IDIS (2008) 1:173–187
DOI 10.1007/s12394-009-0011-9

eID policy in a turbulent environment: is there a need for a new regulatory framework?

Wainer Lusoli · Ioannis Maghiros · Margherita Bacigalupo

Received: 4 August 2008 / Accepted: 16 February 2009 / Published online: 8 May 2009

Abstract There is increasing interest in the EU about the central place of eIdentity (eID) in people's lives. eID is increasingly seen as a bridge between the commercial viability of models based on large-scale provision of e-services and users' need for privacy and security in online transactions. This paper examines technological, social and legal developments in the field of eID and asks whether there is the need for a new regulatory framework that both preserves users' identity and enables the provision of advanced services. Firstly, the paper interprets recent market moves in the eID field as a response to a rising regulatory tide. Secondly, it examines some of the challenges arising from Web2.0, and four emerging socio-legal issues associated with eID—behavioural profiling, social engineering, redlining and other unsocial practices. Thirdly, the paper examines the capacity of the current regulatory framework to absorb this turbulence, and finds it wanting. Finally, it advances a novel model of eID regulation that may help regulators create an identity-preserving, transaction-friendly eID environment.

Keywords eID · Regulation · European Union · Data protection · Privacy · Web2.0 · AmI

The eID market in the face of rising regulation

The year 2008 marked a turning point when major industrial eID players aimed at positioning themselves favourably in the face of increased attention by policy-makers, public worry about personal data and a striking string of data breaches in public and private sector. Google, a major player in the eID field, has become increasingly vocal and apparently proactive on privacy, user control and data retention. A number of large players have joined OpenID after initial scepticism.[1]

[1]See the OpenID 2008 timeline at http://openid.net/2009/01/15/momentum/; also see http://en.wikipedia.org/wiki/OpenID

W. Lusoli (✉) · I. Maghiros · M. Bacigalupo
European Commission - Joint Research Centre (JRC), Institute for Prospective Technological Studies (IPTS), Edificio EXPO, C/ Inca Garcilaso, s/n, 41092 Sevilla, Spain
e-mail: wainer.lusoli@ec.europa.eu

OpenID has been set as a parallel identification mechanism for HealthVault, Microsoft's flagship in e-health. Again in 2008, the *Information Card Foundation*, a consortium of Equifax, Google, Microsoft, Novell, Oracle and PayPal stepped up industry action regarding card authentication. In June 2008 Liberty Alliance made available the Identity Assurance Framework (IAF) and the Identity Governance Framework (IGF) to their members. IAF is a global standard framework for validating trusted identity assurance service providers based on a uniform definition of the security and privacy risks associated with different levels of identity assurance. IGF is a declarative policy framework for managing identity flows within organizations motivated by regulatory requirements, such as those set by the Data Protection Directive;[2] it creates a standard for defining enterprise-level policies and controls for consumer consent for sharing sensitive personal information, including personally identifiable information (Liberty Alliance 2008). In October 2008 a user-centric 'identity meta-system' was proposed by a consortium including IBM and Microsoft which features significantly enhanced privacy and user-control with respect to the original Microsoft vision. The eID industry is fully represented in the EU-funded large scale project STORK,[3] aiming at creating interoperable public administration identities across EU member states (November 2008). A consensus seems to be developing that privacy is core to any new developments in identity management (e- and otherwise) and on the need to factor in privacy (social, technical, legal) early at the design stage of systems and applications (Hansen et al. 2008), especially in federated identity environments (Squicciarini et al. 2008).

This consensus hardly bears on identification alone; rather, it aims to shelter the large prospected revenues from the provision of advanced e-services from growing regulatory pressure, uncertainty and threat. Also, it aims to self-regulate and self-organise to overcome some of the industrial and systemic barriers in the identity management system sector to the development of such services (Maghiros et al. 2007). Apparently confiding in integrated technological solutions and counting on users' willingness to strike a Faustian deal between provision of personal data and fruition of advanced e-services, industry players fear legal barriers the most. Most world e-service companies in healthcare, finance and retail name "compliance with regulations" as the main challenge in the years ahead (Google 2008).

