New Challenges and Possible Policy Options for the Regulation of Electronic Identity *

Anssi Hoikkanen, Margherita Bacigalupo,
Ramón Compañó , Wainer Lusoli & **Ioannis Maghiros**
European Commission's Joint Research Center-IPTS
Anssi.HOIKKANEN@ec.europa.eu

Abstract: This paper discusses the challenges and possible policy options for the regulation of electronic identity (eIdentity). Policy-oriented literature has often focused on technological solutions, and while this interest is warranted, much less has been said on the regulatory challenges and possible solutions arising directly from developments in eIdentity. In this context, we distinguish five main challenges for policymakers: eIdentity as a new legal category, issues related to identity rights, changing role of governments, developments in the eIdentity industry, and proliferation of identity management systems. We analyse these five challenges as they apply to two use cases, Augmented ID and Pinch Analytics, which highlight some practical problems for consumers that have emerged as a result of new concepts of eIdentity. We conclude by discussing possible policy options such as driving the development of a single regulatory market, supporting the development of common standards, enhancing cross-border legislation, defining a clear incentive framework for companies, and uniformly implementing existing legislation.

1. Introduction

The increasing reliance of governments, companies and individuals on technology to manage identity raises a new set of challenges for policy-makers. With the growth of content and services over digital infrastructure, people increasingly lead quasi-digital lives, moving in and out of analogue and digital spaces. Policy makers are increasingly aware that digital identities are vital to the way Internet services are provided and to citizens' everyday life. They 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.[1]

Identity, 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.[2] But there is also a consensus that only when European citizens will be aware of, understand and fully enjoy the 'digital rights' granted to them by current EU regulation, will consumer confidence and the single market for businesses blossom, hence fulfilling the promise of the European digital market.[3] Members of the European Parliament[4], the Council of Europe and EU Commissioners Reding and Kuneva have repeatedly expressed the importance of regulation in addressing the risks associated with these developments.[5]

---

* This paper won the 2009 JICLT Best Academic Paper Award at the 4th International Conference on Legal Security and Privacy Issues in IT held on November 3-5, 2009 at Malta. Originally published in Kierkegaard, S. (2009) Legal Discourse in Cyberlaw and Trade.IAITL.

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

[2] 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.

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

[4] 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).

[5] 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

On the one hand, there is a perceived need to revise and update current EU regulation to take into account the challenges to people's privacy and personal data introduced by new technologies. The Data Protection Directive, the ePrivacy Directive and a range of related legislation (eSignatures, Services Directive, etc) are being scrutinised as to their adequacy and efficiency in regulating an increasing range of online and offline transactions based on identity.[6]

On the other hand, policy-oriented literature often addresses this challenge by focusing on technological solutions. Although the interest in technical solutions is warranted, much less has been said on the regulatory challenges and solutions arising directly from electronic identity (eIdentity).[7] We argue that the current debate in policy circles may underestimate the implications of the digitalisation of identity and the centrality of 'identity' to the legal architecture protecting citizens' personal data, privacy and common wealth in the digital age. Hence, the distinction is between technical systems and citizen choice; while both are necessary, the rights of citizens should have pride of place in the debate taking place.

This paper addresses a number of regulatory challenges arising from recent eIdentity developments and proposes some instruments available to address these challenges. The focus is on regulatory and legal issues, not technical ones, by identifying legal gaps and exploring the relative merits of a coordinated approach to the regulation of identity in the digital age, one that speaks directly to policy agenda.

2. Developments in Electronic Identity

With informatisation, nation states have long lost the near monopoly they enjoyed on their citizens' identities. Providers of internet services, ICT companies and identity assurance providers have all but supplanted public authorities as the largest controllers of people's identity – provision of credentials, identification, authentication and authorisation. But old dogs also learnt new tricks, casting an increasingly wider net of electronic surveillance on the activities of their protégés.[8]

