official interactions; b) unreliable registration processes; c) reduced possibilities for anonymity and pseudonymity (and the attendant threats to freedom of speech and other political participatory values due to the emphasis on using real names); d) potential exclusionary effects for citizens unable or unwilling to use these eIDs; e) problems of neutrality (i.e., which platforms do governments endorse?); f) problems of data ownership; g) security concerns; h) the potential for SNS to track users on government sites; i) jurisdictional issues (i.e., most popular platforms are US-based); j) task complexity; and k) liability issues (assuming that one's SNS-endorsed eID is recognized and used for eGovernment services across different Member States, which party is liable for misuse, theft or impersonation?). Section 5 then describes recent EU policy and legal initiatives in the field of eID, focusing particularly on the legislative measures currently being proposed in Europe, with Section 6 providing a brief conclusion. Throughout, the deliverable calls attention to the need to keep the approach of mutual recognition and interoperability of eIDs open to evolution, technological progress, and new business models. The paradigm of state monopolies over the provision of identities is outdated. Additional alternatives to this model should be sought in the private sector.

3.2 Background

3.2.1 Social networking services

The popularization of the internet and web has been accompanied by the emergence and wide adoption of technologies for social networking. Social networking services (SNS) allow users to create profiles within a bounded system and maintain lists of other users and organizations with which they share a connection, in order to view and traverse these connections (Boyd & Ellison, 2008). These services regularly encourage users to include identity-related information (such as name, location, date of birth, organizational affiliation, photograph, etc.) in their profiles. Similarly, social media applications facilitate communication and social interaction among users and organizations and build on the creation and exchange of user-generated content (Kaplan & Haenlin, 2010), usually based on a social networking component. More than merely being communication tools, these technologies are now being described in terms of "platforms" (Gillespie, 2010). As SNS necessarily involve the collection and sharing of personal information (to varying degrees, depending on the service) they have also been described as identity platforms.

3.2.2 European situation

Citizen adoption and use of SNS in Europe has been impressive. More than half (52%) of Europe's internet users (and therefore about half of all Europeans) use SNS (see Figure 2 below). But there are notable geographical differences across Member States. For example, internet users in Germany (37%) are less likely to use SNS than any of their EU neighbours, while Hungarians, Latvians, Maltese, Irish, Slovakians, and Cypriots are the most active users (between 66% and 80%). SNS adoption has increased with the spread of the internet in Europe; however, there is a generational split as younger people (i.e., digital natives) use the internet less outside SNS in all Member States, while older people who use SNS are practically the same as the percentage of internet users. This generational split may be set at 40 years of age, as the [40-54] age group tends to act more like the 55+ age group while the [25-39] age group tends to act more like the [15-24] age group (Lusoli

et al., 2012). As discussed in Section 5, these generational differences have import on the use of SNS for identity provision.

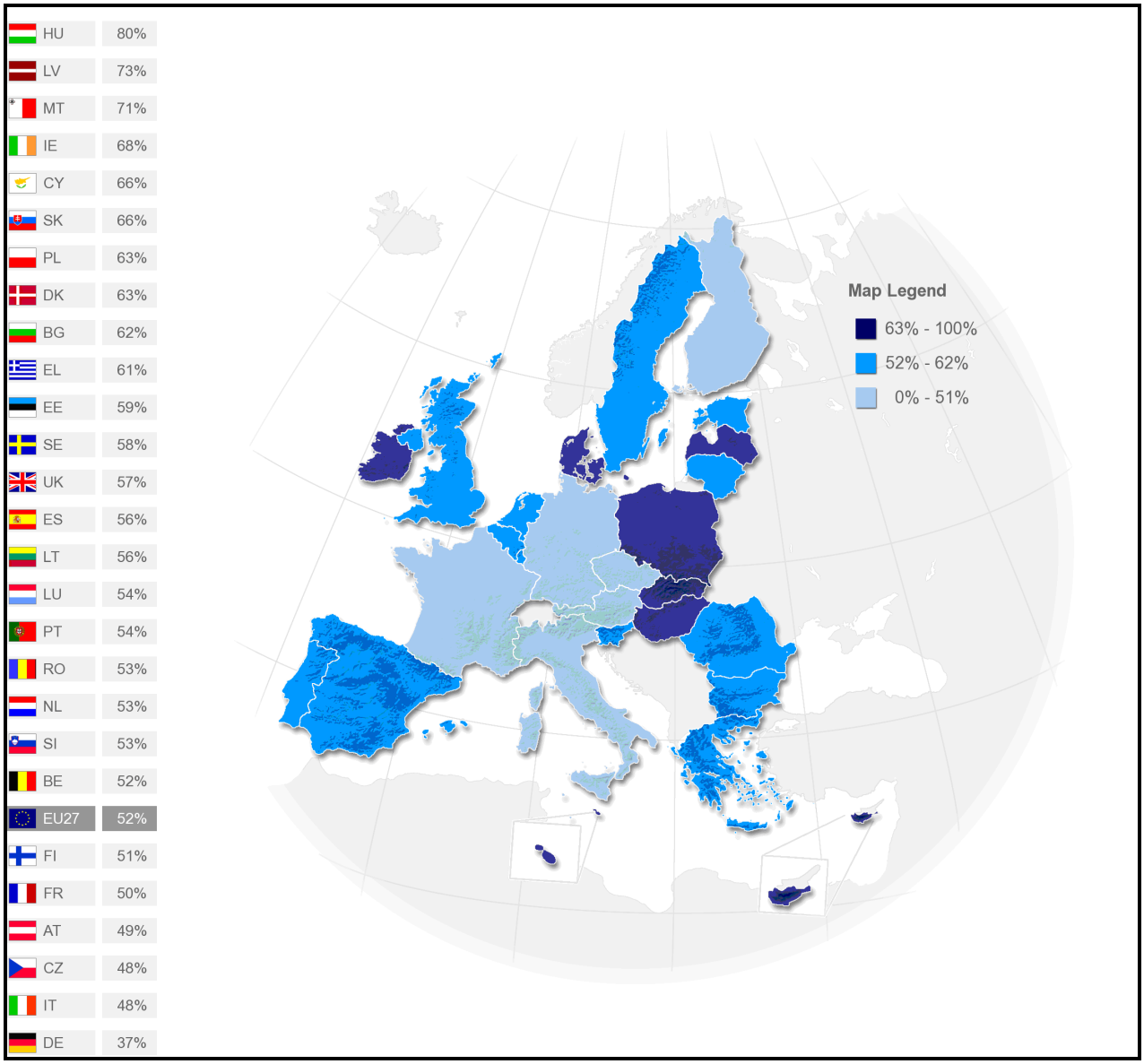


Figure 2: Distribution of SNS users in the EU27 (Lusoli et al., 2012)

Europe's current position in the supply and development of SNS is rather weak. Although usage is almost as high in Europe as it is in the US, American companies provide about two-thirds of the platforms; this includes the number of firms based in Europe that provide SNS, their share of revenues, and the number of employees (Ala-Mutka et al., 2009). As with the differences in user adoption, this market situation affects the potential use of SNS in identity service provision within Europe

3.2.3 eGovernment and online IdM

'eGovernment' generically describes the use of information technology, and more specifically the internet and web, to provide information to the public, to deliver public services, to enhance government performance, and to engage citizens.

For our purposes in this deliverable, it helps to distinguish between basic eGovernment services from more sophisticated services that may require an identification or authentication component.

Basic eGovernment involves the provision of information about public policy, governance, laws, regulations, and documents online, as well as basic forms of (mostly one-way) communication. More advanced forms of eGovernment services involve two-way communication between government and citizen (in which a citizen's identity may need to be authenticated), transactional services including eVoting, filing taxes, applying for certificates, licenses or permits, as well as financial transactions. Advanced eGovernment may also include more interactive and connected services such as eParticipation, eConsultation, and online decision-making (UN, 2012, p. 123).

These more sophisticated eGovernment services stand to benefit from trustworthy and robust IdM systems — particularly those based around transactions and online interaction and engagement (Aichholzer & Strauß, 2010).

3.3 The case for leveraging SNS in government IdM

Having introduced basic ideas around SNS, their current status in Europe, and the opportunities for online identity provision in eGovernment, in this section we address the potential positive reasons for leveraging SNS platforms for government IdM. We do so in light of emerging real-world proposals to do just that. For example, Washington State in the U.S. recently announced that it would begin registering voters via Facebook (Farivar, 2012). Elsewhere, recent reports in the UK claim "ministers are said to be considering using Facebook, among other services, to act as official identification for accessing public services online" (Lee, 2012). Likewise, in the Netherlands there have been discussions surrounding the possible integration of the government's digital signature system (known is DigiD) with Facebook (Schoemaker, 2012). We believe that these trends will likely spread, including throughout other parts of Europe, hence the need to assess both their positive and negative aspects. This section focuses on the former while Section 4 addresses the latter.

3.3.1 Large installed base

One of the most intriguing features of mainstream SNS such as Facebook and LinkedIn for online IdM is the sheer number of users of these services.[175] As social media evangelists are keen to point out, if Facebook were a nation it would be the third largest in the world (The Economist, 2012). If we compare such figures with the numbers of citizen adoption and use of national eIDs we see stark differences.

For example, in Kubicek and Noack's (2010) comparative research on four national eID systems – Austria, Belgium, Germany, and Spain – the use of the eID-based online authentication function was found to be extremely low, despite the differences between the systems. In short, for online tax declarations, the share of online authentication by eID was less than 10%. The percentage of taxpayers providing electronic tax returns through the use of eID for authentication was particularly low: only about 7% in Belgium, 0.2% in Spain and 1.0% in Austria in the summer of 2009.

