White Paper on the Regulatory and Legal Aspects of Electronic Identity

HOIKKAHNEN, A.; Poullet, Yves

Publication date:
2009

Document Version
Publisher's PDF, also known as Version of record

EUROPEAN COMMISSION
JOINT RESEARCH CENTRE

Institute for Prospective Technological Studies
Information Society Unit

First draft
14/07/2009
Not for distribution

White Paper on
Regulatory and Legal Aspects of Electronic Identity

Anssi Hoikkanen – JRC IPTS
Wainer Lusoli – JRC IPTS
Ramón Compañó – JRC IPTS
Ioannis Maghiros – JRC IPTS

Ian Brown – Oxford Internet Institute
Jos Dumortier – University of Leuven
Gloria González Fuster – VUB
Ronald Leenes – University of Tilburg
Yves Poullet – University of Namur
Giovanni Sartor – European University Institute
Thilo Weichert – ICPP Kiel

1. INTRODUCTION

Today, individuals, governments, and companies are increasingly relying on technology; this consequently raises a whole new set of technology-related challenges for regulators and policy-makers. In particular, the new developments and problems posed by electronic identity and personal identity management are taking on an ever more important role. While the importance of identity management systems solutions is widely understood, relatively little has been written on the accompanying regulatory and legal aspects of electronic identity. This is so despite the fact that members of the European Parliament,[1] the Council of Europe and EU Commissioners Reding and Kuneva have repeatedly expressed concern over the negative consequences of these developments[2].

This white paper thus addresses questions relating to the main challenges in the legal sphere, and what policy-makers could do to address these challenges by various legal means and instruments. The focus is on the regulatory and legal issues, not technical ones, as these have been addressed in detail in other for a, such as the recent identity management primer by OECD[3]. The white paper was born as a result of an electronic identity and law workshop in Brussels on 15 May, 2009[4]. It is a systematic extension of the workshop discussions and represents a seminal research paper on electronic identity and law.

The questions addressed in the paper are:

- What evidence exists on important trends and drivers?
- What, if any, are the main regulatory challenges?
- What tools (institutions, regulations, etc.) are available?
- Is a rethinking of the current regulatory framework necessary?

The white paper provides a starting point for a wide reflection on the current, sparse regulatory framework. While it, intentionally, falls well short of proposing an integrated, Community regulation of identity, it identifies in depth the gaps in the current regulatory framework and explores the relative merits of a coordinated approach to the regulation of identity in the digital age, an approach that speaks directly to the policy agendas mentioned. It is a first step in raising consensus on the need to study how the role and characteristics of identity are changing, and how these changes are taking place in the digital domain.

Commentaire [YP1] : To short… Explain why Digital identifiers are so important.

Commentaire [Ronald Le2] : t is for others to decide whether this is a seminal paper.

Supprimé :

Commentaire [YP3] : The first one would have to be : Which identifiers? For which purposes?

Commentaire [Ronald Le4] : agree with Ian that this is not the core of the paper. The analysis given is rather shallow and unnecessary. I would focus on a few clear needs for identity regulation and then describe the issues surrounding this need.

Commentaire [Ronald Le5] : r rather, raising awareness?

Supprimé : .

---

[1] EP Press Release. MEPs Call for Stricter Legislation to Protect Citizens from the Effects of Profiling. Justice and Home Affairs, 24.04.2009. Also see Sarah Ludford, Report with a Proposal for a European Parliament Recommendation to the Council on the Problem of Profiling, Notably on the Basis of Ethnicity and Race, in Counterterrorism, Law Enforcement, Immigration, Customs and Border Control (2008/2020(Ini)) (Strasbourg: EP Committee on Civil Liberties, Justice and Home Affairs, 2009).

[2] Viviane Reding, Citizens' Privacy Must Become Priority in Digital Age, Says Eu Commissioner Reding (Brussels, 14 April 2009: EC DG Information Society and Media, 2009), Meglena Kuneva, Keynote Speech at Roundtable on Online Data Collection, Targeting and Profiling (Brussels, 31 March 2009: Roundtable on Online Data Collection, Targeting and Profiling 2009).

[3] OECD, The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers, 2009, Available: http://www.oecd.org/dataoecd/55/48/43091476.pdf.

[4] Joint Research Centre, Institute for Prospective Technological Studies. Workshop on Regulatory and Legal Aspects of Electronic Identity. Directorate General, Information Society and Media, Brussels, Belgium, May 15, 2009. Workshop minutes on the Internet forthcoming.

2. TRANSITION AND ITS POLICY RELEVANCE

As the availability of digital content and distribution over digital infrastructure increases, the idea of digital living is being enabled. This means that we will need be using a mix of appropriately transformed old services as well as a set of new virtual services and applications. As part of this development, identification, authentication, authorisation (IAA), and access to services need to be managed ever more strenuously to ensure trusted access to both public and private applications. However, at the moment there is no universally accepted Internet identity infrastructure available to handle identification, authentication, authorisation online[5] (Figure 1).

Figure 1. On the Internet, Nobody Knows You're a Dog[6].

Nevertheless, during the last 20 years of Internet operation a certain level of trust has been created, at least in some realms, such as electronic banking where banks have set up their own trusted identity infrastructure using for instance tokens and special devices. As a result we have a plethora of sector specific solutions (based on e.g. SSL encryption, PIN, tokens) and e-services (e.g. PKI infrastructure with either strong or weak authentication). Problems culminate with these varying levels of assurance and protection, as the use of advanced Internet services becomes widespread.