These relatively new identity info-mediaries and practices are today indispensable to ensure access to public and private services – including health, education and security. Increasingly, more of the personal sphere is recorded, stored and analysed (as in the case of nominal e-ticketing, in which identity tags are attached to transactions that were previously anonymous). Yet, identity transactions via such mediators are based on an increasing number and variety of identity systems. Neither Internet, mobile nor other electronic transactions are based on a single, interoperable let alone open-standard identity layer. There is today a plethora of sector specific solutions (based on e.g. SSL encryption, PIN, tokens) and e-services (e.g. based on a PKI infrastructure with either strong or weak authentication). We can also see a new trend from circles of trust to open and/or federated systems; this is part of the development away from centrally controlled systems towards more open identity infrastructures.[9]

At this stage, it is too early to adjudicate whether the trends described go in a direction of increasing fragmentation, decentralisation and user-chosen identity, or toward increased centralisation and more state and business control on people's identities. Regardless, novel possibilities for the qualification of human identity are emerging. These developments raise concerns about the stepping over European citizens' human rights, including privacy, in an ever expanding surveillance society, perpetrated by business[10] and public authorities alike.[11] How much freedom ought to remain for individuals and businesses to opt out from the provision of existing or forthcoming regulation needs scrutiny. Whether it is better to opt out of general rules or from specific transactions

---

Data Collection, Targeting and Profiling (Brussels, 31 March 2009: Roundtable on Online Data Collection, Targeting and Profiling 2009).

[6] Neil Robinson, Hans Graux, Maarten Botterman and Lorenzo Valeri, Review of the European Data Protection Directive (Cambridge: RAND Europe, Information Commissioner's Office, 2009).

[7] With the notable exception of Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt, eds., Reinventing Data Protection? (Dordrecht: Springer, 2009). For a discussion of legal provisions that apply to authentication for services provided by various EU Member States see Ronald Leenes, Bart Priem, Carla van de Wiel and Karolina Owczynik, D2.2 - Report on Legal Interoperability (Den Haag: STORK-eID Consortium, 2009).

[8] Ross Anderson, Ian Brown, Terri Dowty, William Heath, Philip Inglesant and Angela Sasse, Database State (York: The Joseph Rowntree Reform Trust Ltd., 2009).

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

[10] 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).

[11] Anderson, Brown, Dowty, Heath, Inglesant and Sasse, Database State, 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)).

(e.g. repudiation) requires examination. In general, there is today a very cautious attitude towards collection of citizen information, whether by governments or private companies.

Consumers increasingly have to take legal responsibility for their actions online as well as offline. For example, legal responsibility can derive from lack of diligence. It is complex to distinguish, technically and de jure, awareness from diligence. The point is similar to the one raised by the need to safeguard one's online, digital personae, whether a requirement exists to maintain a correct digital identity at all times, and whether there is a requirement to maintain it safe at all times, to prevent misuse.

Furthermore, problems originate at the intersection of personal, group, space and infrastructure (as in the case of: who has legal responsibility of in-links and out-links in a person's Facebook profile? Who has ownership?). For example, the question may be raised of whether links and relations are part of the self, or whether they belong to the context where these are generated (so-called data portability).In this framework, one cannot overemphasise the importance of technical-legal literacy for citizens, developers, legislators, judges. This can be a problem even for those who are called to develop new technologies, information systems and architectures. Software developers, for example, are sometimes unaware of legal consequences of some functionality implicit in the product; law is seen as a marginal element, entering the design equation very late in the design process.

Finally, from an economic perspective there are concerns about the monetisation of any of the possible identity architectures (centralised, federated, standardised, etc.) currently advanced by competing stakeholders, the benefits / risks balance in terms of European internal market, as well as fairness and competition of any such arrangements.

3. eIdentity Regulatory Challenges

We distinguish five main challenges and discuss each of them from a policymaker's perspective.

l) Challenge 1: eIdentity as a new legal category

The initial issue with the regulation of identity is, naturally, one of **definitions**. While this paper does not aim to contribute to this vigorous ongoing debate, we will note three key points.

First, identity and related concepts – entities, partial identities, identifiers, virtual identities, profiles – are currently **not well enough understood** in policy circles. The lack of clear and shared definitions of eIdentity precludes a correct representation of the challenges and as a result hampers building a consensus of a legal definition of the issue. In addition, there is **no common terminology** in different contexts. Conceptual work is required regarding the eIdentity transactions: 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), the resource to which the person gains access (commercial, social, public). The creation of one must precede any structured attempt at assessing the legal consequences of eIdentity. In this context, the policymaker should become much more aware of and engage in accepting available identity related terminology and definitions.