This concern with compliance is not misplaced. Regulators are paying increasing attention to identity, privacy and trust in online and converging environments (Edwards and Fieschi 2008). Understanding and regulating identity in a ubiquitous information environment is a major driver of the future internet economy (OECD 2008). A number of studies were commissioned by policy makers (OECD, Council of Europe, European Commission) to clarify the economic and legal implications of digital personhood (Rundle et al. 2007), of eID profiling for human rights (Dinant et al. 2008) and of self-regulation in the privacy market (Marcus et al. 2007). These domains let envisage an increasingly complex regulation model of individuals' identity management.

[2] Directive 95/46/EC of the European Parliament and of the Council.

[3] Secure Identity Across Borders Linked; STORK is funded under the ICT Policy Support Programme. See http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=224993

In the European Union, this model begins to extend to consumer policy, as location and service fruition and trust and privacy are seen as prerequisites for the common digital market to come (Kuneva 2008); to human rights policy, in relation to the consequences of advanced profiling techniques (Dinant et al. 2008) and with issues of surveillance in relation to information society security (Hammarberg 2008); to online safety policy, especially in relation with younger users (EDPS 2008b); and to a set of policies regarding the economic impact of networks to come (OECD 2008). If fully sketched, eID may need a grander, more integrated regulatory framework than the one that to date responds mainly to the identity-theft threat (cybercrime), requiring one that ensures smooth services fruition across the member states (interoperability) and that shields people privacy from intrusion and abuse (data protection).

Partly, the increasing complexity is due to the significant identity-related technological developments. The technological referents of eID are growing in number and complexity; the 2008–2009 work programme of the Article 29 Working Party[4] plans tackling open questions related to individuals and search engines, social networking sites, behavioural profiling and data mining (on- and off-line), biometrics, ubiquitous computing and Ambient Intelligence, and Radio Frequency Identification (RFID) (Article 29 Working Party 2008). One recent trend in particular presents challenges for the regulation and management of workable eID models: the rise of Web2.0.

Identity and web2.0

Web 2.0 refers to 'social' e-applications such as social networking services (SNSs), e.g. Facebook), collaborative filtering (Amazon, Last.FM), social bookmarking (del.icio.us), folksonomies (Flickr), social search engines (yoono.com), file sharing (Emule), mash-ups (BBC backstage), and online multi-player games (World of Warcraft). In recent years, Web2.0 has become very popular especially with young Internet users. In Europe, about a third of Internet users engage in some way with Web2.0. Some 10% provide feedback, post comments on blogs and reviews on Amazon. About 10% share contents on Flickr, YouTube. Only around 3% of Internet users in Europe are creating new contents (Pascu et al. 2008).

Web2.0 raises important issues in relation to identity, trust, reputation, co-operation and privacy. One issue relates to identification, as virtually all Web2.0 systems mentioned require simple email ID and password identification. This leads to the multiplication of identification across multiple sites, limited security of transactions based on password identification, with potential for data loss,

[4] The "Article 29 Data Protection Working Party" (set up by Article 29 of European Directive 95/46/EC) is a working party composed of representatives of the data protection authorities in the Member States of the European Union, representatives of the Community's supervisory authorities and one representative of the European Commission. It aims to provide expert opinion from member states to the Commission on questions of data protection, to promote the uniform application of the general principles of the Directive in all Member States, to advise the Commission on Community privacy and data protection measures and to make recommendations to the public and to Community institutions. See http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

impersonation and identity theft as the extreme consequence. Within the sites, plug-ins and applications written by third parties endanger users' privacy (Felt and Evans 2007). Some providers, such as MySpace.com, are currently considering biometric (fingerprint) technology enrolment and validation systems for underage users of SNS (NA 2008). Overall, there seems to be a movement towards increased security and questioning of the portability of secure identity across multiple domains.