There is an increasing awareness among policy makers and legislators that digital identities are vital to the way Internet services are provided and to citizens' everyday life (e.g with regard to digital living and advanced eServices). It is recognized that the same personal data that are used to enable access to services transforms into digital traces and the increasing linking of EU citizens' personal data to their online and offline activities raises a new set of issues concerning human rights, fairness and discrimination, competitiveness and competition, and digital market integration. There are concerns about the stepping over European citizens' human rights, including privacy and mobility, in an ever expanding surveillance society, perpetrated by business[7] and

[5] Commonly, people refer to this as 'on the internet nobody knows who you are', but this is conflating the issues, because often it does not matter **who** you are, but rather you're entitlement to some service matters. For instance, for some services one needs to be of age. It would be sufficient to assess that the claim that you are of age is true. This is not possible in many jurisdictions without revealing much more identity data. Also proving one's name (as a shorthand for one's identity) is not possible in many jurisdictions.

[6] Peter Steiner, New Yorker, Condé Nast Publications, July 5, 1993.

[7] MEP Stavros Lambrinidis, Report with a Proposal for a European Parliament Recommendation to the Council on Strengthening Security and Fundamental Freedoms on the Internet (2008/2160(Ini)) (Strasbourg: EP Committee on Civil Liberties, Justice and Home Affairs, 2009).

Supprimé : identify who the Internet user is

Supprimé : .

Supprimé : From the beginnings of Internet when www stood for "wild wide web", indicating the lack of any legislation on the Internet, we have moved to

Supprimé : a situation

Supprimé : with e-banking

Supprimé : , depending on the sector (e.g. health, leisure, work) and the necessary level of risk management (e.g. assets to protect, business model)

Supprimé : are now starting to emerge

Supprimé : protection

Supprimé : and there is ever more crime and abuse related to online identities

Supprimé : y

Supprimé : transactions

Commentaire [Ronald Le6] : his is where identity and personal data (and DP regulation) begin to merge

Commentaire [YP7] : It is not obvious that all identifiers are data, see the present discussion about IP addresses and the Tag number placed on objects.

Supprimé : is

Commentaire [YP8] : I am of opinion that the profiling activities and their increasing use of data personal or not to develop one to one marketing or to ensure an a priori knowledge about the users must be emphasized here in order to illustrate the dangers of e-id uses.

public authorities alike.[8] There are concerns about the potential impact of online data collection, targeting and profiling on consumers, including impacts on privacy, measured against the desire to foster the take up of advanced digital services by EU citizens.[9] Moreover, further issues arise concerning the consequences of the Internet of Things, IPv6 and cloud computing for personal data disclosure, storage and control.

(Personal) identity data, considered as an enabler of the digital economy, is likely to become a key component of DG Information Society and the Media new Commissioner and portfolio.[10] Policy makers have a crucial role to play in setting the framework conditions so as to sustain this shift while maximising the benefits for economy and society.[11] But also there is consensus that only when European citizens will be aware of, understand and fully enjoy the 'digital rights' granted to them by current EU regulations, will consumer confidence and the single market for businesses blossom, hence fulfilling the promise of the European digital market.[12]

3. EMERGING TRENDS

At the moment, many of the building blocks for new identity infrastructures are already in place. The technology and systems in use are reasonably developed, and the existing practices and regulatory framework (i.e. telecommunications, e-privacy, e-signatures, data protection directives, the EU internal market, and consumer protection legislation) enable the further development of electronic identity infrastructures. In the mobile sphere, identification mechanisms have already been established and work relatively well[13]. We can also see a new trend from circles of trust to open systems[14].

From this background, we can foresee the growth in the use of several different forms of electronic identity. Even today there is widespread use of eGovernment, eHealth, and eLearning applications. Furthermore, identity management systems are continuously improving, and activities towards further standards and agreements (cross-border and cross-sector) are being developed and utilised. Some infrastructure for integrated electronic identity infrastructures has already appeared, which allows for a better balance between more accountability and more anonymity in online transactions[15].

Another trend is the increased profiling activities, both for profit (mainly in the case of private businesses) and for security (mainly in the case of governments). However, it is

Commentaire [Ronald Le9] : ague. What do you mean by this. Provide some examples.

Commentaire [Ronald Le10] f this is correct, then why do we have a problem?

Commentaire [Ronald Le11] hat do you mean by this? Do you mean that the telcom provider can link a device to a subscriber('s name/identity)?

Commentaire [Ronald Le12] ague. What do you mean here? Examples would help

Commentaire [Ronald Le13] hy? This depends on the definition of electronic identity and the stakeholders and their influence/power. For instance, the Dutch government until recently considered there to be one electronic identity issued by the state (what you later call eID).

Commentaire [YP14] : The examples you refer are too narrow and mainly in relationships with e-Gov applications.

Commentaire [YP15] : Perha ps it would be interesting to identify who is working on theses standards (see for instance the ONS developed in the context of the RFID by a private standardisation body or the IP v6)

Commentaire [YP16] : What' s about the MICROSOFT platform for digital identities?

---

8 Ross Anderson, Ian Brown, Terri Dowty, William Heath, Philip Inglesant and Angela Sasse, Database State (York: The Joseph Rowntree Reform Trust Ltd., 2009), Ludford, Report with a Proposal for a European Parliament Recommendation to the Council on the Problem of Profiling, Notably on the Basis of Ethnicity and Race, in Counterterrorism, Law Enforcement, Immigration, Customs and Border Control (2008/2020(Ini)).