Second, the **relation between eIdentity and data protection** (DP) should be clarified. Often, as we noted in the introduction, the two are conflated in policy discussion regarding privacy and data protection. But eIdentity encompasses a much wider field than DP. DP rules qualify identity only in relation to controllers' behaviour with respect to personally identifiable information (identifiers and partial identities). Partly, this depends on the fact that DP deals hierarchically with information privacy rather than horizontally with physical privacy and decisional privacy. DP over-determines identifiers in circumstances where identity is under no threat. DP also offers no assurance concerning contextual integrity[12] of identity.

Overall, we can say that the link between data protection regulation and privacy is too unclear. While DP rules are technology neutral, of general value and assist global legal interoperability,[13] they do not address the core challenge identified in the previous section: the extension of identity by digital means, the increasing number of actors, the multiplication of identifiers and type of identifiers. In this context, the policymakers should be prepared to discuss eIdentity as a separate concept from data protection, taking into account their different requirements. Policymakers, while having placed adequate emphasis on data protection, may not have addressed in sufficient scope the wider eIdentity related challenges.

[12] H. Nissenbaum, "Privacy as Contextual Integrity," Washington Law Review 79.1 (2004).
[13] Michael D. Birnhack, "The Eu Data Protection Directive: An Engine of a Global Regime," Computer Law & Security Report 24.6 (2008).; Robinson, Graux, Botterman and Valeri, Review of the European Data Protection Directive.

Third, and in relation to the latter, one key issue regarding the legal aspects of eIdentity is its provider. Traditionally, identity and thus eIdentity have been and are **state-allocated**. In the last few years we have seen the emergence of **user-chosen identity** (but usually mediated by the industry),[14] and **identity otherwise attributed** (by profiling, by objects, by current location, and by fellow SNS users). The first can be referred to as eID, the latter as eId. The last is even more problematic and, as it extends and augments identity in ways unpredictable and unprecedented on this scale. 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.[15] Based on a process-based view of identity, regulation may be best addressed to transactions where personal identity data is exchanged. For this type of transactions, the current framework ensures procedural fairness via the Data Protection Directive (DP). The framework is much less effective in protecting **identity-relevant non-transactions**: where people go, online and offline, who they are with, what they do, who they know, and what they think. Moreover, such non-transactions may be used in ways that the user could not anticipate, as digital traces are identified, assembled and re-presented. In this context, the policy actions required vary according to provider and type of identity, as well as type of transaction; hence policymakers should be prepared to tackle each aspect according to the specific requirements it places on the regulatory framework.

2) Challenge 2: Issues related to identity rights

Beyond definition, one important challenge is to determine whether, a right to identity exits that may address the challenges described in the introduction. In legal doctrine, there are two different understandings of identity-related rights – if any such rights may be thought to exist independently – which are strongly linked to the ongoing discussion on eIdentity in academia.

The first is **the right to identity**; this is the right to be able to identify oneself in every circumstance, and not be forced to do so. On the one hand, it is a protective right, imposing limits on identification based on privacy principles (protecting from undue interference) and based on limitation of purpose (defining the boundaries / aims of identification). **Anonymity and pseudonymity**, both of which are enablers of privacy, have long been recognised as social values per se. Personal data minimisation and transparency of transactions are of course important: increasing intrusion invites regulatory action concerning companies' value propositions, which need to be transparent and whose benefits should be evident. But we also need more possibilities for anonymous and pseudonym transactions, for transactions concluded through a third-party anonymiser, for mechanisms that allow 'switching off' identity (for instance deactivating RFID tags). In this context, policymakers should consider specific legal provisions that allow for and regulate transactions without the use of personal identity data, and which take into account the possibility of temporary switching off of identity.

The second is **the right of one person's identity not to be misrepresented.** The second right 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. Identity is seen in this second understanding as a way to be recognized by third party in the context of a relationship; it thus protects the identity of individuals. The right is closely related to the idea of contextual integrity of identity. It protects the individual from discrimination based on incorrect representation, and relates to the concept of decisional privacy (again, a developmental principle).