Despite the systems' dissimilarities, the authors explain the limited expansion and usage of official eIDs as follows:

- They are not compatible with established values and procedures.
- The technical process of authentication is too complex and not easily understood.
- The relative advantage of higher security is neither visible nor observable.
- The technical components are not easy to install and easy to use.

[175] For example, at the time of writing Facebook claimed 1 billion users (Lee, 2012) — although at least 83m of these are said to be fake (BBC News, 2012)

3.3.2 Critical mass of users

More than just having lots of users, it may be the case that certain SNS (especially Facebook) have reached a critical mass such that, through ongoing network effects, the rate of adoption is becoming self-sustaining and is creating further growth. Governments may wish to leverage these network effects for their own purposes especially as their own eID systems have witnessed limited uptake.

3.3.3 Infrastructure reliability

While most SNS are relatively new platforms dating back to the late 1990s or 2000s (e.g., LinkedIn was founded in 2003 and Facebook in 2004), they are frequently visited and heavily used. For example, Facebook users spend 10.5 billion total minutes per day on the platform (a figure that excludes mobile activity) (Protalinski, 2012). Despite such heavy usage, these services have proven fairly reliable to date.

3.3.4 Social acceptance of SNS

The success of the most popular SNS also bears testament to the high degrees of social acceptance, despite ongoing concerns about unintentional information disclosure and other privacy violations on many platforms. They are even becoming taken for granted facets of online life, especially among young people for whom these networks are indispensable communications tools.

3.3.5 Cost-effectiveness

Because much of the infrastructure for identity provision is already in place with SNS, they are arguably a cost-effective option for government online IdM. For example, Washington State's decision to use Facebook for voter registration was motivated in large part by costs concerns:

> "Your name and date of birth are pulled from Facebook profile, then it operates exactly as it does if you're not in Facebook. Our state database checks to see if you're already registered. If you are, it will take you to MyVote service, [where] you can update registration information. You also need a Washington state ID or driver's license. We do another real-time check to match that this is a real person who is registering.
>
> *It saves the county $0.50 to $2 per registration and saves the state $0.25 per registration, as of 2009*. If this works as we expect, Facebook and Microsoft will be more than happy to work with any other state that has online registration." (Farivar, 2012)

In Europe, where public finances are especially strained, such costs saving will very likely prove attractive to enterprising public sector organizations.

3.3.6 Real-name policies

As SNS move to encourage, if not require, users to register their real names, these identities would likely prove more trustworthy and adequate for official uses. As examples, both Facebook and Google+ are pursuing policies for the use of real names in an attempt to make them more reliable:

> "Facebook is a community where people use their real identities. We require everyone to provide their ***real names***, so you always know who you're connecting with."[176]
>
> "Google+ makes connecting with people on the web more like connecting with people in the real world. Because of this, it's important to use your common name so that the people you want to connect with can find you. Your common name is the name your friends, family or

[176] 'Facebook's Name Policy': https://www.facebook.com/help/?page=258984010787183 (emphasis original) [Accessed November 5, 2012]

coworkers usually call you. For example, if your legal name is Charles Jones Jr. but you normally use Chuck Jones or Junior Jones, any of these would be acceptable."[177]

Of course, verifying that users are actually providing their real names is very difficult in practice, as we discuss in Section 4. Moreover, beyond policies for the use of real names, a robust and usable identity platform would need access to other types of 'real' data such as date of birth, place of birth, nationality, and so forth. These are data types that mainstream SNS are not currently capable of reliably enrolling.

3.3.7 Mutual recognition and cross-border interoperability[178]

Today there is a proliferation of different IdM systems across the EU — a fact that makes the eID process more and more complex. Furthermore, as previously discussed, new actors and institutions are emerging in the data processing and eID fields.

One of the principal factors hampering the development of interoperable IdM systems[179] across Europe is the diversity (and, often, incompatibility) of technical approaches to the protection and management of eIDs by EU Member States. As observed in previous studies (Graux et al., 2009) and surveys (Leenes et al., 2009), 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 or drivers licenses), to reliance on electronic signatures and two-factor authentication systems.

The construction of a harmonized and fully functional pan-European IdM, where eIDs issued by one EU Member State can be identified, authenticated, and recognized in a different one, is thus deemed fundamental for the deployment of cross-border services within the EU27, as well as for the economic growth of Europe and the completion of the EU Digital Single Market. Incompatible technical systems for the provision, authentication, and recognition of eIDs create barriers to the use of electronic communications and electronic commerce, and hinder the free movement of goods and services in the internal market. Therefore, it is important to make these different IdM systems and architectures interoperable, ensuring the mutual recognition of different eIDs across Europe.

Hence, in a European context, the concept of interoperability[180] assumes outstanding importance — eIDs will have little value for the free movement of persons, goods, services, and capital, as well as the stated objectives of constructing a fully operational single digital market, if they are not recognizable outside national borders and across different Member States.

Relying on existing SNS identity credentials and authentication systems, and benefiting from the mass of users they encompass and the different countries in which they operate, could constitute a valid way to ensure the interoperability of IdM systems and the mutual recognition of eIDs.

3.3.8 Biometrics

SNS are increasingly integrating biometrics such as facial recognition into their platforms. Facebook's facial recognition system, which facilitates the "tagging" of uploaded photos in an animated fashion, is a prime example of this trend. Depending on the reliability of the implementations, such moves would arguably strengthen government identity assurance by providing a second factor with which to identify or authenticate users.

---

[177] 'Google+ Page and Profile Names': http://support.google.com/plus/bin/answer.py?hl=en&answer=1228271 [Accessed November 5, 2012]

[178] In the eID context, 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 an electronic communication" (Myhr, 2008).

[179] Four main models of IdM can be identified within the massive proliferation of eID systems: "siloed", centralized, federated, and "user-centric" IdM systems (OECD, 2009).

3.4. Drawbacks

Having reviewed the possible merits to leveraging SNS for government online IdM, this section reviews some of the downsides. It is likely that there are additional drawbacks that we have yet to identify. What follows is a preliminary description of the potential problems with government use of SNS for identity provision.

3.4.1 User unease

Despite high levels of social acceptance of SNS and ever-impressive growth, for different reasons users may be uncomfortable with the idea of their social networking credentials being used for official interactions with government. For one, SNS are often seen as spaces for socialization and play. Designating them as platforms for official administration and government transactions may unintentionally make them less attractive to users. There are also fears of government surveillance of users on SNS — warranted or not — which would be amplified if SNS credentials were used to transact with public sector bodies (Martin & Bonina, 2013).

Another relevant dimension regards under what circumstances government organizations are permitted to block users or reject credentials in these online environments. An incident in the U.S. from late 2010 speaks to the ongoing uncertainty and sensitivity of these issues. It was revealed that the Transportation Security Administration (TSA) — the U.S. government agency responsible for overseeing the nation's airport security — had blocked a critical member of the public on Twitter who had expressed his opposition to the agency's latest round of security measures (involving 'advanced imaging technology' and 'enhanced pat-downs'). While he was eventually unblocked by the TSA, the reasons for the original censor remain unclear (Sassaman, 2010). Relevant to the current discussion is the importance of establishing rules of engagement for public bodies interacting with citizens through SNS.

3.4.2 Registration reliability

Currently, SNS do not normally check the physical identification of a person in order to ensure the unambiguous matching between an electronic identity and a physical person (SNS base the creation of accounts on purely online interactions, although services such as Twitter are now requiring proof of identification for certain 'verified' accounts such as those of celebrities and politicians[181]). The interesting question in this respect is whether SNS would introduce general processes that would pass suitable accreditation requirements to satisfy their use for non-trivial government applications, or whether governments will (reluctantly) accept the guarantees that these SNS can offer. Arguably, it would be in the interest of SNS to satisfy government reliability requirements because they would likely not want their users to log out of their service in order to log on with another provider to use an eGovernment service.

3.4.3 Threats to anonymity and pseudonymity

Using SNS to interact and transact with government — and particularly those services based on real-name approaches — reduces the possibilities for user anonymity and pseudonymity. Depending on the type of eGovernment service, interaction or transaction, it may be appropriate to require users to provide certain identifying information (e.g., paying tax online). In other contexts, however, it may be unnecessary or inappropriate to do so. For example, for certain kinds of government interaction (e.g., seeking health advice or online voting) it may not be conducive or necessary to fully disclose an identity. For politically sensitive activities, such as engaging in an online consultation around a controversial subject, there are attendant threats to the freedom of speech and other political participatory values if the use of real names or other identifying information is required. The ongoing "nymwars" attest to the importance and policy relevance of these debates.

[181] However, this verification process is not foolproof. For example, in 2012 a 'verified' account for Rupert Murdoch's wife was falsely created (Mitchell, 2012).

3.4.4 Exclusion

As noted in Section 2, despite the incredible and rapid growth of SNS not all Europeans use the services. In fact, just around half of them currently do. Therefore, there are potential discriminatory effects for citizens unable or unwilling to use these kinds of eIDs — those sans ePapiers, as it were. This becomes highly relevant from a public policy perspective if and when the use of these kinds of identifiers is made mandatory for access to online public services.

3.4.5 Neutrality

Policies that designate the use of commercial SNS for online access to eGovernment services face the problem of deciding which platforms to endorse. Should governments be selecting certain providers over others? If so, based on what criteria? This is, in effect, a problem of neutrality, which some authors are now considering (Thierer, 2012).

There are ways of solving this problem. Governments could introduce a voluntary system with minimum standards for platforms to meet in order to qualify as an official identity provider. If SNS were so inclined, they could apply to become a provider of identity services. Users could then choose their preferred provider, much like they already do with banks.

A more fundamental concern however, which is particularly salient in the European context, is whether governments should even be adopting policies that encourage (or potentially require) citizen adoption and use of commercially-driven platforms.