9 Meglena Kuneva, Key Challenges for Consumer Policy in the Digital Age (London, 20 June 2008: Roundtable on Digital Issues, 2008).

10 Euractive, Reding Makes Plans for New Commission Term, 23 June 2009, InfoSociety News, Euractive, Available: http://www.euractiv.com/en/infosociety/reding-plans-new-commission-term/article-183406, 29 June 2009.

11 Council of the European Union, Council Conclusions on Future Networks and the Internet (Brussels: Council of the European Union, 2008).

12 European Commission, Consumer Rights: Commission Wants Consumers to Surf the Web without Borders (Luxembourg: European Commission, 2009).

13 See for example: Günter Müller and Sven Wohlgemuth, Study on Mobile Identity Management (Albert-Ludwigs-Universität Freiburg, Germany: FIDIS Network, 2005).

14 Eve Maler and Drummond Reed, "The Venn of Identity: Options and Issues in Federated Identity Management," IEEE Security & Privacy 2008.

15 Stuart Short, Slim Trabelsi, Andrea Rota and Michele Bezzi, "An Architecture for Privacy Policy Composition," Research paper produced as part of FP7 program PrimeLife (2008).

not always clear what the benefits to the citizens may be. Various kinds of profiling models (advertising business model, crime detection, compliance with rules, health monitoring) present new problems in terms of privacy and data protection. Social networking sites (SNSs), where citizens profile themselves for fun and bonding with others, also create new challenges for social transactions, because citizen reputations (online and consequently offline) are at stake[16].

Emerging technologies exacerbate the complexity of identity-related issues. Technologies such as cloud computing and Internet of Things create new objects related to people and hence new profiling possibilities. Mobility presents yet another challenge, in this case for location-based profiling.

Overall, identity-related issues remain the same as in the past but many more parameters have to be considered. The most important of these are accountability, anonymity, technological robustness, legal liability, and their various implications. In general, the trends seem to point to the direction of user-chosen identities increasing in importance, and government-allocated ones decreasing (I am not sure since e-ID might be as regards at least transactional operations be viewed as more secure and as they are moreless gratuitously delivered quite interesting for people. Other problem the difficulty for people to manage a variety of different electronic keys. As I suggested the question of competition between private electronic signatures and official ones must be underlined)

4. CURRENT CHALLENGES IN REGULATORY AND LEGAL ASPECTS OF ELECTRONIC IDENTITY

In this white paper, we have identified and categorised the current challenges for the use of electronic identity into three clusters. These are the definitions-related challenges, identity rights related challenges, and the ones arising from the developments in the electronic identity industry. We will look at each of these in turn.

Definitions

One key issue regarding the legal aspects of electronic identity is its provider. Traditionally, identity and thus electronic identity have been and are **state-allocated**. In the last few years we have also seen the emergence of **user-chosen identity** (but mediated by the industry)[17]. The former can be referred to as eID, the latter as eId. In addition to this basic division, there is a need for a further definition and clarification of terms. Some key concepts are: identity, electronic identity, identifier, and partial identity.

A major threat in the future will come from **identity being linked to objects**, raising new issues concerning what is personal data, and what is personal identity data[18] (Internet of things as a challenge).

Historically, identity has been in the background, which raises uncertainties about its legal role in a transactional context[19], but as a result of technological development,

[16] Anders Albrechtslund, "Online Social Networking as Participatory Surveillance," First Monday 13.3 (2008).

[17] Thierry Nabeth, "Identity of Identity," The Future of Identity in the Information Society: Challenges and Opportunities, eds. Kai Rannenberg, Denis Royer and André Deuker (Springer, 2009).

[18] Article 29 Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/En, Wp 136 (Brussels: 2007).

Commentaire [YP17] : I don't see the link between the two sentences.

Commentaire [YP18] : What do you mean?

Commentaire [Ronald Le19] am not entirely clear what these issues are at this point.

Commentaire [Ronald Le20] his is not substantiated by the preceding text but comes later.

Commentaire [YP21] : I have really difficulties to see the logic existing between the different points analysed in that Point 4.

Commentaire [YP22] : I prefer to use the term "Categories" and to have a presentation following different criteria: the provider, the nature of the identified thing (person vs Object), the way by which persons are identified (name, serial number, body), the purpose of the identifier (traceability, authentication, …). Apart from these distinction we must have a grid presenting the peculiar issues of each of these types of identifiers

Commentaire [YP23] : We must refine these first distinction. The distinction is not only between identifier imposed by the state or chosen by the users. You have also digital identifiers imposed by companies. Additionally we must envisage biometric identifier apart from other identity linked to individuals.

Commentaire [Ronald Le24] agree with Ian that this is a novel way of distinguishing the two types of eid's. But why not.

Commentaire [Ronald Le25] hy are these problematic concepts

Supprimé : : s

Supprimé : problematic

Supprimé : of this type include

Supprimé : s

Supprimé : ies

Commentaire [YP26] : At my opinion cookie is an identifier Why not discuss about this kind of identifier?

Commentaire [YP27R26] :

Commentaire [Ronald Le28] ithout reading Sullivan, I have no clue what you mean b

... [1]

identity and its use context will become ever more significant. In addition, it can be dangerous to define identity in abstract terms, without being specific about its practical consequences, given that different rules apply in different contexts and businesses, as well as being different in the private and public sectors.