Furthermore, certain 'special' characteristics of Web2.0 challenge regulation of behaviour as they are to all effects *cultural markets*. In short, when people come together to share their knowledge, reputation, consumer experiences and tastes, identity becomes negotiable. Establishing identity, the act of making oneself known, becomes socially bound, allowing multiple presentation of the self across heterogeneous platforms (DiMicco and Millen 2007). Identity also becomes relational (you are what you link, purchase, post), becomes portable, as identity data is becoming increasingly portable. Trust subsumed to transactions also becomes portable (my friends' friends are my friends, my friends tastes are my tastes, etc). In these Web2.0 'places', masses of user generated contents (hence identity and trust) are manipulated according to different logics (Thomas 2006). User generated content, the source of *collective intelligence* that most observers consider as a key characteristics of Web2.0 applications is channelled by logics based on proprietary algorithms (Allen 2008). These logics help mould specific regimes of trust, identity and privacy and are perceived differently by different generational cohorts. Examples of these logics span the production / consumption continuum of social computing (see Appendix). In other words, Web2.0 enables distributed systems of trust-making, distributed systems of identity making and complex reputation systems where users interact with rules. The purposeful behaviour of users makes the game a strategic one, even where negative behaviour is discouraged.

Overall, these Web2.0 logics are vicarious both to the legal framework for the fruition of e-services and to the regulation of identity in 'real life'. To these logics people become easily accustomed. These logics shape suggested morphologies of eID, whereby it is more or less convenient to share information about one's tastes, identity, personal behaviour, orientation, and relations as well; these morphologies constrain users' perceptions and behaviour in manifesting identity online (by engaging in the exchange, generation and reception of data flows). Below, we discuss three specific challenges proper to this new environment: personal data proliferation, traceability and unsocial practices.

Personal data proliferation

Unprecedented amounts of user information are generated in countless online and offline interactions, most of which is beyond user control. Less than half of the digital universe related to users is accounted for by their activities—pictures taken, phone calls, emails—while "the rest constitutes a digital 'shadow'—surveillance photos, Web search histories, financial transaction journals, mailing lists" (Gantz et al. 2008, p. 2). If these are systematically harvested, they can return to haunt users along with delivering targeted services via Web and Web2.0 (Story 2008a, b); especially, this may happen when data-points from different sources, such as search engines and Web2.0, are brought together (Zimmer 2008). The Google-Doubleclick

merger may open new scenarios and new legal challenges concerning online 'behaviour tracking'. In short: linking of Internet Service Provider (ISP) data with cookies data, with information from 'social' spaces of search engines lead to an unprecedented amount of collated information about single users. The recent case of Phorm well illustrates this point.[5]

Traceability

The linking of digital context and content to physical location is one of the defining traits of Web2.0 (e.g. geo-tagging, geographical data meshing); in fact, mobile social computing is increasingly seen as the next market trend in the mobile field (Feijoo et al. 2009). A number of emerging technologies, such as location-based services, IPv6, third generation mobile phones and RFID establish even stronger links between physical location and digitised knowledge about people. With the integration of sensors in everyday life, the boundaries between physical and digital space will become increasingly difficult to distinguish (Daskala and Maghiros 2007). Mobile phones and mobility present newer challenges for data protection and eID safety, in relation to highly mobile identity, the mobile being a very personal device, easy to intrude and to track. Surveillance problems will be enhanced by IPv6, which links personal digital devices and information/communications. Privacy problems may arise from the creation of networks to manage billions of tags at global level (e.g. EPCGlobal system).[6] RFID can potentially violate privacy and enable a control of persons (e.g. profiling, verification of tracks, control of geographical position). Overall, the greater dimensionality of digital identity conferred by location and mobility technologies makes it much easier to 'overkill' with digital information: not to use proportionate technologies or minimal data for the aims of the personal identity data processing.