This second right is the most relevant to eIdentity, as it directly speaks to the challenges of fragmentation, centralisation and data control discussed above. But the claim of the existence of this underlying identity right is complex for data that is not under the control of the individual (e.g. by governments, companies, other individuals). In this context, more work is needed that specifies what aspects the policymakers need to address under the heading of a right to identity (i.e. which data contribute to provide a picture of one's personality or identity), and how this needs to be reflected in the law.

3) Challenge 3: Government as both friend and foe

A relatively common view today is that the logic governing user-chosen identity (eId), often via commercial applications, is influencing developments in government-provided identity (eID). Governments face increasing challenges in terms of ensuring user personal data privacy[16], as issues arise regarding the long-term safe storage and appropriate usage of personal information, and eliminating identity-related personal information when it is no longer needed; the solution is not obvious, as for evidence purposes, private and public authorities need to retain transaction records. In addition, various government departments and agencies may occasionally have different

[14] Thierry Nabeth, "Identity of Identity," The Future of Identity in the Information Society: Challenges and Opportunities, eds. Kai Rannenberg, Denis Royer and André Deuker (Heidelberg: Springer, 2009).
[15] Article 29 Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/En, Wp 136 (Brussels: 2007).
[16] OECD, The Role of Digital Identity Management in the Internet Economy: A Primer for Policymakers (Paris: OECD, 2009).

practices as to how they handle particular identity and data protection issues. This may lead to questions over the government's role as an impartial arbiter and legislator on identity related issues.

Differences may arise as to which practices of identity and data collection, use, and retention can be left to market forces and which should be subject to government intervention. The proliferation of eIdentity places a significant **burden on the information handling capabilities of governments**. The high economic costs[17] may imply that that most eIdentity management would have to take place outside of government systems. If this is the case, then other regulatory instruments besides legislation may be applicable. Governments' purchasing power and demand-side regulation endows them with 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).

Another challenge related to the relationship between governments and business is that in some cases there may be **collusive behaviours** between governments and companies on the covert release of citizens' data. This creates an economy of personal data which creates significant dangers for erosion of privacy. Personal data that may be at risk due to its business relevance include passenger travel records, hotel accommodation records or SWIFT data for financial transfers.

For these transactions to be effectively monitored, rules that openly oversee them are needed. The problem concerns the shape of these rules. Firstly, state control does not seem to be a particularly strong guarantee in a context where states pass information to other states (in the light of law enforcement and fight against terrorism). Secondly, subject access (let alone user control) of such personal data is today virtually non-existent; data protection principles are either excepted-to in this domain, or violated (e.g. data minimisation). Thirdly, there is a need for an open debate on who is best placed to oversee these rules, and whether the overseeing authority should be one or many in different contexts. It is not sufficient to rely on rules, and in-built guarantees cannot ensure "responsible" usage.

All this means that the role of the government is more than just that of a regulator. Governments, even though functioning as policymakers, have their own data protection and management challenges. It is not even always clear whether governments are the best placed stakeholders to manage specific kinds of information. In this context, the challenge for policymakers in this environment is to create a regulatory framework that recognizes this changing role of governments, and that certain responsibilities for identity management may be shifting towards the private sector.

4) Challenge 4: Market developments in the eIdentity industry

In general, there is a need to ensure that EU institutions and Member States collect and process citizens' data correctly and transparently, in an equivalent fashion across national borders, as the most important regulating bodies, supported by regional and local authorities. Lately companies have begun arguing that data availability does not matter as long as it is dealt with according to data protection provisions; but there are questions as to whether all businesses get the same level of scrutiny, between themselves and in relation to governments. It may be the case that some **companies** operating in the eIdentity market are **outside the control of a single identity market regulation**. This may especially apply to companies in dominant market positions (though their competitive positions should predominantly be addressed by the EU competitive legislation). In this context, it is important that EU and Member State policymakers seek to establish a single regulatory market for eIdentity so that the same rules apply across the common market. Companies need a clear, actionable structure of incentives and disincentives, both economic and legal, to respect user privacy by relinquishing personal data as a potential source of revenue at negligible marginal costs.[18] The ultimate purpose of this incentive framework is to ensure a level playing field and that no company exploits its dominant position in the market to gain an unfair competitive advantage. There may also be a need to more clearly distinguish between company activities within the EU and activities crossing the border between member and non-member states, as different rules and regulations may apply in the two contexts.