3.4.6 Data ownership

A related issue concerns data ownership within SNS. Who owns the identities and transaction-related data that are generated through eGovernment applications of SNS? Moreover, are SNS permitted to aggregate data from government-citizen interactions and transactions into their profiling and advertising activities? These questions will impact on European data protection laws and the legal interpretations are anything but trivial.

3.4.7 Security

If and when the credentials provided by SNS are adopted for eGovernment services, they will be used more frequently and for increasingly important transactions (such as tax, health, or voting). Their value to users will therefore increase, and so will their value to malicious actors. There will inevitably be increased attempts to fraudulently obtain and abuse these identifiers, which means unless systems are adequately secured, new forms of identity fraud will arise.

3.4.8 Privacy

The use of SNS credentials for online public services introduces new privacy risks such as the potential for these third-party identity providers to track users on government sites. A case from the UK illuminates these risks. In November 2010 it was revealed that users of a National Health Service website that provides health advice (known as NHS Choices) had details of their visit unknowingly communicated to Facebook and other companies (Hoeksma, 2012). The information that was passed on to these firms included details of the ailments or conditions that the user was investigating, which is clearly medically sensitive.

The underlying problem relates to the ubiquitous online tracking that SNS engage in. Many, if not all, of these services actively track their users across the web, sometimes even when they are not logged in (Valentino-DeVries, 2011). Should such practices be allowed on an official tax or health service website?

3.4.9 Jurisdictional problems

Compounding the privacy problems are jurisdictional ones related to the enforcement of EU data protection law. Since most of the more popular social networking platforms are based in the U.S.,

their use by European governments for online IdM purposes introduces additional complications and complexities. For example, Google and Facebook's ongoing problems with data protection authorities in Europe would likely be multiplied if these services were officially adopted for online identity provision. In a sense, this would be like adding fuel to an already raging data protection fire.

3.4.10 Task complexity

Becoming a certified official identity provider would mean that SNS would need to configure their platforms to able to deal with a range of different kinds of eGovernment transactions and interactions. These eID technologies would need to enable the secure identification and authentication of persons that then interact with public administration bodies and governments (from different Member States), as well as with businesses. This, we believe, is a much more complex proposition that providing basic social networking functionality. It may involve a considerable amount of system re-engineering.

3.4.11 Liabilities

Assuming that one's SNS-endorsed eID is recognized and used for eGovernment services across different Member States, which party is liable for misuse, theft or impersonation? Unless mechanisms and safeguards are put in place to account for and reconcile errors or the misuse of identifiers, then the use of SNS for identity provision in eGovernment services may open up a "Great Liability Sinkhole" (Stevens, 2012) with unknown consequences.

3.5. EU policy and legislative initiatives in the field of eID

Recently we have seen an onslaught of legislative and policy initiatives aimed at facilitating the identification and authentication of eIDs, both at the EU and Member State levels. This section analyses the recent EU model for electronic identification presented by the European Commission, and then explores how it fosters or inhibits the potential adoption of SNS for government IdM purposes. We start by reviewing the main steps taken at the EU level regarding the revision of the Electronic Signatures Directive and the proposal for a new Electronic Trust Services Regulation182. This legislative initiative embodies a new Identification, Authentication and Signature (IAS) policy for Europe.

3.5.1 Revising the Electronic Signatures Directive to propose an electronic trust services regulation

The main objective of Directive 1999/93/EC on a "Community framework for electronic signatures" — adopted in 1999 — was to promote trust in the digital environment. The idea was fairly straightforward: establish a framework for electronic signatures (eSignatures) that would facilitate their use within the European internal market. Nevertheless, more than a decade later it is notorious that this Directive has largely failed to accomplish this objective, generating little interest and traction. In effect, eSignatures are rarely used in Europe. Different reasons have contributed to this state of affairs, including the technical complexity of eSignatures (the understanding and use of which requires not only time but also sophisticated technical knowledge) and the development of different online business models (namely in the e-commerce sphere) that did not require, and thus did not promote, the use of digital signatures and other forms of identification schemes as envisioned in the Directive.

Furthermore, not only did the Directive cover just one part of all types of electronic IAS, it did not offer a legal definition of the concept of identity and how identity can be established in an electronic environment (Graux et al., 2009, p. 118). Moreover, it failed to solve the key question of authentication: "who is the person with whom I am communicating, and how do I know this for

[182] Proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market COM(2012) 238.

certain?" (Graux et al., 2009, pp. 108-109).[183] Divergences in Member State implementation of the Directive only contributed to deepening the discrepancies and the different legal approaches to eID management. As a result, the current legal framework regarding eID on a European level is deeply fragmented, borrowing some elements from the ePrivacy and Data Protection Directives, others from the eSignatures Directive, and others from national regulatory approaches (Andrade, 2012a).

The Electronic Trust Services Regulation proposal lays down a comprehensive EU cross-border and cross-sector framework for secure, trustworthy, and easy-to-use electronic transactions that encompass electronic IAS. The idea is to strengthen the EU Single Market by proposing a legal framework to enhance trust and confidence in cross-border electronic transactions. The need to reduce legal fragmentation, to enhance harmonization, and to provide greater legal certainty regarding the rules regulating the functioning of the internal market (namely in the area of IAS) justified the choice for a Regulation — a legislative act that becomes immediately enforceable as law in all Member States simultaneously (dispensing the need for transposition into national law). Further to establishing and regulating a series of Electronic Trust Services (i.e., eSignatures, electronic seals, time stamping, electronic delivery services, electronic documents admissibility, website authentication), the proposal enables mutual recognition and acceptance of different national eID schemes across the EU. It is important to note that the legal basis underlying this draft Regulation is the development (and completion) of the internal market (i.e., Article 114 of the Treaty on the Functioning of the European Union), and not the provision of identity per se — a task that is acknowledged as falling under the sphere of competences of Member States (cf. Andrade, 2012b). The main purpose is thus to provide a common legal basis to engage each Member State to recognise and accept eIDs issued in other Member States to permit citizens to access online services, enhancing the cross-border interoperability of national eIDs, and thereby allowing citizens and businesses to benefit fully from the Digital Single Market. The identification and authentication scheme proposed by the Commission does not interfere with Member States' own national structures and schemes of eID management, nor does it impose a new mandatory scheme.[184] On the contrary, the draft Regulation adds to the various national eID schemes an overarching and common platform for mutual recognition and acceptance that Member States may adhere to on a purely voluntary basis.[185] The draft Regulation puts forward an EU-wide mutual recognition mechanism according to which Member States, provided they fulfil the five conditions of eID schemes envisaged in the Regulation (see Article 5), may notify the Commission of the national eID scheme(s) used domestically for access to public services. Once these national eID schemes enter into the Commission's list of "notified" eIDs, a Member State must recognise and accept the notified eIDs of other states for cross-border access to its public services that require e-identification.

3.5.2 SNS identity provision in the IAS scheme proposed by the electronic trust services regulation

The objective set out by the proposed Regulation is fairly simple: ensure that citizens and businesses can use and leverage — across borders — their national eIDs to access public services in other EU countries. An interesting aspect of the new Regulation, and important to our discussion on the use of SNS for government IdM purposes, concerns the possible involvement of the private sector in the proposed regulatory framework. In effect, the new legislative act leaves open the possibility of Member States facilitating the use of private sector 'notified' eIDs. While the main focus and priority of the proposed Regulation is on official eIDs, it does not exclude, a priori, private

[183] As stated in the report: "This is an issue which is not resolved by the Directive, which assumes a prior resolution of the identity question without offering specific guidance."

[184] The regulation clarifies this point: "The Regulation does not oblige Member States to introduce or notify electronic identification schemes." Paragraph 2 of Article 4 clarifies that the mutual recognition and acceptance principle applies only to those Member States that have notified their eID schemes.

[185] Article 5 – Mutual recognition and acceptance: "When an electronic identification is required under national legislation or administrative practice to access a service online, an electronic identification mean issued in another Member State which is included in the list published by the Commission pursuant to the procedure referred to in Article 34 shall be recognised and accepted to access this service."

sector eIDs (which we would call 'non-official eIDs') from being notified by Member States and recognized across EU borders. The Regulation, in sum, opens the door to the regulation of private sector eIDs through its eID notification process. Recitals[186] 11, 14 and 20 are pertinent to this point:

- Recital 11: Member States remain free to use or introduce means for electronic identification purposes used to access at least public services. ***They are also able to decide to involve the private sector in the issuance of these means***. [emphasis added]

- Recital 14: One of the aims of the Regulation is to stimulate the functioning of the internal market (…) This can be achieved by enhancing legal certainty and ***allowing the private sector the use of notified electronic identification means for identification purposes when needed for online services or electronic transactions. The possibility to use notified electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many Member States at least for public services and to make it easier for customers or clients to access their online services across borders***. In order to facilitate the use of notified electronic identifications by the private sector, the authentication possibility provided by the Member States cannot discriminate between public or private relying parties. [emphasis added]

- Recital 20: This Regulation sets a general framework for the use of electronic trust services. However, it does not create a general obligation to use them. In particular, it does not cover the provision of services based on voluntary agreements under private law.

If we complement these recitals with the Impact Assessment Report and the Legislative and Financial Statement that accompany the draft Regulation, we can infer that the notification process is not limited to public sector issued eIDs and that Member States may also notify eIDs issued by the private sector (including, potentially, SNS-based identities) that they recognize to be used for access to their own public services. However, with that said, it is noteworthy that the exact role of the private sector in the new IAS model established in the Regulation is still uncertain and ambiguous. Although the draft proposal invites the private sector to build on 'notified' eIDs, the details regarding how that may be accomplished need to be better explained. And although the regulation seems to craft a mixed private-public sector model for the mutual recognition and acceptance of eIDs in the EU, it is not clear if private sector service providers only have the option to use national and notified identification schemes as the basis for their schemes, or if they may also render the eIDs they issue into official ones (by submitting them to the notification process). Regarding the latter option, private parties would be allowed to issue formal eIDs for cross-border use (which the respective governments would deem apt for the notification scheme). This possibility is not only controversial,[187] but also extremely unclear: how could a private sector company decide to apply to become an electronic identification identity provider issued by, on behalf or under the responsibility of the notifying Member State (rendering its eID an official one), falling then under the scope of the Regulation? In other words, and bearing in mind that the notification process is not limited to the public sector issued eIDs, can Member States also notify eIDs issued by the private sector that they recognize to be used for their own public sector services?