Unsocial practices

New media provide enhanced ammunition for social engineering and phishing (Workman 2008), notwithstanding strong technical security as very often the weak link of the chain is human. Through more or less sophisticated persuasion techniques, the social engineer can persuade people to communicate information which—alone or in combination with further information—can give access to sensitive sources such as bank account and credit card numbers. Increasingly, also, unsocial online practices do not infringe the law, but may create a great deal of discomfort to those on the receiving end. Information from social networking sites is increasingly used as evidence to screen job and university applicants, possibly

[5] Phorm is a company liaising between ISPs and advertisers, data mining user session files to provide advertising companies with intelligence as to users' tastes, to favour the provision of context-sensitive advertising. Although Phorm maintains that its technical arrangements shield users' identity, the compliance of this system with Data Protection law was called into question by the Foundation for Information Policy Research (http://www.fipr.org/080317icoletter.html). Phorm is currently under scrutiny by the UK Information Commissioner regarding issues of Data Protection and EU and national laws regarding pseudonymity and interception (http://ww.ico.gov.uk/upload/documents/pressreleases/2008/phorm_statement.pdf).

[6] See http://www.epcglobalinc.org/home

prejudicing future reputation and career (Bennett 2008); cyber-bullying is on the rise, whereby young and older adults are targeted online and offline (Hammond 2007); cases of suicide in relation to SNS campaign of harassment have been reported (Davies 2007). Harassment involving SNS have been before the courts; in one case, a man was cleared of harassing his ex-girlfriend over Facebook, saying prosecutors had not proven that he used a Facebook friend request to harass (Williams 2008). In another case, a man was jailed after a Facebook friend request he made violated a previous restraining order (Clout 2007). In other words, online actions revolving around the boundaries of digital identity may have significant offline consequences, many of which, however, remain uncharted.

The EU legal framework and eID

This turbulence created by technological developments is, of course, mediated and absorbed by existing regulation. Overall, EU citizens enjoy a significant degree of protection of personal data, privacy and ultimately identity. Personal identity is a constitutionally protected right. It is closely linked to the right to respect for private and family life, as it shields people from unwanted external attention and control (Rodotà 1997). The right to personal identity encompasses two of EU Charter of Fundamental Rights: the right to privacy, which prevents public authorities from privacy-invasive measures unless certain conditions are met, and the right to data protection, which establish conditions under which it is legitimate and lawful to process personal data. In Europe, a number of Directives have created a general and technology neutral system[7] of data protection in all Member States that also protects 'the fundamental rights and freedoms of natural persons' (Directive 95/46/EC, Art. 1).

> "Not only privacy but other rights such as fairness, defence, non-discrimination are to be protected. This vision is especially important in relation to judicial authorities, as in many cases it overlaps and complements other principles enshrined in Article 6 of the ECHR" (Rodotà 1997, pp. 605–606).

National and EU Data Protection institutions monitor personal data processing by public and private institutions and individuals can access Courts to settle issue related to the infringement of their data protection rights.

However efficient technology neutral regulation may be, identity-protection legislation is tested by rapid technological developments and social change, as novel issues and dimensions that remain elusive to 'hard' legislation (Daskala and Maghiros 2007). The right to identity implies the "correct representation in each context" and also an "integral representation of the person" (Rodotà 1997, pp. 605–606), also to be intended in a diachronic sense. However, specifically in relation to Web2.0, identity is no longer conceivable as a pre-existing, static datum but rather as a dynamic, ongoing process of manifestation of the self in multiple transactions, interactions and exchanges of data. While strictly speaking digital identity is information about users of an information system and the techniques for their identification (usually protected with an authentication system), in a broader sense it

[7] http://www.edps.europa.eu/EDPSWEB/edps/pid/17

corresponds to the on-line or virtual identity of a person. Especially for young people, 'being digital' is more than the mere electronic processing of personal data, it encompasses a distinct online life, often implying multiple different digital identities (for instance through multiple profiles on social networking sites).