A second challenge relates to **infomediaries including web 2.0 platforms**: private gatekeepers of people's personal data (ISPs, Google, Facebook) have a significant degree of control on areas which have been, and still are, opaque, unless there is a financial incentive for the collection and reselling of specific data which will cover the cost of the collection. These gatekeepers have an overview of how people act with different companies and Internet sites and in different situations, as a result of users being identified and matched correctly. In this context,

[17] 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.

[18] Rainer Bohme and Sven Koble, "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 (2007..

policymakers should ensure the adequacy of the legislation in place to deal with the increasing role of infomediaries and to ensure data protection in their operations.

Furthermore, economics of identity are in general not well enough understood at the moment. In addition, the question is not only about analysing the market and the transactions taking place in it, but about defining what kind of economic object identity is. Economics of identity can be looked at from several different perspectives: the first of these we call identity as a consumption good, where users choose their identity according to circumstances. In this case, identity results from *explicit* choices by the individual. This implies that it is transactable and can be sold, either temporarily or permanently; it is also be possible for identity to be stolen. The classic economic approach to study identity as consumption good would be economics of choice.

Identity can also be understood as a capital asset. In this case, identity is dealt with as a property that can be publicly traded. Identity will have a changing value over time and space, because people value their identity differently at different times and in different use cases and social contexts. Economics of identity can then be studied via behavioural economics and game theory.

Thirdly, identity can be analysed as a public good (economics of esteem and reputation). In this case, identity is understood to have network effects, meaning that identity increases in economic value by its increased use (by companies, by people). This understanding of economics of identity can most gainfully apply to social networking sites such as Facebook and mySpace.

Finally, the conventional way to understand identity is purely as a cost (economics of security). This means that the economic value of identity is only recognized as far as it incurs costs for the different stakeholders (governments, companies, consumers). Hence, this definition does not really deal with identity, but with privacy and data protection. The positive (i.e. value-generating) effects of identity are not taken into account, which makes this definition somewhat unsatisfactory.

In the context of economics of identity, policymakers should be much more aware about what consequences the different definitions of economics identity have, and how they therefore want to treat it as an economic object. The identity market should also be followed in much more detail than it currently is. Although the identity market is for the moment (mostly) intangible, policymakers still need proper metrics and modelling tools to keep track of the development of the market.

5) Challenge 5: Proliferation of identity management systems

In recent years, there has been a proliferation of identity management (IdM) systems in the marketplace. Consumers and citizens are faced with numerous digital identification systems and techniques, which combine different identity attributes, apply different standards and technical processes, and provide different levels of assurance. This makes it difficult to understand how each system works and to adopt appropriate ways of using them. As a result, there is a need to provide guidance for citizens and to address the education and awareness challenges so that citizens will be able to appropriately manage their digital identities.

Education and awareness are of crucial importance in creating trust and alleviating user concerns. A major element in increasing awareness is improving the level of accountability and transparency provided by IdM systems. There may be a need for consistent policies that accurately define the required level of accountability and transparency, which should then be applied across all the systems. Accountability and transparency across multiple services in diverse legal and technical regimes are issues making the situation even more complicated.

These factors make it ever more difficult for citizens to make *informed* choices about how they manage their digital identities. Yet, the issues posed by the high number and complexity of IdM systems in operation must be addressed if electronic identities are to reach their full potential. In this context, policymakers should be prepared to implement measures aimed at raising citizens' knowledge and awareness with regard to identity management, and to consider measures requiring a greater degree of accountability from IdM system providers.[19]

4. Possible Policy Responses to Current Challenges

Today, various institutions and tools already deal with the challenges of eIdentity. The legislation already offers substantial possibilities for data protection and the regulation of personal data management issues. But while existing legislation is extensive and provides many tools, there are still problems due to a lack of standard implementation. Below we present an overview of some possible solutions classified by thematic area.