[186] The purpose of the recitals is to set out concise reasons for the chief provisions of the enacting terms in legislation, without reproducing or paraphrasing them.

[187] According to a recent study, this option should be discarded due to the risk of fragmentation: "Given the overall requirement by Member States to mutually recognise formal eIDs and the need to find common regulatory and operational principles to make the cross-border eAuthentication work, allowing private parties to issue formal eIDs would issue additional complexities and would hamper the mutual recognition process of eIDs and eAuthentication" (Ducastel et al., 2012, p. 50).

Part 4 – Facial Recognition, Privacy and Identity in Online Social Networks

4.1 Introduction

Marina walks into a bar. As she enters, a camera snaps her photograph and transmits the image to her preferred online social network (OSN). Through facial recognition she is identified and her physical presence recorded. The establishment registers her arrival. Luckily for Marina, today it has a promotion for its most loyal customers. The waitress greets Marina by name (they have never met before) and offers her a complimentary drink: a low-carb mojito — her favourite. Without her knowledge, at the same time a second camera takes another photo to infer Marina's age and sex, aggregating this information to the rest of the clientele's in order to provide a live score for those in the area. As it happens young women are currently over-represented in the bar. Based on this information, within half an hour a flock of young men arrive to chat up the ladies. People are enjoying themselves, snapping photos on their smart phones and uploading them to their favourite OSNs, which automatically tag those in the images. All of this happens through the power of biometrics and social connectivity.

Biometrics are technologies for the automatic recognition of a person based on some physiological or behavioral trait. OSNs are beginning to introduce these technologies as part of their platforms and services. Most notable is the case of the popular social networking site Facebook,[188] which is incorporating a facial recognition system that automates the tagging of photos uploaded by users. A separate app called Facedeals employs passive facial recognition to provide a "seamless method" for customers to announce their presence at restaurants, cafés, bars and other venues on Facebook — an event known as 'checking in'. And mobile phone-based OSNs, such as SceneTap, offer facial detection technologies to determine the average age and gender ratio of people at bars, in order to help bar-hoppers find the 'right' place to drink. These three examples represent a range of different consumer applications of biometrics in OSNs (i.e., photo tagging, checking in, and deciding where to socialize). In future these applications are likely to grow and expand to include other biometric modes such as iris recognition, keystroke dynamics recognition, and speech or voice recognition.

While biometrics have traditionally been used in security contexts (e.g., for law enforcement and immigration purposes or authentication systems for access control), the introduction of these technologies and techniques into social networking contexts is quite new. Facebook, for example, first introduced its facial recognition-facilitated "Photo Tag Suggestions" in December 2010. Yet the use of biometrics within OSNs is not uncontroversial. It is not just that biometrics have privacy and security implications – they certainly do (even their most ardent supporters admit this); it is also that the collection and processing of biometric data within OSNs may lead to novel privacy problems.

With these developments in mind, this deliverable provides an overview of the main social and legal implications of the use of biometric technologies in OSNs, focusing in particular on facial recognition technologies, and explores ways of governing the privacy implications associated with their use on these platforms. The focus on facial recognition is due to its power to de-anonymise a

[188] Facebook's photo collection contained around 100 billion photos as of mid 2011 and increases by 300 million photos per day. See Facebook Photo Trends [Infographic], Pixable (Feb. 14, 2011), http://blog.pixable.com//2011/02/14/facebook-photo-trends-infographic; According to Facebook, its users provide "more than 100 million tags" per day to that photo collection. See Justin Mitchell, Making Photo Tagging Easier, The Facebook Blog, Dec. 15, 2010: https://www.facebook.com/blog.php?post=467145887130

face (which cannot be easily hidden or altered) and to instantly connect it to one's online activities.[189]

4.2 Biometrics, privacy, and regulation in 'meatspace'

Whereas some authors argue that biometrics may be used to enhance the security of our digitally mediated interactions and transactions,[190] others fear what the future holds if and when their use becomes ubiquitous.[191] If in future people's identity must be invariably verified by biometric scans in order to be valid and accepted — if we are not ourselves without mechanical confirmation that our codified bodies match some previously recorded information — then repeated validation of our bodies will prompt to become an increasingly important activity in social life. In other words, our biometric identity will be perceived as our primary and single identity, while our bodily privacy will be increasingly threatened. This process will, on the one hand, further disclose identity information (due to the distinctive, unique nature of biometric data); while — on the other — it will reduce and limit one's identity expression. It is for this reason that several authors have examined the relationship between biometrics, identity, and privacy in meatspace (that is, the physical world as opposed to the virtual).

In 2001, Clarke[192] enumerated the privacy threats posed by biometric technologies, including privacy infringements *of the person* and of personal behaviour,[193] reduced opportunities for anonymity and pseudonymity, and dehumanization, among others. This potential risk of dehumanization is noteworthy insofar as the latest OSN applications of biometrics, like those described in the scenario in the introduction, are focused more on socialization and consumerism than on controlling people's access to places and services, which in some ways complicates the dehumanization argument. This is 'fun' surveillance.

Clarke further argued that the available potential safeguards (i.e., industry self-regulation, social impact assessments, data protection law, and biometrics-specific privacy legislation) would not sufficiently curtail these risks. He therefore called for a moratorium on the application of biometrics until a comprehensive set of design requirements and privacy protections were put in place. However, this moratorium never materialized, and considering the current state of biometric technologies across the globe (including their emerging applications in OSNs), we would be wise not to expect its arrival anytime soon.

4.3 Biometrics in cyberspace: the case of online social networks

The popularization of digital cameras, especially 'smart' mobile phones embedded with high-resolution cameras, has resulted in an enormous increase in the user-creation and publication of

---

189 Yana Welinder. A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks. *Harvard Journal of Law and Technology*, 26(1), 2012 (forthcoming).

190 Salil Prabhakar, Sharath Pankanti, and Anil K. Jain. Biometric Recognition: Security and Privacy Concerns. *IEEE Security & Privacy*, 1(2):33 – 42, March/April 2003.

191 Anonymous. In the Face of Danger: Facial Recognition and the Limits of Privacy Law. *Harvard Law Review,* 120(1870):1880 – 1891, 2007.

192 Roger Clarke. Biometrics and Privacy. Working Paper, Department of Computer Science, Australian National University, April 2001. Available at: http://www.rogerclarke.com/DV/Biometrics.html

193 For example, the Article 29 Working Party (comprised of representatives from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission, whose mission is to provide expert advice to Member States and to promote a common application of the Data Protection Directive) defines biometrics as "biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability. Biometric data changes irrevocably the relation between body and identity, because they make the characteristics of the human body 'machine-readable' and subject to further use".

digital images. For a while these were uploaded online to dedicated photo-sharing websites. More recently, however, users have begun sharing their photographs on OSNs. This turn is significant for several reasons. First, OSNs are more than just hosting sites — their value lies in the connections and interactions established between their users. Photos here tend to be praised for their personal value rather than artistic ones. They constitute the main means of users' self-presentation and identification within these social networks. Moreover, and as shown in a 2011 Eurobarometer poll, more than a third of European citizens access OSNs and more than half use websites to share pictures and other media content.[194] OSNs, in fact, are contributing to the further refinement of these technologies.

For one, the so-called social graph within OSNs (which describes the relationships between individuals of a network) potentially reduces the severity of false matches (traditionally a major problem for biometrics) by prioritizing candidates who happen to be in close proximity to the person uploading a photo. In other words, information from the social graph ("who is 'friends' with whom?") can help to limit the scope of the search and thus reduce the opportunity for false matches. This is a sea change in biometric identification.

A related issue involves the unintentional honing of the facial recognition algorithms being developed by OSNs by users through popular 'tagging' features. By correcting misidentifications on these networks, users gradually but steadily improve the underlying technology without realizing they are doing so.

In contrast with the application of facial recognition technologies in meatspace (e.g., security applications based on what are normally standalone systems) the use of these biometric technologies in the online world — namely their use by OSNs — not only enhances old privacy problems, it creates new ones. Related to the enhancement of traditional privacy problems is the issue of how the different contexts (i.e., public and private) for the use of biometrics like facial recognition are increasingly blurring (e.g., the combination and integration of data collected through OSNs and detection technologies for security purposes), and how this mix impacts on the regulation of these technologies. As examples of novel issues we have the meshing of personal data from different users in group photos (and the issue of separating one from the other — either in terms of data portability or data erasure), the ownership of the data (does it pertain to the person uploading the photo or to the person identified in the photo), the fact that the deletion of a photo does not necessarily delete the biometric data collected from that photo, or the complexity involved in explaining, through privacy policies, the mechanics and implications of facial recognition processes.

These novel issues introduced by the application of biometric technologies by OSNs call into question and challenge important aspects of the current regulatory framework. The following section examines the main problems and concerns that — from a regulatory perspective — arise from this situation.

4.4 Problems and concerns

The introduction of Facebook's facial recognition feature faced strong opposition from privacy advocates not only in Europe but also in the U.S. These technological developments have raised public concerns about automated identification and unwanted tracking. So much so that policy makers in the U.S. (i.e., the Federal Trade Commission) and EU (i.e., the Article 29 Data Protection Working Party, Irish Data Protection Commissioner, and Hamburg's Data Protection Authority) are monitoring these developments and publicly opining on the use of biometrics within OSNs.