Apart from the lack of generally accepted terminology, there is **no common language** in different contexts and businesses. A common language is necessary to reach a shared understanding of the issues and the equal development of identity infrastructures in different sectors. The problem is compounded by policy-makers' in general not being prepared to tackle the issue, since most policy-makers of today are not well versed in web and identity related issues.

Identity Rights

There is evidence that, while with traditional service provision the requirement for identification lies with the provider, with the Internet it is the user that requires to access a service (most likely offered by another user who does not consider becoming a service provider) and thus it is the user that requires being authenticated. This leads to **two different understandings of identity rights** (if any such rights are thought to exist independently). These are, firstly, the right to be identified (with accurate identity information available when and where required, and on the other hand the limits of identification: privacy and data protection), and secondly, the right of one person's identity not to be misrepresented[20]. The second issue is more complex to deal with, and also a relatively new one, having emerged to such an extent as a result of the extremely fast developments in personal identity. On the other hand, the claim of the existence of an underlying right to identity is far more complex for data that is not controlled by the individual (e.g. by governments and companies) and that is not unique (proliferation). The correct representation (contextual integrity) of the data, based on autonomy, may be the underlying principle in both circumstances.

Anonymity (or/and pseudonimity?), an underlying principle of privacy, has long been recognised as a social value. Even though data minimisation is important, we must go beyond: more possibilities for anonymous transactions, for transactions using a pseudonym or concluded through a third party anomyser must become available than there currently are. On the one hand, we need mandatory mechanisms that allow 'switching off' identity. On the other hand, the increasing intrusion invites regulatory action concerning companies' value propositions, which need to be transparent and whose benefits should be clearly stated and measurable. This should be acceptable for businesses, as the guiding principle for their activities is what we want, not who we are. Therefore the key principles here are opacity of information and transparency of transaction.

Furthermore, it is important to discuss **which identity is used in which situation**: for example, private/public might be one useful distinction. Electronic identity also means different things in different use cases: for healthcare, social networking sites, and business transactions, to give just a few examples, the characteristics of and requirements for electronic identity are very different. A related point is that the data provided by individuals may be considered the personal property of the individual, at least in cases where the data is personal and specific to the person providing it.

---

[19] Claire Sullivan. Digital Identity – The Legal Person? Computer Law & Security Review, Volume 25, Issue 3, 2009, pages 227-236.

[20] The need for strong identity legislation has been emphasized, among others, by the EU Commissioner for Human Rights: Hammarberg, T. Strong data protection rules are needed to prevent the emergence of a surveillance society. Strasbourg, 2008, Council of Europe, Commissioner for Human Rights.

Commentaire [Ronald Le29] hat do you mean by language here? It appears to be terminology by another name.

Supprimé : This

Commentaire [Ronald Le30] or are they nuclear experts, yet, there is plenty of regulation regarding nuclear plants. What do you mean?

Commentaire [YP31] : We must clearly distinguish two different meanings of Identity: Identity from the subject's point of view is defined as the ipse of the individual. It means all the potentialities its personality might deploy. The protection of this identity refers to privacy issues as a way to guarantee the persons against undue interference (problem of traceability is obvious in that context). Perhaps it would be also interesting to see that under privacy concept the right to have a name and to a certain extent to have the possibility to choose it is considered as very important in order to build my own personality. Identity might also be seen (second understanding) as a way to be recognized by third party in the context of a relationship I will develop with him or her.

Commentaire [Ronald Le32] don't understand this sentence.

Commentaire [Ronald Le33] s far as I know there is no right to identity in the jurisdictions I know. There is a right to a name in the Netehrlands, but I would not call this a right to identity. Certainly not if the term is undefined.

Commentaire [YP34] : Right to see my identity protected and not right to identity

Commentaire [Ronald Le35] hat goes a bit too quick. Anonymity and privacy are related, but anon does no ... [2]

Commentaire [YP36] : Make reference to the Art. 29 WP about RFID suggesting the possibility of desactivating the RFID tag

Commentaire [Ronald Le37] t would be important to discuss that individuals (should have a right) to have multiple ... [3]

However, there are alternative cases such as the health sector, where the data are not known or understood by users well enough to be given control over them.

A common view today is that **user-chosen identity (eId) will drive the government-provided identity (eID)**. The rationale behind this argument is that however much data governments hold does not matter; instead, what matters is the way the data is used (i.e. according to OECD principles[21]). A real danger is posed by the fact that due to information technologies, profiling not only is possible, but becomes easy and can be automated[22]; this leads to profiles that are generated and used without citizens' knowledge[23]. Generally speaking, it is unclear what are the benefits for the citizens of increased surveillance; there is limited evidence of the impact of these technologies on security (especially in the case of national security, as profiling is not a reliable method for predicting rare events), but also in other fields, the impact of increased surveillance needs to be assessed[24]. Surveillance activities always involve economic trade-offs; these need to be monetised and economically modelled to make informed decisions.

Commentaire [Ronald Le38]
hat do you mean by this? Governments seem to pave their own road.

Commentaire [YP39] : I do not understand

In addition, the proliferation of eId means a significant **burden on the information handling capabilities of governments**, a burden they in general find difficult to handle. Some common problems are the economic restraints faced by governments and the occasional security issues[25] with government databases. Indeed, in many situations auditing controls may be useful or even necessary. The economic and security-related problems seem to indicate that a major part of the development of electronic identity would have to take place outside of government systems (in terms of *quantity* of developments, not in terms of their absolute value, since the crucial identity management systems will still have to be provided by governments). Moreover, states are not only controlling citizens, as government behaviour may spread into business; but then, through its purchasing power and through demand side regulation, the state at least has the capacity to dictate de facto standards in relation to personal data handling (and setting a moral precedent based on the following argument: we have more data than we need, but we will use them appropriately).