As such, digital identity can be endangered by misrepresentation, de-contextualisation, non-transparent flow of information. It can be distorted and fragmented, as personal data are stored in several databases that provide a partial and potentially endangering picture of the person reduced to the sum of its electronic projections (Rodotà 2004, p. 141). More in general, the legal concept of personal identity *misrepresentation* takes on new nuances that may be difficult to forecast and regulate; digital identity can be under-represented (Frean 2008), over-represented (time-wise), otherwise represented, presented out of context, stolen, concealed via anonymity and pseudonyms (Campbell 2007; Koops 2005; Leenes et al. 2006). Although these issues may not be new, the complexity of data protection in relation to digital identities and the uncertainty regarding its application and enforcement are. We flag here four problematic areas of the current regulatory framework: complexity, uncertainty, responsibility and oversight.

Complexity

Firstly, complexity makes the problem qualitatively different. What is 'personal' remains to-date elusive in relation to digital environments. There is a clear problem with contextualising what data requires protection, as law "does not distinguish between personal data that affects or does not affect private life" (Daskala and Maghiros 2007, p. 27). The distinction is important enough to merit detailed discussion by Article 29 (Article 29 Working Party 2007).[8] Data protection legislation currently struggles to regulate digital tracks and trails, in truth digital fragments of identity, which are left behind unintentionally or unknowingly, such as, for instance, the IP address of origin of users. When it allows tracing a user, Article 29's opinion is that it constitutes personal data, therefore falling under the provisions of data protection legislation (Hogben 2007). Other instances remain more controversial. Unclear domains include terms searched for in search engines. It is unclear whether search terms are to be considered as data to be protected and who the actual owner of such personal data is.[9] There is lack of clarity concerning behavioural information stored in cookies and information provided for social purposes and 'relational' information, specifically in SNS. All these are remainders of digital transactions that the user has no knowledge about, awareness of or control on, often resulting from the design of the transaction under scrutiny.

Uncertainty

Secondly, there is a significant problem with uncertainty. The growth of person-related information and user generated content make compliance and control more

[8] Established under Article 29 of EU Directive 95/46/EC, it comprises national Data Protection Commissioners from EU member states.

[9] An Article 29 opinion on Search Engines and Privacy was released on 4 April 2008.

difficult (Gantz et al. 2008; Pascu 2008).Whether identity data controllers should be trusted has been recently questioned, when an increasing number of data breaches are not reported to customers and potentially sensitive data are disclosed to third parties (BBC 2008). Also, checking compliance with privacy and personal data rules in the digital space is problematic, as often there is not enough transparency about the outcome of such activities (Daskala and Maghiros 2007). Although institutions are required to perform compliance audits regarding data protection and prior checks in relation to privacy impact (audits tools are increasingly made available by national Data Protection authorities)[10] there is no guarantee that audits have been performed thoroughly and that results are valid and reliable. National Data Protection officers are confronted with the gigantic task to monitor hundreds of thousands of delegated data controllers, private and public, within their generally wider remit which goes far beyond a bureaucratic interpretation of the Data Protection Directive (Thomas 2008).

Responsibility

It is becoming increasingly harder to identify responsibility in complex identity environments, due to the large *control gap* between data subjects and data controllers. Users have limited control on their data when these are uploaded to a electronic database system and transferred trans-nationally[11] and limited control over their data and connections in relation to data merging from different sources (Kirkpatrick 2008). While about 70% of the online information is created by individuals, companies are responsible for the security, privacy, reliability and compliance of 85% of the digital universe (Gantz et al. 2008). Even the deletion of personal data and trails left is problematic (Hogben 2007). 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. The issue of whether people can rightfully 'export' their online social graph (their online friends, tastes, writings) to other sites in currently unclear. Overall, it is unclear to what extent people can be held accountable for the accuracy of their digital identity, whether one may posit a burgeoning duty of care of one's digital identity (e.g. maintain it safe) or to maintain an accurate digital identity, alongside established rights of protection by institutions. In other words, whether users are to some extent data controllers of their digital identity.