Across the Atlantic, the Electronic Privacy Information Center (EPIC) filed in June 2011 a complaint with the U.S. Federal Trade Commission (FTC) over Facebook's biometric system, urging the FTC to

[194] Eurobarometer. Attitudes on Data Protection and Electronic Identity in the European Union, 2011.

determine whether the company had in fact engaged in unfair trade practices. This complaint also demanded the company to endow its users with meaningful control over their personal information. In Europe, some Data Protection Authorities (DPAs) strongly contested Facebook's initiative to use facial recognition software on uploaded photographs. This was the case of the Hamburg DPA, which argued that the use of such biometric technology enabled the social network to build and maintain an enormous database of its users' photos, along with their biometric data, without their prior consent, clearly breaching German privacy laws. The German regulator envisaged the possibility that one of the reasons behind Facebook's use of facial recognition software, in addition to improving users' online experience, was the unlimited retention of biometric data, which would be unlawful according to European data protection principles. Therefore, in November 2011 the Hamburg commissioner began an investigation of Facebook's facial recognition system, stating that "the social networking giant is illegally compiling a huge database of members' photos without their consent"[195] and repeatedly requesting the OSN to disable its facial recognition software and delete any previously stored data. In its last order the Hamburg authority "obliges the US-company [...] to make sure, that biometric profiles of its already registered users will only be created and stored with their active consent. Additionally, users have to be informed about risks of the practice in advance".[196] The aim of this decision seems, then, not to prevent the use of this technology, but "to give tools to the users which enable them to a conscious and active decision whether or not to participate in this technology". At the same time as the Hamburg decision, another important regulatory development was the publication of the second Audit Report ("Report of Re-Audit") by the Irish DPA on Facebook's implementation of audit recommendations.

As a consequence of the Hamburg commissioner's investigation, and as a follow-up to the new recommendations established in the Irish DPA's Re-Audit Report on Facebook,[197] together with the relevant Article 29 Working Party opinions, the facial recognition feature has been turned off in the EU for new users and templates for existing users were (supposedly) deleted in October 2012. Facebook's commitment to honor best practices in data protection compliance is a positive signal from the OSN; however, it leaves some issues unresolved, as discussed below.

Focusing on the use of facial recognition technologies by OSNs, and looking in particular to Facebook's Photo Tag Suggest feature as a case study, this section analyses several privacy and security concerns that arise from the use of biometrics in OSNs.

4.4.1 Consent

Facebook's regulatory problems relating to its biometrics software are based, to a certain extent, on the fact that, until recently, its facial recognition system integrated an *automatic* tagging feature that did not take into account the consent of the people subject to these identification means. In effect, this feature – which processes biometric data (a sensitive category under EU Data Protection) – was *active by default* on users' accounts. Data subjects could only deactivate the automated biometric recognition by (actively) opting out from it, and only after realizing that they had been tagged in a given photograph.

---

[195] Kevin J. O'Brien. Germans Re-open Investigation on Facebook Privacy. *New York Times*, 15 August 2012. Available at: http://www.nytimes.com/2012/08/16/technology/germans-reopen-facebook-privacy-inquiry.html

[196] See the press release on the Hamburg authority's administrative order against Facebook, 21 September 2012: http://www.datenschutz-hamburg.de/uploads/media/PressRelease-2012-09-21-Facebook_AdministrativeDecision.pdf. The investigation started in this state due to the fact that Facebook's German office is in Hamburg (Germany has a federal system of several data protection authorities, at the federal and Länder (i.e., state) levels).

[197] Two audits of Facebook Ireland have been conducted by the Irish Data Protection Commissioner, aimed at providing 'best practice' recommendations, with the last being published in Sept. 2012: http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf

The opt-out system originally adopted by Facebook indicates that users have not been asked to express their previous consent to data processing, but that they can decide to withdraw it afterwards. In theory, this is not necessarily in contradiction with European data protection principles, but as recently stated by the Article 29 Working Party, consent obtained from the mere passiveness or silence of individuals has an intrinsic ambiguity and fails to demonstrate the actual will of the data subject. Facial recognition activated by default should thus be resisted and consent should be positively expressed, and not inferred from privacy settings that allow users to opt out of the collection and use of biometric data. This is in line with what the Council of Europe has stated: "The use of techniques that may have a significant impact on users' privacy – where for instance processing involves sensitive or biometric data (such as facial recognition) – requires enhanced protection and should not be activated by default".[198]

Moreover, facial recognition technology also provides increasingly reliable technological means of identifying and tracking people who have chosen not to participate as users of the network (i.e. non-registered members of OSNs), but who are nevertheless subject to these identification technologies. For example, when an OSN member uploads multiple photos of a friend who does not have a profile on the site, the facial recognition system may nonetheless generate a biometric profile for this person. One challenge in this respect is how OSNs can ensure, both legally and technically, that biometric profiles of non-registered people are not created or maintained.

In a nutshell, the use of automated facial recognition techniques on OSNs complicates the data protection principle of consent (i.e., that the processing of photos for biometric purposes is based on free, informed, and active consent of concerned users and that biometric templates created without proper consent must be deleted). Opt-out consent for facial recognition features is not acceptable, partly because users would likely simply not understand what they accept by default, as it would be presented in terms of trust vis-à-vis friends, not vis-à-vis the social network. The mere retention of a huge database of this special category of data (i.e., biometrics) by a social network and without users' consent may increase the risks of unwanted recognition.

4.4.2 Transparency

The importance of providing transparent, easily accessible, and understandable information to data subjects regarding the protection of their personal data and privacy has led the European Commission to establish a specific transparency principle[199] as a new element of the General Data Protection Regulation (Article 5). The framing of this principle could not have come at a better time. In fact, the use of facial recognition technology by OSNs generates novel transparency issues that go clearly beyond traditional privacy concerns. In this way, the use of facial recognition creates (or should create) a set of additional obligations on the side of OSNs — as data controllers — to explicitly inform data subjects of the legitimate interests pursued with the processing of personal (biometric) data.

Informational transparency requirements should make users aware of the difference between a photo as a visible item and the biometric data, which is not visible to a human eye, which can be

[198] See Recommendation CM/Rec (2012) 4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services, Council of Europe, Apr. 4, 2012. Available at: https://wcd.coe.int/ViewDoc.jsp?id=1929453

[199] As explained in recital 46: "The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose."

used to identify the user in other photos.[200] In this respect, users should be made aware of the consequences and the implications of uploading photos, namely of the underlying and automatically identifying biometric (and other personal) data that can be extracted or inferred from these photos, and the transmission of such identifying information to third parties (that escape users' control and privacy expectations), and which in turn can identify users in other contexts without their knowledge and consent.

The privacy risks that the processing of biometric data may generate, and which will only tend to become more serious with its combination with other technological trends such as cloud computing, ubiquitous computing, data mining, and big data, requires data controllers to comply with an extra set of information obligations and transparency requirements vis-à-vis data subjects. More has to be done than merely allowing users to specifically opt out of being automatically identified in photos.[201] More has to be done than allowing users to restrict access to their photos to certain groups through privacy settings.[202] More has to be done than simply notifying the user that he/she has been tagged and that the data subject can 'un-tag' oneself. The notification that a given user has been identified (i.e., tagged in a photo – either by another user or through the Photo Tag Suggest, which employs face recognition technology and previously tagged photos to identify individuals in new photos) and the possibility for users to un-tag themselves constitutes, in this light, a procedural remedy or tool that only partially protects (or restores) one's privacy. The fact that a data subject can un-tag him or herself from a photo does not ensure that the processing of biometric data ceases to be performed by the OSN. Tagging and un-tagging are features built for users (allowing them to identify or de-identify themselves) which, even if de-activated, do not necessarily prevent the facial recognition system to keep working in the background. One thing is what happens at the users' layer (managing, for example, who can have access to the photos), another thing is what occurs at the internal level, that is, what and how social networks collect, store and use personally identifiable information about these users. Moreover, by the time the user un-tags himself (or opts out from the collection and use of biometric data) there is no guarantee that the facial recognition process has not already occurred in the first place and that such data has not already been collected and potentially used to identify the user in new photos. In addition, the extent to which users can effectively deactivate the automated biometric identification is not entirely clear and, thus, transparent. One may question if the technical process of biometric interpretation of the photos is running in the background regardless of the opinion of the persons appearing on the photo, and for purposes that the users may not be aware of. The provision of this information to the user is essential for the attainment of a consequential and operational transparency principle, as well as for the clarification of the scope of the consent and the actual meaning of an opt-out choice.

The lack of transparency regarding the means and purposes to which the processing of biometric data may be further used for (such as for behavioural advertising) only increases the control over users' personal information by data controllers. In addition, the fact that – in the context of OSNs – users may fall under the ambit of data protection as data controllers (or co-controllers – for posting

[200] As Welinder (2012) argues, "Facebook cannot [i.e., should not be allowed to] extract biometric data from a persons' face even if the person shows that face in public". See also: Nancy Yue Liu. Bio-Privacy: Privacy Regulations and the Challenge of Biometrics. Routledge, p. 177, 2012: "While there may be no expectation of privacy in public places, there may still be an expectation of anonymity".