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

Table 1. Potential policy responses to eIdentity regulatory challenges

Category	*Policy response*	*Description*
Creating a single market for eIdentity regulation	Legislation applicable across all Member States	Uniform implementation of existing and future legislation across EU27
	Cross-border legislation	Further legislation on cross-border identity-relevant transactions should be developed, both for transactions within the EU and between EU and non-EU countries
Compliance to existing regulation	Enforcement and implementation	More emphasis should be put into making sure that the (already extensive) legislation is taken into use and its principles are being followed across all Member States
	Review of powers of data protection authorities	The powers of data protection authorities need to be proportional to their tasks, to avoid their being unable to fulfil their mission
	Layering of regulation and increased granularity	Use of additional legislation in specific fields of application as necessary (on top of existing provisions)
Identity by design	Application of privacy principles to systems at design stage	Require that companies apply key privacy principles such as data minimisation, unlinkability and proportionality to new data management systems
Soft law and alternative regulatory mechanisms	Best available techniques, guidelines for compliance, Commission Recommendations	Soft regulatory tools that achieve results quickly and address the most evident legal gaps while higher-impact solutions are developed
	EC de facto regulation	European Commission exerting de facto regulation via its purchasing power, thus steering market development to the desired direction

5. Use cases with regulatory implications

In this chapter, we discuss two use cases that pose specific challenges for policymakers from a regulatory point of view. Our discussion of the use cases is aimed to illustrate practical problems raised by some identity-based services, and it is outside the scope of this paper to study the theoretical questions associated with scenario analysis. Significant work in this are is carried out, for example, the FIDIS consortium.[20]

5.1 The Astonishing Tribe: Augmented ID[21]

Augmented ID is an augmented reality concept for mobile phones from the Swedish company The Astonishing Tribe. The product uses a facial recognition software (provided by a company called Polar Rose) installed in the mobile phone to recognize the people around the user, and to then retrieve pre-selected information about them according to their preferences. All users are able to control their own augmented appearance by selecting the content and social network links they wish to display to others. These can contain anything from phone numbers and email addresses to links to their tastes, whereabouts, social networking platforms, and other media chosen by the user.

[20] http://www.fidis.net/. For more details, see deliverables 17.1 and 17.3, at http://www.fidis.net/resources/deliverables/privacy-and-legal-social-content/#c2480
[21] http://www.tat.se/

The core of the system is the facial recognition software. It performs the recognition by matching 3D models of faces to the image captured by the user. It takes into account distinctive features of the face such as the contours of the eyes, the nose, and the chin. The product only works when both people have registered into Augmented ID, so it can only be used to identify, and retrieve information about, persons who have created an Augmented ID profile.

The Augmented ID concept presents several challenges for policymakers from an identity management perspective. With regard to eIdentity as a new legal category, the service may be used in ways that the user does not anticipate. For example, it is possible that the information is combined with that from other sources, thus creating possibilities to create a more complete or accurate portrait of the user than intended or desired. The service may also be problematic when it comes to switching between several different profiles. For example, many people may want to switch between a "time off" profile and a business profile; but what happens if the person using the service forgets to switch the service off? Or what if he is in a location (such as a restaurant) after hours, but there are people present from his working environment? Clearly, there is a need to differentiate between different uses contexts and between people you share your information with, whether the sharing is broadcasting, narrowcasting or one-to-one. The contextualisation of the information is thus the key to appropriate functioning of the service, and these contextual aspects must be adequately covered by the legal framework.

With regard to identity rights, the user should not be forced to identify himself in all the contexts, or to divulge every type of information about himself. There is a clear need for personal privacy control for services such as these. However, applications such as Augmented ID tend to start from an opposite principle: they are oriented towards being completely public and allowing you to publicise information about yourself, that is, they are designed to disseminate information, not to contain it. The challenge for users is to manage their data filters and to make sure they only share the data they want, in the circumstances they want. Furthermore, the Augmented ID concept generates problems due to the nature of electronic identity itself, which is by its nature dynamic and changes according to context. While current legislation seems adequate to regulate static information, the question must be raised whether the current regulatory lregime can cope with the more dynamic nature of identity in blended physical and digital environments.