Commentaire [Ronald Le40]
hy? I don't understand this.

Finally, according to the OECD primer for policy-makers, there are four main challenges in terms of ensuring user privacy: (i) issues regarding the long-term safe storage and appropriate usage of personal information, and eliminating identity-related personal information when it is no longer needed; (ii) since the greater availability of credentials from high-level assurance systems could increase their use in systems with lower-level assurance needs, there could be an increased risk for personal data; (iii) the identity systems that facilitate anonymity and pseudonymity may raise new issues with regard to who has the right to decide which data should be veiled and when it can be unveiled; (iv) the fact that differences may arise as to which practices of identity and data collection,

Commentaire [YP41] : The problem is not obvious since as regards evidential purposes, private and public authorities needs to keep transactions' records during a long period. That problem raises also the question of the duration of life of our electronic signatures and the way to "re-generate" them.

---

21 OECD, Oecd Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2009, Available: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

22 Hildebrandt M, Gutwirth S. (eds.) Profiling the European citizen. Cross disciplinary perspectives, page 373, Springer Science, 2008.

23 Serge Gutwirth. Beyond Identity? Identity in the Information Society, Issue 1, 2009..

24 Mark Andrejevic, "The Work of Watching One Another: Lateral Surveillance, Risk, and Governance," Surveillance & Society 2.4 (2005).

25 Adrie van der Luijt, Audit Chiefs Still Lax on Data Privacy, 26 June 2008, Online article, Director of Finance Online, Available: http://www.dofonline.co.uk/governance/audit-chiefs-still-lax-on-data-privacy6637.html, 24 July 2008.

use, and retention can be left to market forces and which should be subject to government intervention.[26]

Developments in the Electronic Identity Industry

An ever more important issue in the eId industry is the **increasing monopolies** that are **outside the control of a single eId market regulation**. In this context, there is a need for the European Commission to ensure that EU institutions and member states (MS) are dealing with citizens' data correctly and transparently, as the most important regulating bodies, supported by regional and local authorities. Lately some companies have begun making the same argument (data availability does not matter); but there are questions as to whether businesses get the same level of scrutiny as governments do, and whether the data protection processes of all businesses are scrutinised equally. It should be kept in mind that collecting consumer information for business purposes and respecting their privacy can be competing goals[27].

Another problem related to the relationship between governments and business is that there may be **collusive behaviours** between governments and companies on the covert release of citizens' data (sometimes, as in the US, for money); this creates an economy of personal data which poses significant dangers in terms of erosion of privacy. The kind of citizen data that may be at risk due to its business relevance includes passenger travel records, accommodation records or SWIFT data for financial transfers. Rules that openly oversee such transactions would work best. There should be in-built guarantees that the data will be used responsibly, e.g. via state control, or through the user being able to decide how his data will be used. However, there is still a need for a debate on who is best placed to govern the overseeing of the implementation, and whether the supervising authority should be the same or a different actor in different contexts. Finally, the companies should also have economic incentives[28], apart from moral ones, to act responsibly.

A yet another industry-related challenge relates to **infomediaries including web 2.0 platforms**: private gatekeepers (such as the ISPs, Google, Facebook) of people's personal data that have a significant degree of control eating into areas which were previously opaque (such as the case of nominal e-ticketing, in which identity tags are attached to transactions that were previously anonymous). These gatekeepers have an overview of how you act with different companies and Internet sites and in different contexts. There should be adequate legislation in place to deal with the increasing role of infomediaries and to ensure data protection in their operations.

We can identify four different sets of problems in relation to infomediaries: (i) they do more than the collection of digital traces, collecting data from different sources, and there is little transparency over their current or future use which can create monopolistic attitudes; (ii) this in turn creates issues of trust and a need for a behavioural assessment of the user, as well as a need to evaluate benefits to consumers and society; (iii) it adds implications for responsibility and accountability, and provokes a re-thinking of economic incentives; (iv) it raises issues in relation to supervision and control, governance, soft regulation and benchmarking of company activities.

Commentaire [YP42] : The problem is not directly linked with e-id or e-ID but more generally a question of outsourcing as regards the processing of data collected by the public authorities.

Commentaire [Ronald Le43] tate control does not seem to be a particularly strong guarantee in this context as the state passes information to other states (in the light of law enforcement and fight against terrorism, which seems to include ever more actions)

Commentaire [YP44] : I see the problem but I don't see how you justify to speak about it at this moment (link with infomediaries,)

Commentaire [YP45] : Once again at my opinion the problem you stress here is not directly linked with e-id

---

[26] OECD, The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers.

[27] Bohme, R. and Koble, S. On the Viability of Privacy-Enhancing Technologies in a Self-Regulated Business-to-Consumer Market: Will Privacy Remain a Luxury Good? Workshop on the Economics of Information Security (WEIS), Carnegie Mellon University, June 2007.

[28] Acquisti, A. Security of personal information and privacy: Technological Solutions and Economic Incentives. In Camp, J. and Lewis, R. (eds.), The Economics of Information Security, Kluwer, 2004.