[201] Following Facebook's Data Use Policy, unless a user specifically opts out of being automatically identified in photos, Facebook uses tagged photos of that user as training images to identify the user in newly uploaded photos. See: https://www.facebook.com/about/privacy/your-info#inforeceived

[202] In effect, if a user restricts access to a photo so that it is only visible to his or her family, Facebook may nevertheless extract biometric data from it and use it with Photo Tag Suggest to allow his or her other Facebook friends to identify them in new photos (Welinder, 2012)

photos that will then be potentially used for automated biometric identification)[203] only further complicates this question, as OSN users should not be burdened with transparency obligations that exceed their personal, technical, and financial capabilities. Compliance with the transparency principle requires that social networks provide users with thorough and comprehensible information about how it collects, stores, processes, and shares users' biometrics. Given the complexity of the information to be explained, the provision of clear and comprehensible information about biometric data collection and processing could (and should) be done through other means in addition to the long and 'legalese' privacy policies that users hardly ever read. Examples of good practices that could be further explored and applied to information obligations and transparency requirements can be found in the field of infographics (graphs and charts), non-linguistic or 'visceral' notices, and demonstration videos.

4.4.3. Further uses of biometric data on OSNs

Once OSNs have built up extensive databases of facial images and have honed their algorithms through the active participation of their communities, there is a risk that these systems will be used for previously unspecified or unanticipated purposes. This raises the question of other potential purposes (both positive and negative) for which biometric data can be used. An OSN may want to use this data, for example, to improve their advertising or marketing efforts by deriving new insights about their users (e.g., 'this user spends a lot of time with Asians and may be interesting in the following products').

Law enforcement authorities may seek to access these systems during an investigation. For example, the police may work with companies to process facial images captured from video surveillance footage against an OSN's facial recognition database. Such requests ought to be regulated.

4.4.4. Profiling and discrimination risks

Facial recognition systems deployed by OSNs may be perfectly linked to current or future profiling techniques. It is on the basis of profiles that many decisions regarding users are taken. Moreover, some of these decisions can have very important impacts on the lives of the users, such as allowing or denying them access to a service or product, recruiting or rejecting someone for a job, granting more or less expensive insurance scheme, and so forth. As these examples demonstrate, one risk that profiling raises, and especially so with its alliance with facial recognition systems, is the possibility to misrepresent or discriminate the individual being profiled. Another serious risk is the one of misidentification caused by the inaccuracy of the automatic identification, which also has the potential for human error as it employs tags previously generated by Facebook users. There are important social and financial costs associated with these kinds of misidentifications.

4.5 Possible solutions

The possible set of regulatory responses to the problems and concerns arising from the use of biometric technologies by OSNs should take into account not only the strengthening of the existing legal framework for privacy and data protection, together with its core values, but also the use of new technologies and business models that empower users vis-à-vis control over their own data. This section briefly examines a range of possible responses to the problems posed by biometrics by dividing them into three categories: legal, technological, and business model responses.

4.5.1. Legal responses

4.5.1.1 Strengthening the Principle of Consent

One of the main problems that emerges with the use of biometrics by OSNs is the lack of user consent to the collection of this type of data. As a consequence, one of the urgent legal responses

[203] Natali Helberger and Joris Van Hoboken. Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers. *Computer Law International (CRi)*, 4:101 – 109, 2010.

that needs to be taken is to strengthen the principle of consent. In its 'opinion on facial recognition in online and mobile services', the Article 29 Working Party stresses that in the context of facial recognition technologies, consent for enrolment cannot be derived from the user's general acceptance of the overall terms and conditions of the underlying service: "Users should be explicitly provided with the opportunity to provide their consent for this feature either during registration or at a later date".[204] Therefore, not clicking (i.e., remaining passive) may (or even should) not be considered as *unambiguously consenting* to data processing, at least not according to the current European legislation, namely Article 7 of the Data Protection Directive. In fact, by strengthening consent mechanisms, OSNs should ask for prior consent and to inform users about changes in the default settings.

Referring specifically the case of facial recognition, the Working Party has noted that:

> "Registered users [of an OSN] must also have been given a further option as to whether or not they consent to their reference template to be enrolled into the identification database. Non-registered and registered users who have not consented to the processing will therefore not have their name automatically suggested for a tag [...]"

4.5.1.2 Enhancing access rights

It is currently unclear whether OSNs allow users to access the biometric information they store, including a user's biometric template or any biometric codes assigned to a person's profile. In Europe, Subject Access Requests permit citizens to request any and all personal data that an organization possesses, which in theory would include biometric data. However, there are currently limitations to how this kind of data can be reproduced and visualized to present to user who have requested access. In addition, providing this information to non-registered users would present considerable challenges. Despite these difficulties, further research should explore how to enhance data subjects' access to their biometric data held by OSNs.

4.5.1.3 A right to be forgotten

The right to be forgotten – that is, the right of individuals to no longer have their data processed and for it to be deleted when it is no longer needed for legitimate purposes – is currently being considered in Europe.

One can observe a movement towards rendering the right to be forgotten an explicit legal provision within the Europe's general data protection framework. This right, in fact, already exists – although implicitly. According to the current European Data Protection Directive, the subject can withdraw his or her consent to the storage of personal data. This is so unless there is a legitimate reason (i.e., a public interest exception like free speech) to keep the data stored. It is understood that the burden of proof of this legitimate reason should lie on the data controller. With the recent EU proposal for a General Data Protection Regulation, the right to be forgotten is now explicitly enshrined in the text of the Regulation, namely in its Article 17.

This right can thus play an important role in mitigating the concerns that the increase of biometric data and its use by OSNs will certainly pose. In following such legal provision, OSNs would have to remove the data from its site upon request. This rule is particularly important concerning the storage of biometric data.

It was revealed during the Irish DPA's audit of Facebook Ireland, through a code review, that the facial recognition signature generated for users is now deleted when a user disables the Photo Tag Suggest feature. This is a positive development. However, there are several things that remain unclear. By deleting a photo does a user delete the biometric data generated from that photo? How can we guarantee that facial recognition techniques, used by third parties (e.g., search engines), are incapable of performing facial recognition on publicly available images within OSNs in which a user

[204] Article 29 Working Party. Opinion on Facial Recognition in Online and Mobile Services, 2012.

has previously deactivated facial recognition? In other words, how can the user be sure that his or her photograph will not be used or recognized by other entities that have previously accessed his or her OSN profile? Moreover, it is still not clear whether other OSNs will adopt the same best practices (that, in the case of Facebook, were reached after a compliant was lodged).

4.5.2 Technological responses

A right to delete has also been addressed from an enforceability point of view. Some are now arguing in favour of embedding this right in the design principles of technology, enabling its automatic application in a sort of forgetting by default and oblivion by design. In this sense, researchers have proposed attaching expiry dates to personal data, which would then be automatically deleted after a certain period of time and without any necessary action from the data subject. Based upon such a technologically-embedded solution, one could thus mitigate the privacy concerns that emerge with the biometric identification of OSNs' users, and their automatic tagging in photos spread throughout the network, by attaching expiry dates to those very same photos, enabling their automatic deletion after a certain period of time.

Another technological response would consist in incentivizing the sharing of photos with one's friends through a distributed social network, preventing thus a centralized social network from extracting biometric data. For users of centralized OSNs the technical solution is to devise a way of uploading photos that prevents the collection of biometric data.

There are also techniques – both user-led and system-generated – for blurring or pixelating faces in a photo in such a way as to avoid automatic face recognition (and the extraction of biometric data), while still allowing humans to recognize the persons featured in a photograph. Yet there are no guarantees that this process of image manipulation cannot be spotted or reversed, so this potential technical measure merits further research (specifically in computer science).

4.5.3 Business model solutions

Today we live in an economy in which data is said to be the "new oil". Business models, particularly those based on advertising, build upon and incentivize the collection of more and more personal data, analyzing it afterwards in order to allow companies to offer tailor-made products and services to their customers. Moreover, there are companies specialized in collecting data on users' behaviour, especially through cookies and other tracking mechanisms, and selling their data without their consent. Nevertheless, this current panorama seems to be changing as new business models are emerging that allow individuals to more effectively control their data (i.e., to decide who can access their personal information) and to even profit from this access.

A market for personal data management tools is thus emerging through different start-ups, which work as data lockers (a sort of safe-deposit box for data) that allow users to store and manage their digital information and assets (e.g., financial information, photos, medical records, music, and so forth). The idea is that companies would then pay to access this data as it would allow them to offer personalized products and services. Supporters of data lockers believe that these systems will solve privacy concerns and, moreover, they will allow people to share more data as there would be a market to benefit from. Leveraging this new business model, user's facial recognition data would thus be kept in these digital data vaults and exchanged, under the control of the individual, forming a possible response to some of the concerns raised by the use of biometrics by OSNs. Users would thus be empowered to negotiate their own data use terms when sharing photos in social networks. A social network, implementing this business model, would allow users to decide for instance when they want to give out their personal information to advertisers in exchange for discount, for example.

However, it is still to be seen whether these data lockers could guarantee the tight control of user data as they promise, and whether the unauthorized biometric interpretation of photographs by

advertising companies or other third-parties could be prevented. The issue of shared assets that become the content of these data-lockers (e.g., contacts details or photographs with several people) may also be problematic: would only fragments of these information/images be stored in lockers? Should the others appearing in the same image provide previous consent? Who would benefit (i.e., earn money) from them? How would one safely withdraw from the lockers?

These and other questions should be carefully addressed as a centralized system of data storage (especially of biometric data) could be, if breach, highly risky for individual privacy.

An alternative would be the 'pay or play' model in which users are permitted to subsidize their OSNs by paying them to avoid the collection of their biometric data and to negotiate their own data use terms when sharing photos in social networks. As Welinder has noted, this would also indicate to social networks when certain data usage – e.g., biometrics – is unwelcome, because many users would pay to avoid it and the OSN may ultimately remove the facial recognition feature because it would not have sufficient biometrics to keep it running. Nevertheless, an important side effect of this model is that it would force individuals that cannot afford it to sacrifice their privacy.

However, these market-based solutions, as Welinder points out, should be thought as possible solutions only in combination with legal (i.e., opt-in consent and notice) and architectural ones (i.e., the design of the OSN) in order to protect social network users from unwanted collection of facial recognition and other biometric data.