With regard to the developments in the eIdentity market, the position of the company storing this information has to be considered. In essence, the company offering this type of service functions as an infomediary (such as Facebook), and the same regulatory challenges (the company has an overview of how people act with different companies and Internet sites and in different contexts) exist. Another issue is presented by the possibility of the system being hacked. What happens if the information is published in the public Internet? How does the existing legislation take this possibility into account, e.g. by providing a safety net for the users or by specifying the legal consequences and responsibilities for the companies?

With regard to the proliferation of identity management systems, the Augmented ID service is one more to the long list of services or systems requiring users to manage their electronic identity. The proliferation of IdM systems is thus a challenge with this service too: how to manage the identity attributes, technical processes, and levels of assurance associated with the service.

Many policy responses outlined in this paper could be used to better regulate mobile augmented reality services. Most importantly, they should be uniformly regulated over the EU market. Regarding compliance, it should be ensured that the current identity related legislation extends to novel services such as this, and it could be bolstered by specific legislation for mobile services. Identity by design offers many possibilities: identity protection measures should be included in potentially risky concepts like this one from the start. Softer regulatory measures could be used to provide additional coverage, though their impact could be more limited.

5.2 Pinch Media: Pinch Analytics[22]

Pinch Media is a US-based company that has created a software for monitoring the usage of iPhone applications and services. Their main product, Pinch Analytics, consists of a library and a brief code that companies can add to the mobile applications used by their customers. The product allows companies to keep track of, with simple method calls, the number of times, users and sessions in which any action occurs. It reveals statistics like the length of usage of a particular application, which features are used more often than others, at what times of day are the applications being used, and so on. The goal of providing this information is to allow developers to gather data about the usage patterns of their applications and to develop them according to customer preferences.

It is true that there are many applications available that track iPhone applications' user data, such as location, the iPhone's unique ID, the phone model, and possibly even more personal data like age, gender, contact details and Facebook information. However, Pinch Media can be construed as being much more intrusive than other companies related to this sort of tracking. The data whose collection their application enables can include not

[22] http://www.pinchmedia.com/

only personal details, but also the user's current latitude and longitude, the exact times and dates a service is used, and information on the operating system of the user's phone. This data can also be continuously tracked every time the phone is being used. Therefore there are significant privacy challenges created by Pinch Analytics and similar services.

Firstly, we have to assess the existing legislation's applicability to these kinds of new problems. Software collecting detailed identity information over mobile networks has only existed for a relatively short time. Does the current regulation cover, in sufficient detail, the legal complications posed by such novel services? Furthermore, here may not be enough awareness on the part of policymakers of these new challenges. Policymakers may on some occasions be underprepared or even unwilling to engage in these issues.

From the perspective of identity rights, the transparency of company actions must be emphasized. Are the users adequately informed of what information is being collected, how it is stored and for what length of time, are they given sufficient opportunities to opt out of information collection, etc.? In addition, there is the question of defining the boundaries of the information collected by companies such as Pinch Media. Where are the limits of acceptability? While companies clearly desire to collect customer information for business and marketing purposes, definitions of appropriate limits for data collection are still lacking.

In terms of market developments, there are challenges as to whether these services are similarly regulated across the EU, how cross-border transactions are monitored, and how those transactions that cross the EU – non-EU border. Since many iPhone and mobile users routinely use their devices in multiple national markets and access services offered in different markets, problems regarding such usage of mobile services are certain to increase over time. Pinch Media is an US-based company, but its software may have many institutional users in Europe; does the existing legislation adequately cover the regulatory implications of using such products?

As to potential solutions, it is crucial that the legislation of novel mobile services is addressed in a uniform fashion, and with appropriate regulation, especially since the applicability of the current regulatory regime appears to be in doubt. Secondly, the boundaries of acceptable data collection should be clearly defined, as discussed above. Thirdly, we see a need for some kind of proof of compliance with the regulation from the companies. This would include an assessment of the risks, how they are mitigated, how would possible leaks of information be dealt with in legislation, and so on. As with the Augmented ID case, there is also a possibility for specific new legislation. Fourthly, softer mechanisms are also a possibility, though in this case their impact might be even more questionable.