Other Challenges

In addition to the direct challenges to identity law and regulation discussed above, there are also indirect challenges. Most importantly, identity (as implemented in today's eID and eId systems) is necessarily linked to **trust** and societal acceptance, since we have no way to know whether people are misusing our personal data, which we voluntarily supply to access a given service. In general, there is **very limited if any societal discussion** on these topics, with the exception of a few countries, and definitely not at EU level. On a societal level, there is a strong need to link whatever implementation of eID and eId to measures of benefits for citizens and society. There is thus a need to do **impact assessment**: are citizens trading their personal data? In exchange for what? Under what assumptions? As a concrete example, it can be argued that data collection could be justified by the added public security, but in the UK the courts have not accepted this argument.

Commentaire [YP46] : References are needed

Technologies like web2.0, SOA with Web3.0, Internet of Things, cloud computing, IPv6, and location based services will also **generate further challenges** to the existing framework. They further increase data maximisation vs. minimisation, confer systems ways to identifying people, reduce possibilities for non-nominative transactions, link identity to objects and create further data fragmentation (which may then be data-mined). These growing tensions also apply to other 'identity' principles, such as purpose and unlinkability, which become more complex to manage in such environments.

Finally, not everything revolves around data protection, as **consumer protection and social discrimination** are significant components to consider in the regulatory discussion (where not only personal data at stake: the benefits and consequences of data protection in these contexts are equally important, if not more so).

5. TOOLS AND INSTITUTIONS

Even today, we already have various tools and institutions available to deal with the new requirements for identity management. The existing legislation is already extensive and provides many tools for tackling the challenges, but there are still problems due to a lack of standard **implementation.** In this context, there are many difficulties related to the inefficiency of data protection supervision (the relatively passive involvement across the EU, the limited powers of the Article 29 Working Party, and the differences in how proactive the national data protection authorities are), the inexistence of a single market for eId (because of differences in legislation across member states), and great **disparity** in national implementation of identity-related legislation, across members states and sectors (possibly even more disparity than has been previously argued, though some information exchange takes place, for example, in the legal system[29]). Almost nothing is known, for instance, about **data protection across national borders** (in the form of comparative studies or similar). Currently, data protection works under EU first pillar, which concentrates on consumer protection and market integration. At the moment data protection is processed differently under EU pillar three (security and defence, including protection from terrorist activities), though a similar processing under this pillar would be highly relevant. [more on this in the final version of the paper]

Commentaire [Ronald Le47] f whom?

Supprimé : need for more

Supprimé : active

Supprimé : legislation

Commentaire [Ronald Le48] ow does this relate to eID/eId? Cross Eu service delivery may involve eID/eId in the sense that the user can provide authenticated claims about her attributes or even identity, while the data protection consequences may be nil (because they data need not be stored).

Supprimé : 3

Supprimé : 1

The biggest implementation-related issue is the **compliance** of member states and companies with existing principles enshrined in the current legislation. Therefore, compliance with the law and its **enforcement** by data protection authorities is a key step

[29] Bayo-Delgado, J. European co-operation in the field of data protection. Ninth Plenary Meeting of the European Network for the exchange of information between persons and entities responsible for the training of judges and public prosecutors (LISBON NETWORK). Palais de l'Europe, Strasbourg, 10-11 October, 2007.

to be taken, the need for the enforcement being made increasingly visible by technological developments. At the moment, most member states have implemented the e-signatures Directive in their legislation[30], which is an important step towards standardized legal environment. This facilitates *legal* interoperability regarding a building block for electronic identities[31]. A complementary issue is the interoperability of identity solutions across contexts and/or national boundaries (which we call *business* interoperability): it may become an issue if the technological implementations are too specific or too tailored to the needs of a particular country or situation, as argued in the report quoted by Hayat et al[32].

The main issue, then, is the **application of the principles** (self-induced, regulatory, technological) underlying different pieces of legislation[33], as even the systems being considered and designed today clearly do not conform to them. The most important of these principles are *minimisation*: use and collection of the minimum personal data necessary to complete a transaction; *proportionality*: the maxim that no action should be taken which exceeds the demands of the situation in question; and *unlinkability:* ensuring that two pieces of unrelated personal data cannot be linked to each other by any actors. For instance, personal data centralisation and fragmentation are both a problem and a solution; there is a need to find a balance between identity efficiency and protection in scalability. The 'privacy by design' approach (one where identity protection measures are built into the systems from the start) is a possible solution in this respect[34].

The current tools at our disposal also include the more specific **compliance-inducing regulations**, such as drafting of industry Codes of Conduct[35] (for specific fields) to create a level playing field and for risk management, again needing support and approval from consumers (e.g. recent RFID recommendation); support for elaboration of standards (regulatory: W3C, pling, etc); and enforcement of EU regulation towards members states (infringement procedure). All these solutions point to a need for a more focused EU legislation addressing the 'grey' area surrounding the implementation of existing regulations (industry, member states). The latter item can be seen as a tried and tested and well understood way of ensuring member state activity in a given field, and as such relatively easy to implement.

One possible solution is **embedding the principles directly** in the new architectures to come. In this respect, an important problem is personal data fragmentation; fragmentation is both a resource (if it enables privacy and enables identities that are limited to a specific use) and a challenge (as it may create market dynamics of oligopoly on people's identity and de facto standards). This is related to the issue of centralisation

Supprimé : c

Supprimé : an be called

Commentaire [Ronald Le49]
ere you focus on DP, which is broader than identity. Provide a clear link with identity.

---

[30] Amir Hayat, Reinhard Posch, Herbert Leitold. Identifying Obstacles in Moving Towards an Interoperable Electronic Identity Management System. Institute for Applied Information Processing and Communication, Tech. Univ. Graz, Austria.