Conclusions

In the first part of this deliverable we explored the difficulties, barriers and challenges in implementing a regulatory framework for a pan-European electronic identity, before suggesting a conceptual framework of principles to address these challenges and overcome the obstacles.

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"[205] within the envisaged digital single market, as business and citizens still need to deal with 27 different legal systems for the same transaction. As this deliverable 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 the unique identifiers used in their administrations to additional protection mechanisms.[206]

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 deliverable, contributing to the discussion on the need for a shared eID legal framework for 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.

The principles listed in this deliverable 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 launch 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.

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 deliverable aims to orient and contribute to this endeavour.

In the second part of this deliverable we presented the results of our analysis on emerging behaviour and attitudes of the youngest users of digital technologies, as regards privacy and identity, from which we draw our policy and legal considerations.

As the Art 29 Working Party has confirmed, despite the emergence of new technologies and the galloping pace of the globalization trend, the main principles of data protection are still valid and applicable. According to the WP, "the level of data protection in the EU can benefit from a better

[205] Commission, "Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth," 19.

[206] Graux, Majava, and Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 115. Member States have also implicitly introduced in their legislation the already alluded authentic source principle.

application of the existing data protection principles in practice".[207] This assertion is, nevertheless, limited. It looks at the objective factors of technology development and not to the subjective factors of perception, habit, preference and understanding of the users of these new technologies.[208] Hence, future revisions of the data protection legal framework should not only be promoted taking into account new technological developments, but also – and mainly – the new data subjects[209] and their behaviour.

We thus argue that future revisions of DPD legal framework (namely their corresponding IA exercises) should also take into account the image of the emerging DN, recommending a higher degree of flexibility in the application of its rules. This will allow legal systems to become closer to the legal subjects and to be more effective in the application of its rules.

The approach to EU law making processes advocated in this deliverable is an inherently prospective one. In this respect, the law should bear in mind that DN will have grown up in a couple of years and that they should, as such, not only be shaped by what the law says but also influence how the law should be. Law-makers should thus learn to look at the future, to foresee and to anticipate the needs and the changing perceptions of those who are DN of today and adult citizens of tomorrow. In effect, the current framework should strive not only to adapt itself but also to anticipate both forthcoming technological landscape and their future users.

In his attempt to devise an empirical measurement of law-system quality, Schmidt observes that the "quality of a law system is not only related to its success in fulfilling the requirements of the design (...), it is also related to its capacity to attract people, (...) to generate willingness to participate.[210] Nevertheless, the reality of data protection regulation is progressively striding away from the reality of its addressees, namely from the digital natives and their current perceptions and practices of privacy. This deliverable aims to call the attention to this fact and to the need to bridge the legal reality with the social one.

In the third part of this deliverable we have attempted to frame the debate regarding public sector use of SNS-based eIDs in the EU. To this end we reviewed the pros and cons associated with the use of SNS for government IdM. As it stands, SNS are probably currently only capable of serving as an eID channel or interface for limited kinds of online public service provision: low-risk, low-value, and non-sensitive transactions. Advanced transactions will require SNS to ensure much more reliable profile data or to check it against official data sources, which is no easy task. Policies encouraging public sector use of SNS-based identities must remain platform-neutral and should not force citizens to register with commercial providers against their will. And moreover, to prevent the misuse of these eIDs, platform providers must build in additional security and privacy protections, which should also be accounted for in regulation. As regards eID regulation in Europe, we claim that future legislation needs to be more ambitious, to consider technological progress and new business models for identity provision. As currently drafted, the proposed Electronic Trust Services Regulation does not adequately account for public sector use of SNS-based eIDs. This is a missed opportunity.

The debated recent use of facial recognition in OSNs, that enables the processing and exchange of personal information on an unprecedented scale, has been explored in the last part of this

---

[207] Article 29 Working Party, "The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", 2009a. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

[208] It is obvious that perception – as a subjective factor – is inexorably influenced and shaped by the technological environment – objective factor – surrounding them.

[209] "Not only technology has changed over the past 30 years: the individuals using it have changed too", Omer Tene, "Pivacy: The New Generations", *International Data Privacy Law* 1 (2011).

[210] SCHMIDT, A. 2009. Radbruch in Cyberspace: About Law-System Quality and ICT Innovation. *Masaryk University Journal of Law and Technology,* 3.

deliverable. As discussed in this deliverable, novel and complex privacy problems emerge with the rise of biometric recognition in these networks. It is important to note that Europe's proposed solutions to these issues go beyond the old continent's frontiers. Recently it has been observed that when Europe moves to regulate privacy more strictly, Internet users outside of the EU indirectly benefit from these measures. When regulators in Germany, for example, insist that Facebook implement a privacy-enhancing measure or otherwise face a ban, netizens in California will also be affected when the OSN complies. The point is that the ongoing developments in Europe concerning the future regulation of the use of facial recognition within OSNs, like Facebook, will impact everyone on the networks. Not just Europeans. We eagerly await the outcome.

Annex 1 – Terminology

This annex provides a general overview of the most relevant concepts, terms and notions regarding electronic identity (eID) and electronic identity management systems (IDM). It lays down the terminological grounds on which the legal analysis provided in this deliverable 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 endeavour, 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).[211] The notion of "**attribut**e" 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 or entire identity,[212] that is, without identifying him/her in absolute terms).[213]

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."[214] Two classes of identifiers can be distinguished: 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 off-line world, claims that an individual is a 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.

---

[211] In order to distinguish the concept of exact identity from the one of partial identity, I shall also use the term "full identity."

[212] The distinction between full and partial identity we 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 Andreas Pfitzmann and Marit Hansen, "A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Version V0.34)," (2010), 31. While for these authors, partial identities may encompass attributes through which a person can be identified; we 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.

[213] As we shall see further on, this specific characteristic of the processing of eIDs enables the use of multiple identities by the same individual.

[214] Hans Graux, Jarkko Majava, and Eric Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," (2009), 113. 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, Majava, and Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 113.

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."[215] 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 systems** (IDMs). The overall objective of eIDM systems is to associate information with people, enabling transactions between different parties in an eco-system 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 organisation's policies."[216] On the administrators' side, identity management 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 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: **identification** and **authentication**.

While the purpose of identification is to "link a stream of data with a person,"[217] 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."[218] 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.).[219] 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."[220] 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,

---

[215] Ronald Leenes, Jan Schallaböck, and Marit Hansen, "Prime (Privacy and Identity Management for Europe) White Paper," (2008), 8.

[216] Ibid., 1.

[217] Thomas Myhr, "Legal and Organizational Challenges and Solutions for Achieving a Pan-European Electronic Id Solution: Or I Am 621216-1318, but I Am Also 161262-43774. Do You Know Who I Am?," *Information Security Technical Report* 13, no. 2 (2008): 77.

[218] Graux, Majava, and Meyvis, "Eid Interoperability for Pegs - Update of Country Profiles - Analysis & Assessment Report," 113.

[219] Ibid. As we shall see, it is based on this type of authentication that I will argue in favour of a principle of multiple identities.

[220] Ibid.

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.[221] Examples of digital credentials include: an electronic signature, a password, a verified bank card number, a digital certificate, or a biometric template.[222] 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)."[223]

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".[224] 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."[225] 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."[226]

---

[221] OECD, "Oecd Recommendation on Electronic Authentication and Oecd Guidance for Electronic Authentication," (2007), 12.

[222] ———, "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers," (2009), 6.

[223] Leenes et al., "Stork - Towards Pan-European Recognition of Electronic Ids (Eids) - D2.2 - Report on Legal Interoperability," 25-26.

[224] Myhr, "Legal and Organizational Challenges and Solutions for Achieving a Pan-European Electronic Id Solution: Or I Am 621216-1318, but I Am Also 161262-43774. Do You Know Who I Am?," 77.

[225] Ibid.

[226] Ronald Leenes et al., "Stork - Towards Pan-European Recognition of Electronic Ids (Eids) - D2.2 - Report on Legal Interoperability," (2009), p.15. 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., "Stork - Towards Pan-European Recognition of Electronic Ids (Eids) - D2.2 - Report on Legal Interoperability," 16.

To conclude, and in line with previously mentioned proposals for an eID terminology,[227] the term eIdentity is used in this deliverable 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[228] (such as passwords or biometrics[229]). 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 identity management systems, and that are then recognized by public and private entities (such as national governments and private companies).[230]

[227] 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, "A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Version V0.34)."

[228] OECD, "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers," 6.

[229] "Biometrics are measurable biological and behavioural characteristics and can be used for strong online authentication. A number of types of biometrics can be digitised 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" Ibid., 7.

[230] 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 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., "Stork - Towards Pan-European Recognition of Electronic Ids (Eids) - D2.2 - Report on Legal Interoperability," 16.

References

2030, Reflection group on the Future of the EU. "Project Europe 2030. Challenges and Opportunities - a Report to the European Council by the Reflection Group on the Future of the Eu 2030." 2010.

Aichholzer, G., & Strauß, S. (2010). Electronic identity management in e-Government 2.0: Exploring a system innovation exemplified by Austria. *Information Polity*, 15(2010), 139–152.

Ala-Mutka, K., Broster, D., Cachia, R., Centeno, C., Feijóo, C., Haché, A., Kluzer, S., Lindmark, S., Lusoli, W., Misuraca, G., Pascu, C., Punie, Y., & Valverde, J. A. (2009). *The Impact of Social Computing on the EU Information Society and Economy*. European Commission, Joint Research Centre, Institute for Prospective Technological Studies.

Andrade, Norberto N. G. de. "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights." In *Privacy and Identity Management for Life: 6th Ifip Wg 9.2, 9.6/11.7, 11.4, 11.6/Primelife International Summer School, Helsingborg, Sweden, August 2-6, 2010, Revised Selected Papers*, edited by S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes and G. Zhang, 90-107. Berlin ; Heidelberg: Springer, 2011.