6. Policy options

This section discusses some policy options policymakers should consider based on this paper. The policy options are divided into two groups. We differentiate between enabling actions, i.e. things that can be done so that policymakers are well informed, and policy actions with a direct impact on the eIdentity market.

As to the enabling actions, many of the challenges discussed revolve around different definitions of eIdentity. Generally speaking, identity and related concepts are not as well known in policy circles as they should, and at the moment there is no commonly accepted terminology for these concepts. Therefore much conceptual work is required before any structured attempt to assess the legal consequences of eId can begin. While the majority of the definition work is carried out in different standardisation organisations, the policymakers need to support the development of common standards and shared ways of operation, and ensure that they are uniformly understood within the EU.

The policymakers would also likely benefit from differentiating between two forms of identity-related rights. These two rights are the right to identity and the right not to be misrepresented. The legal framework must define what precisely is meant by these, and which means are used to address these rights. Identity rights legislation is made particularly difficult by the fact that identity is by nature dynamic and changes according to context, as illustrated by the Augmented ID case. Finally, in order to keep up to date on the competitive landscape, policymakers should also consider building a repository of eIdentity market information describing the most important developments in the industry as well as the key stakeholders and their activities.

As to the direct policy actions, the two use cases analysed in this paper illustrate the importance of distinguishing different use contexts and the information supplied by the user in each. The legislative framework should accordingly be able to recognize the requirements posed by contextualisation of information. As can be seen from the Augmented ID case, many applications are built with a view towards publicising personal information, not towards containing it, which raises questions about the personal responsibility of the consumers who choose to use such services.

The position of governments is also challenging. They can no longer be considered the sole provider of identity, especially not electronic identity, which in many cases has meant that the logic of privately provided identity has infiltrated the logic of government-provided identity (eId vs. eID). The governments also increasingly

face issues related to safe storage of data and its appropriate use. There is a further question of how to regulate transactions between states and businesses; specific rules overseeing such transactions may be needed. Therefore, the regulatory infrastructure should be designed so as to take into account not only the particular issues facing the private sector, but also address the challenges for the public sector.

The shaping of the eIdentity market represents an important opportunity for the regulation of the industry, enabling policymakers to influence its evolution in consideration of citizens' rights. Increasingly, there are companies operating in multiple national markets in the EU27, and across the EU – non-EU border, some of which may not be adequately covered by the existing legislation. The cross-border legislation is still very limited, making it difficult for businesses and institutions to operate across national borders, and making the legal position of both the users of the services and the companies offering them unclear. The Pinch Analytics case illustrates the importance of clearly defining the specific responsibilities and liabilities for stakeholders in different national markets. It can also be noted that without these definitions, consumers and companies will both likely be more reluctant to take up such new services.

This issue also extends to infomediaries, gatekeepers of consumers' personal data, who in some cases may be under limited supervision. The Augmented ID and Pinch Analytics cases both highlight the extensiveness of data that certain companies can collect about users. Therefore there is a need to set boundaries for acceptable collection of information (and also for the authorities to ensure the total transparency of this collection). Further, there should be a clear and actionable framework of incentives for companies to respect user privacy and to limit data collection only to those use contexts where the collection is clearly justifiable. The Pinch Analytics case further illustrates that there may also be a need to require from companies some kind of proof of compliance with the existing legal standards, though how this could in practice be assessed is a more complicated issue.

The highest-impact direct policy action will most likely be driving the emergence of a single market for regulatory purposes. There are still probably possibilities that have not been fully exploited. For example, while the existing legislation is already quite extensive, uniformly enforced legislation across the Member States has still not been achieved. One promising possibility for the enforcement of legislation is for the regulator to exert influence through EC's purchasing power, thus driving the evolution of commercial systems in the direction approved of by policymakers.

A single, EU-wide eId regulatory infrastructure would also be beneficial for the economic development of the electronic identity markets. The realisation of this structure would facilitate the development of a common market and make it easier for companies to operate across the EU, thereby providing them with a higher number of potential customers and help them achieve economies of scale. Furthermore, the existence of uniform legislation would also enable a higher level of cooperation between companies in different Member States or operating in different parts of the value chain.