Oversight

Furthermore, as oversight ensures efficacy of any regulatory framework, further thought should be devoted to identifying what is the most appropriate supervision source. The recent case of SNS regulation in Britain highlights a number of competence criss-crosses, whereby the communication watchdog Ofcom[12] is

[10] E.g. http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf

[11] The French Data Protection Authority (CNIL) fined in May 2007 Tyco Healthcare France € 30,000 for unlawful cross-border transfers of human resources data to Tyco's U.S. headquarters.

[12] Ofcom is the UK national telecommunications regulator, see http://www.ofcom.org.uk/.

concerned with safety and privacy of media contents of the sites, the Home Office is concerned with safety for younger children and safety guidelines, the national Information Commissioner's Office is concerned with data protection, identity and privacy matters, and courts are concerned with all that falls between the lines. Furthermore, member state Data Protection Authorities operate in very different business and political cultures and sensitivities, witness the Phorm case in Britain, the biometric passport case in France,[13] and the Italian tax disclosure case.[14] At EU level, the competence boundary between European Data Protection Supervisor and European Ombudsman has been contentious for some time, partly addressed by a memorandum of understanding (European Ombudsman & European Data Protection Supervisor 2007). Furthermore, EDPS is now involved in assessing the privacy and personal data consequences of project funded under the Seventh Framework Programme for Research and Technology Development (*FP7*); the main aim is the promotion and reinforcement of the 'privacy by design' in all stages of Information Technologies EU-funded research (EDPS 2008a).

Is there a need for a new regulatory framework?

So far, we have identified a number of key challenges for eID. These revolve around the need to re-assess identity to arrive at effective solutions to the turbulence introduced by new developments. Overall, the principle challenge for regulators is to enable the effective management of one's own and, for businesses, one's customers' identity in a climate that tends to fragment its definition, use and regulation. Not surprisingly, a key research challenge identified in the European Commission vision of Future Internet relates to "Managing and protecting the 'identity' of billions of networked persons, devices, "things", services and virtual entities connected in the Future Internet" (European Commission 2008b, p. 111).

To assist policy-making in managing and protecting eID, a more integral approach to the problem may be required, one that takes into account users' identity across platforms and life activities. Research funded by the European Commission under the FP7 IST programme include projects that favour a holistic view of identity management, such as PRIMELIFE, SWIFT and PICOS[15] (European Commission 2008a). Primelife aims to "fundamentally understand privacy-enhancing identity management 'for life' (practical life, throughout life & beyond), to bring privacy to the Web and its Applications, and to develop and make tools for privacy friendly identity management widely available—privacy live". These are valuable, necessary R&D steps towards developing technologies that factor in privacy and personal data protection at the earliest possible stage of design.

However, we argue the need to move beyond discussions about privacy and move into full fledge discussion of identity in relation to eID. The legal concepts of

[13] See http://www.edri.org/edrigram/number6.10/cnil-biometric-passports

[14] See, jointly, http://www.garanteprivacy.it/garante/doc.jsp?ID=1519208 and http://news.bbc.co.uk/2/hi/europe/7376608.stm

[15] SWIFT, Secure Widespread Identities for Federated Telecommunications, http://www.ist-swift.org; PICOS, Privacy and Identity Management for Community Services, http://www.picos-project.eu; PRIMELIFE, Privacy and Identity Management In Europe for Life, http://www.primelife.eu/.

privacy and *data protection* struggle to regulate citizens' conduct in the new information space. Both are remote from people's practical understanding of the new environment. They are subject to a well-known paradox (recently, see The Gallup Organization 2008), whereby people declare to value them highly instants before selling them cheaply. They are hard to define and enforce, both legally and practically, in the new complex information space.

Of course, privacy is indispensable to protect the *core of citizens' identity*, *sensitive data* or the *safety of users*. People possess an understanding of privacy as a defensive right to control access to one's own person and personal information (Palen and Dourish 2003). Privacy in this sense helps one define the criteria that would dictate 'opacity' of data (Gutwirth 2002) while data protection is defining the conditions for the 'transparency' of data; data protection is indispensable in ensuring that personal data are processed fairly, efficiently, to the benefit of the user. The Data Protection Directive framework is successful in ensuring a technology neutral high level of protection of personal data (European Commission 2007).