———. "The Right to Privacy and the Right to Identity in the Age of Ubiquitous Computing: Friends or Foes? A Proposal Towards a Legal Articulation." In *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, edited by C. Akrivopoulou and A. Psygkas, 19 – 43. Hershey, PA: Information Science Publishing, 2011.

Andrade, Norberto N. G. de. (2012a). Towards a European eID regulatory framework. Challenges in constructing a legal framework for the protection and management of electronic identities. In S. Gutwirth, P. De Hert, R. Leenes, & Y. Poullet (Eds.). *European Data Protection: In Good Health?* (pp. 285-314). Dordrecht, Netherlands: Springer.

Andrade, Norberto N. G. de. (2012b). Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID. *Computer Law & Security Review*, 28(2), 153-162.

BBC News. (2012, August 2). Facebook has more than 83 million illegitimate accounts. *British Broadcasting Corporation*. Retrieved from http://www.bbc.com/news/technology-19093078

Boyd, D., & Ellison, N.B. (2008). Social Networking Sites: Definition, History and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210-230.

Commission, European. "Delivering an Area of Freedom, Security and Justice for Europe's Citizens: Action Plan Implementing the Stockholm Programme." Brussels, 2010.

———."A Digital Agenda for Europe." 2010.

———."Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth." Brussels, 2010.

———."First Report on the Implementation of the Data Protection Directive (95/46/Ec)." Brussels, 2003.

———. "A Roadmap for a Pan-European Eidm Framework by 2010 - V.1.0." 2007.

———. "Signposts Towards Egovernment 2010." 2005.

———. "Towards Interoperability for European Public Services." 2010.

Craig, Paul. "The Treaty of Lisbon, Process, Architecture and Substance." *European Law Review* 33, no. 2 (2008): 137-66.

Ducastel, N., Fisher, R., Gehrt, D., Hooghiemstra, T., Remotti, L. A., van Schoonhoven, B., van den Broek, T., & van Paassen, R. (2012). *Study on impact assessment for legislation on mutual recognition and acceptance of e-Identification and e-Authentication across borders SMART 2011/0075 IAV.*

Dumortier, Jos. "Legal Considerations with Regard to Privacy Protection and Identity Management in the Information Society." *112e rapport annuel, Hochschüle für Technik und Architektur Biel, Tilt*, no. 15 (2003): 66-69.

The Economist. (2012, July 22). Facebook population: Status update. *The Economist*. Retrieved from http://www.economist.com/node/16660401

European Commission. "A Comprehensive Approach on Personal Data Protection in the European Union." In *European Commission*. Brussels, 2010.

Farivar, C. (2012, July 18). Washington State will enable voter registration via Facebook. *Ars Technica*. Retrieved from http://arstechnica.com/business/2012/07/washington-residents-to-be-able-to-register-to-vote-via-facebook

Gillespie, T. (2010). The Politics of 'Platforms'. *New Media & Society*, 12(3), 347-364.

Graux, H., Majava, J., & Meyvis, E. (2009). *eID Interoperability for PEGS: Update of Country Profiles - Analysis & Assessment Report*. IDABC Programme of the European Commission.

Hoeksma, J. (2010, November 25). NHS Choices allowing Facebook tracking. *E-health Insider*. Retrieved from http://www.ehi.co.uk/news/ehi/6454

Jones, Andy, and T. Martin. "Digital Forensics and the Issues of Identity " *Information Security Technical Report* (2010): 1-5.

Kaplan, A.M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizon*, 53(1), 59-68.

Kubicek, H., & Noack, T. (2010). The path dependency of national electronic identities. A comparison of innovation processes in four European countries. *Identity In The Information Society*, 3(1), 111-153.

Lee, D. (2012, October 5). Facebook surpasses one billion users as it tempts new markets. *BBC News*. Retrieved from http://www.bbc.co.uk/news/technology-19816709

Leenes, R., Priem, B., van de Wiel, C., Owczynik, K. (2009). *Towards Pan-European Recognition of Electronic IDs – Deliverable 2.2 – Report on Legal Interoperability*. STORK Project.

Leenes, Ronald , Jan Schallaböck, and Marit Hansen. "Prime (Privacy and Identity Management for Europe) White Paper." 2008.

Lusoli, W., Bacigalupo, M., Lupiañez, F., Andrade, N., Monteleone, S., & Maghiros, I. (2012). *Pan-European Survey of Practices, Attitudes & Policy Preferences as regards Personal Identity Data Management*, European Commission, Joint Research Centre, Institute for Prospective Technological Studies.

Martin, A. K., & Bonina, C. M. (2013). Open Government and Citizen Identities. In M. L. Smith & K. Reilly (Eds.). Open Development: Technological, Organizational, and Social Innovation in International Development. MIT Press.

Mitchell, J. (2012, January 2). The Verified Twitter Account for Rupert Murdoch's Wife Was Fake. *Read Write Web*. Retrieved from http://www.readwriteweb.com/archives/the_verified_twitter_account_for_rupert_murdochs_w.php

Modinis-IDM-Consortium. "Modinis Study on Identity Management in Egovernment, Identity Management Issue Interim Report Ii1." 2006.

———. "Modinis Study on Identity Management in Egovernment. Common Terminological Framework for Interoperable Electronic Identity Management - Consultation Paper V.2.01." 2005.

Myhr, Thomas. "Legal and Organizational Challenges and Solutions for Achieving a Pan-European Electronic Id Solution or I Am 621216-1318, but I Am Also 161262-43774. Do You Know Who I Am?" *Information Security Technical report* 13, no. 2 (2008): 76-82.

———. "Legal and Organizational Challenges and Solutions for Achieving a Pan-European Electronic Id Solution: Or I Am 621216-1318, but I Am Also 161262-43774. Do You Know Who I Am?" *Information Security Technical Report* 13, no. 2 (2008): 76-82.

Nabeth, Thierry. "Identity of Identity." In *The Future of Identity in the Information Society : Challenges and Opportunities*, edited by Kai Rannenberg, Denis Royer and André Deuker, 19-69. Berlin ; London: Springer, 2009.

OECD. "Oecd Recommendation on Electronic Authentication and Oecd Guidance for Electronic Authentication." 2007.

———. "The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers." 2009.

Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization " *University of Colorado Law Legal Studies Research Paper No. 09-12* (2009).

Party, Article 29 Data Protection Working. "Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware." 1999.

Pfitzmann, Andreas, and Marit Hansen. "A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Version V0.34)." (2010).

Poullet, Yves. "About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?" In *Data Protection in a Profiled World*, edited by S. Gutwirth, Y. Poullet and P. de Hert, 3-30. Dordrecht: Springer Science+Business Media B.V, 2010.

Protalinski, E. (2012, March 28). 10.5 billion minutes spent on Facebook daily, excluding mobile. *ZDNet*. Retrieved from http://www.zdnet.com/blog/facebook/10-5-billion-minutes-spent-on-facebook-daily-excluding-mobile/11034

Rundle, Mary. "International Personal Data Protection and Digital Identity Management Tools " *Berkman Center Research Publication No. 2006-06* (2006).

Sassaman, L. (2012, December 10). TSA and Social Media: Being Blocked From TSA Twitter Stream. Retrieved from http://iwilloptout.org/2010/12/10/tsa-and-social-media-being-blocked-from-tsa-twitter-stream

Schoemaker, R. (2012, May 2). Advies: integreer DigiD met Facebook. *Webwereld*. Retrieved from http://webwereld.nl/nieuws/110366/advies--integreer-diågid-met-facebook.html

Smedinghoff, Thomas J., and David A. Wheeler. "Addressing the Legal Challenges of Federated Identity Management." *Privacy & Security Law Report* (2008).

Stevens, T. (2012, March 30). The Great Liability Sinkhole. *The Data Trust Blog*. Retrieved from http://www.computerweekly.com/blogs/the-data-trust-blog/2012/03/the-great-liability-sinkhole.html

Thierer, A. (2012). The Perils of Classifying Social Media Platforms as Public Utilities. Mercatus Center at GMU Working Paper No. 12-11, March.

United Nations. (2012). *United Nations E-Government Survey 2012: E-Government for the People.* United Nations.

Valentino-DeVries, J. (2011, September 2011). Facebook Defends Getting Data From Logged-Out Users. *WSJ Digits*. Retrieved from http://blogs.wsj.com/digits/2011/09/26/facebook-defends-getting-data-from-logged-out-users

van Rooy, Dirk, and Jacques Bus. "Trust and Privacy in the Future Internet – a Research Perspective." *IDIS - Identity in the Information Society* 3, no. 2 (2010): 397-404.

European Commission
EUR 25834 – Joint Research Centre – Institute for Prospective Technological Studies

Title: Electronic Identity in Europe: Legal Challenges and Future Perspectives (e-ID 2020)

Authors: Norberto Nuno Gomes de Andrade, Shara Monteleone, Aaron Martin

Luxembourg: Publications Office of the European Union

2013- 81 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424 (online)

ISBN 978-92-79-28778-7 (pdf)

doi:10.2791/78739

Abstract
This deliverable presents the work developed by the IPTS eID Team in 2012 on the large-encompassing topic of electronic identity. It is structured in four different parts: 1) eID: Relevance, Le-gal State-of-the-Art and Future Perspectives; 2) Digital Natives and the Analysis of the Emerging Behavioral Trends Regarding Privacy, Identity and Their Legal Implications; 3) The "prospective" use of social networking services for government eID in Europe; and 4) Facial Recognition, Privacy and Identity in Online Social Networks.

LF-NA-25834-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

Publications Office

ISBN 978-92-79-28778-7