[31] R. Leenes, "Legal Interoperability in Pan European Authentication," FP7 project STORK (2008).

[32] E-security Task Group – APEC. Electronic Authentication Issues Relating to Its Selection and Use. APEC#202-TC-01.2, 2002.

[33] Marit Hansen, Ari Schwartz and Alissa Cooper, "Privacy and Identity Management," IEEE Security & Privacy 6.2 (2008).

[34] M Langenreich, Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems (Springer, 2001).

[35] Such as those provided by the CEN workshop: European Committee for Standardization CEN, Cen Workshop on Data Protection and Privacy (Ws/Dpp), 2008, Available: http://www.cen.eu/CENORM/Sectors/sectors/isss/activity/wsdpp.asp.

Mis en forme : Anglais Royaume-Uni

vs. decentralisation[36]: we generally assume that decentralisation is better (safer, more efficient, etc.), for example due to a smaller likelihood of the system being abused later on if there are several different stakeholders, but this is not necessarily the case in practice.

If we then move to a more general view of the legislation, most of the existing legislation does not deal with identity per se, but this is not true if we move down to specific applications and fields[37]. Therefore stating the need for a reform of the regulatory framework may be *dangerous*: this needs time to reach down, it is counterproductive to constantly modify and criticise current regulation, and technological neutrality is necessary. What may be required is a sort of **translational legal science**, whereby abstract principles are made more understandable in practice by integrating perspectives, and possible solutions, from other domains (see an example of how this can be done from the medical domain).[38] In the case of eId, this would imply looking at cryptography on the one hand and at value embedded design on the other hand (as an example of the translational paradigm of combining different perspectives). In this context, privacy by design and 'Code'[39] as code, as a technological choice would be a very valuable regulatory tool.

6. Possible Policy Responses to Current Challenges

This section addresses the following questions:

- What – if any – are the solutions? What is the (likely) impact of these solutions? How difficult would it be to implement them?
- Who are the stakeholders involved? What should they do?

Possibly the most important policy action, as discussed in the previous chapter, is the **enforcement of current legislation**. The legislation already offers substantial possibilities for data protection and the regulation of personal data management issues. What remains to be done is to ensure that all current business and government practices in this area conform to the law as it is, and that there are no loopholes in the legislation being exploited. The European Data Protection Commissioner has a significant role to play in this; for details, see e.g. Hustinx (2004)[40].

Commentaire [Ronald Le50]
s Ian also pointed out, EDPS only sees to the practices at the EU level. More relevant is the Article 29 WP.

Another very important issue is the **layering of regulation** on eId in the data protection directives (DPD) of specific fields such as health. In these cases, specific legislation and regulation is deployed on top of general provisions. On the one hand, this runs counter to attempts at systematisation, but on the other hand, it could provide a good rationale

---

36 Kurt Nielsen, "Is Distributed Trust More Trustworthy?," 7th Workshop on the Economics of Information Security 2008, 25-27June (Tuck School of Business, Dartmouth College, Hanover, NH: 2008.

37 See FIDIS work in this area, for example on legislation on ID theft in different member states: FIDIS, A Survey on Legislation on Id Theft in the Eu and a Number of Other Countries (2008).

38 http://en.wikipedia.org/wiki/Translational_medicine

39 A term coined by Lawrence Lessig in his 'Code' and other laws of cyberspace, New York: Basic Books,1999. By this he refers to technology as a regulatory tool. See also on the relation between Code and privacy, Bert-Jaap Koops & Ronald Leenes (2006), '"Code" and the Slow Erosion of Privacy', Michigan Telecommunications & Technology Law Review 12:1, p. 115-188

40 Hustinx, P. J. (2004). The Role of the European Data Protection Supervisor in the EU Framework for Data Protection. Polish Parliament, Warsaw, 26 May 2004.

for understanding which issues are specific to each field and which is shared between different sectors.

The role of the EC and EU as a large client for many companies in the eId industry should also be considered. Based on this, the **Commission could exert significant regulation** on privacy and data protection **via its buying power** (i.e., only buy into the best standards). The EC could also persuade the member states to act likewise at the procurement stage of eId.

Also, it should be kept in mind that **'identity'**, electronic or otherwise, **is not Community Law**. Identity can be discussed (and has been discussed: see e.g. Sullivan 2008[41]) under different headings to address the issues (the Commission has pushed in this direction several times, e.g. the eServices card); this is problematic, unless Community Law is changed.

The policy option that would possibly have the largest impact, though not the easiest feasibility, is **societal discussion** and acceptance of identity implementation; a democratic process of acceptance that is almost unanimously seen as legitimising eId in Europe. This has more to do with the active involvement of citizenship in the understanding and definition of personal data, privacy, and user control, than with education and awareness raising. The citizens must be empowered to manage their own digital identities appropriately and with means suitable to various situations. If the impacts of new identity implementations on the citizen are neglected, we will most likely end up with unsuitable solutions or with a low rate of acceptance.

Another area of policy options is formed by **soft legal-technical regulatory solutions**, based on Best Available Techniques for identity: anonymous identity, cryptography, DRM, guidelines for compliance, and Commission Recommendations as a suitable tool (e.g. on identifiers). These, largely based on soft regulation and persuasion, would offer a good balance between impact and chances of implementation at the present time. These include solutions that keep personal data separate, allowing data control *on behalf of* citizens, rather than *by* citizens (which could carry problems, due to increasing responsibility in case of lack of skills).