However, if privacy and data protection are stretched to intend and regulate zones of personality that do not require or even invite opacity and procedural fairness, such as an increasing array of citizen online and offline activities, then they display visible stretch marks. The current regulatory framework is inefficient in dealing systematically with the enlarging digital data shadow harboured by the Internet; the challenges faced by Data Protection authorities in patrolling data controllers' behaviours point to the natural, one-sided 'opacity' of a growing Internet. Further regulatory mechanisms could prove beneficial in ordering the invisible as well as the visible transactions involving personal data.

We propose an alternative eID regulation regime to privacy and data protection, one which we name the *Autonomy* regulatory framework; Autonomy places different emphasis on the principles, object, and focus of eID regulation. Data protection and privacy are not discussed here, as they have been discussed extensively elsewhere in this journal issue.

In as much as users' identity is tied to *where they go*, *who they are with*, *what they do*, *who they know*, and *what they think*, the regime has multiple advantages for the understanding and regulation of eID in turbulent times. Normatively, the new regime stresses the need to regulate behaviour, rather than procedures or access. Away from the privacy paradox, what deserves attention is users' actual behaviour rather than intentions. Overall, the *Autonomy* regime may be considered as an enactment of 'decisional privacy', whereby citizens can take decisions for themselves and act on those decisions free from external interference, truly creating a space for autonomous action (Rössler 2005). It underlines the importance of user control, transparency and responsibility in relation to personal data in the new environment; these facets of identity have been long disregarded in the discussion of eID. This does not mean focusing only on use, quite the contrary; attention is required to structural properties of a regime based on the praxis of identity, on increased transparency and on distributed responsibility.

Firstly, regulation is required in the lived domain of actual activities carried out online which have identity implications. That of identity is a special market, one which requires closer scrutiny of a larger number of variables. In the new environment, it is hardly sufficient to balance security and privacy, as convenience, trust, reputation, location,

transparency and responsibility are crucial variables. The evolution of eID will ultimately depend on user negotiation and acceptance (Backhouse and Halperin 2007) of a complex model of regulation of their online and offline eID behaviours. We need to address the user perspective and regulate extant behaviour as society's values limit the practical viability of identity management systems (McKenzie et al. 2008). The difference between stated preferences and actual practice in relation to privacy has been documented over time in numerous studies (Acquisti and Varian 2005; Gunther and Spiekermann 2005).

Secondly, regulation needs to increase the overall transparency of the new environment, balancing the clear imbalance in favour of data controllers. Transparency is in line with the call for greater transparency in public policymaking and life,[16] and is consistent with developments in ubiquitous computing (Hildebrandt and Koops 2007). Also, it works in relation to the configuration of identity in relation new internet developments such as the Semantic Web and the Internet of things. Two-way transparency and reciprocity may enhance users' experience by reducing the gaps between privacy, personalization and transaction discrimination, beyond the information privacy paradigm where this rapprochement has been recently proposed (Acquisti 2008). Finally, increased transparency resolves the tension inherent in the practical application of different principia of EU regulation: freedom of information and data protection (Hustinx 2004).

Thirdly, regulation needs to harness responsibility (according to some: accountability). The autonomy regime proposed is underpinned by a strong ethos of personal responsibility, which is in line with recent thinking about personal data portability, self-regulation of online experience, alternative methods of dispute resolution and, overall, much greater user control on their own data and experience (LaRose et al. 2008). More responsibility may have positive behavioural effects. Young people, who display little to no relationship between online privacy concerns and information disclosure (Tufekci 2008), adapt intuitively in privacy-oppressive environments by over-informing their peers about their whereabouts, thinking and sexual preferences. They adjust profile visibility and use nicknames but do not restrict information within their profile, with little regard for issues of persistence, searchability, and cross-indexability (Tufekci 2008). The trick is thus to envisage (design, regulate) identity environments that capitalise on such propensity to disclose, bargain, transact. This may have positive economic externalities in business markets. By stressing accountability, open declarations and users' duties, *responsibility* reduces some of the burden that derive from sub-optimal game results in an environment where privacy would limit the flow of information.