However, best available techniques (BATs) need to be seen as clearly linked to compliance; therefore not BATs in general, but BATs that generate compliance with specific eId regulation. In this context, the behavioural issues regarding the acceptance of different types of soft solutions should be analysed. Standardisation solutions, not necessarily EU level, (technical: privacy seals, ISO for IDMS) are often held to have a lower impact than other types of policy actions: this identifies a need for a debate on what the aims and benefits of standardisation (legal, technical) are in the field of eId.

In Annex 1, we provide some more specific policy actions that the European Commission and the member states could take, based on a list compiled in the Electronic Identity and Law workshop held in Brussels on May 15, 2009.

7. CONCLUSIONS

[to be written when the paper has been completed]

REFERENCES

Supprimé :

[41] Claire Sullivan. Privacy or Identity? International Journal of Intellectual Property Management, Volume 2, Issue 3, pages 289-324, 2008.

ANNEX 1. LIST OF POSSIBLE POLICY OPTIONS FOR ELECTRONIC IDENTITY. COMPILED IN "ELECTRONIC IDENTITY AND LAW" WORKSHOP, BRUSSELS, MAY 15, 2009.

a. Enforce EU regulation towards non-EU companies. (With regard to the common belief that companies whose home base is outside the EU enjoy a competitive advantage because the privacy laws and regulations in their home countries are not as strict as in the EU.) [42]

b. Enforce EU regulation towards members states (infringement procedure). (Currently member states do not enforce existing regulations with equal efficiency.)

c. Enforce Article 29 work + opinions (implementation by data protection authorities)[43]. (Article 29 is very valuable work but carries limited regulatory weight.)

d. Standardise definitions of personal data across EU. (Different definitions make it difficult to enforce common regulation.)

e. Standardise implementation of application of DPD + consumer protection. (Again, different approaches and implementations complicate regulation.)[44]

f. New supra-national legislation on eId. (EC should take a more active role in legislation given that the existing legislation is not sufficient.)

g. Standardisation solutions, not necessarily EU level (technical: privacy seals, ISO for IDMS) (Standards as a tool for creating technical uniformity and facilitating regulation.)

h. eId package relying on existing tools (regulation). (A new collection of laws and regulations that together form a package for regulating identity, privacy, and data protection issues.)[45]

i. eId regulation as infrastructural, like the eSignatures Directive. (A new directive, or similar higher-level legislation, that provides technology-neutral legislation on how to regulate identity.)

j. Including identity in Community Law (for parts not related to government activities).

k. Co-regulation for specific aspects, like SNS for young people (co-regulation between the industry and the Commission)[46].

l. Privacy enforcing using ePrivacy Directive art. 14.2 on compliance of terminals

---

42 For more information, see for example: Article 29 Working Party, Working Document on Frequently Asked Questions (Faqs) Related to Binding Corporate Rules, 1271-00-02/08/En, Wp 155 (Brussels: 2008).

43 Article 29 Working Party, Work Programme 2008-2009 (Brussels: 2008).

44 For an overview of current legislation, see: Stewart Dresner and Amy Norcup, Data Breach Notification Laws in Europe (Pinner: Privacy Laws & Business Copyright, 2009).

45 For an description of a similar "Telecoms Package", see: European Parliament, Electronic Communications: Universal Service, Users' Rights Relating to Networks and Services, Processing of Personal Data, Protection of Privacy, Consumer Protection Cooperation ("Telecoms Package" [Amend. Directives 2002/22/Ec, 2002/58/Ec and Regulation (Ec) No 2006/2004]) 24 September 2008 2008, European Parliament, Available: http://www.europarl.europa.eu//oeil/file.jsp?id=5563642.

46 See for example: Christian Fuchs, Social Networking Sites and the Surveillance Society (Salzburg/Vienna: Forschungsgruppe "Unified Theory of Information" - Verein zur Förderung der Integration der Informationswissenschaften., 2009).

m. Best Available Techniques – BATs for identity (anonymous identity, cryptography, DRM)

n. Guidelines for compliance. (Provision of guidelines by the EC to the industry.)

o. Recommendations as a suitable tool (e.g. identifiers).

p. Support for elaboration of standards (regulatory: W3C, pling, etc).

q. Codes of conduct (for specific fields) to create level playing field and for risk management; eCommerce Directive: CoC needs support from consumers (e.g. RFID recommendation). (The provision of codes of conduct by the industry itself, which all companies operating in the EU27 market must fulfil, and the breaching of which would lead to some kind of sanctions.)

r. Societal discussion, social shaping of identity technologies (consultation, consumer action, activism mobilising civil society). (As a way of better understanding what kind of laws, regulations and underpinning moral standards we want.)

Page 5: [1] Commentaire [Ronald Le28] **Ronald Leenes** **12/08/2009 12:44:00**

Without reading Sullivan, I have no clue what you mean by this. YP : I agree with Ronald.

Page 6: [2] Commentaire [Ronald Le35] **Ronald Leenes** **05/08/2009 11:23:00**

That goes a bit too quick. Anonymity and privacy are related, but anon does not underlie privacy. If one adopts the Warren/Brandeis definition of privacy, then anon has got nothing to do with it.

Page 6: [3] Commentaire [Ronald Le37] **Ronald Leenes** **05/08/2009 11:26:00**

It would be important to discuss that individuals (should have a right) to have multiple electronic/digital identities and use these (within boundaries) in different contexts. Audience segregation, partial identities etc belong here.