Conclusions

In this paper we argued that technological developments such as Web2.0 pose novel challenges for the regulation of eID. We identified and discussed four such challenges: complexity, uncertainty, responsibility and oversight. Policymakers are only beginning to address the consequences of these challenges for consumer protection, data

[16] Transparency Initiative, http://ec.europa.eu/commission_barroso/kallas/transparency_en.htm

protection and privacy, safety and economic growth and competition. We claimed that industrial players are increasingly vocal on the issue of privacy; there is a perceivable movement towards greater industry co-ordination aiming at shielding large prospective revenues of eID-enabled services from increasing and uncertain regulatory pressure. This is especially important with an incoming European Commission and forthcoming European Parliamentary Elections (June 2009).

In this context, we asked whether there is the need for a new regulatory framework that both preserves users' identity and enables the provision of advanced services. We examined the capacity of the current regulatory framework to absorb this turbulence, and found it wanting. We thus advanced a novel model of eID regulation, the Autonomy regulatory framework, that may help policymakers create an identity-preserving, transaction-friendly eID environment.

Overall, effective regulation of the new environment requires putting in place a range of market-enhancing rather than market-limiting regulations in relation to advanced interactions in complex, multi-layered digital spaces. Although (or because) eID industry integration is proceeding at full steam on the privacy track, led by market players to remove some of system barriers to eID, much more remains to be done at individual and project level (Maghiros et al. 2007). What may be required is a set of identity management principles to guide users and companies in an environment in which the application and policing of data protection principles is increasingly problematic. Possibly, one could take as a point of departure OECD privacy principles as received in the Data Protection Directive. Obviously, significant research is required which envisages and examines the behavioural, legal and economic consequences of any such alternative regulatory model. Depending on the results of research based on a relevant set of concepts to the emerging new environment—user-centricity, transparency and responsibility—a policy mix of soft-regulation, *transparency by design*, self-regulation, semiotic guidance, guide lining, safeguarding, cross-regulation or other regulatory mechanisms of the eID economy may be advisable.

Acknowledgements The views expressed in this paper are the authors' and do not necessarily reflect those of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of the information and analysis presented.

Appendix

Web2.0 application	*Logic*
eBay	Consumer-to-consumer auction site based on user-generated reputation feedback and comments; identity is chosen and managed, often strategically, by the seller; recently eBay has tried to tag real-life information to the seller, to improve trust.
Amazon	Market site where users rate and provide feedback on different products; this is complemented by behavioural tracking of users' purchase behaviour and attention; identity is implicit in purchasing/browsing behaviour (culture of consumption) and further commoditised by the website's algorithms.

PatientOpinion	Heath system rating site, where patients pass comment on or rate the performance of public health system practitioners and structures; identity in this case is related to personal medical information shared with other users of the system; there are clear concerns for professionals' privacy and reputation.
Radio 2.0—Last FM	A musical taste-sharing system. More user-centred, it uses a recommendation system to build profiles of each user's musical taste based on songs listened to, linked to a webpage. User can tag, annotate, and share their tastes via social networking features.

Other Web2.0 platforms such as Linkedin, social networking sites (Facebook, Myspace), WIKIs, Technorati and GNU (communities of software developers) operate alongside different logics, concerning identity, trust and privacy.

References

Acquisti A. Identity management, privacy, and price discrimination. IEEE Security & Privacy. 2008;6:46–50.

Acquisti A, Varian HR. Conditioning prices on purchase history. Mark Sci. 2005;24(3):367–81.

Allen M. Web 2.0: an argument against convergence. First Monday. 2008;13(3). Available from <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2139/1946>.

Article 29 Working Party. Opinion 4/2007 on the concept of personal data. Brussels; 2007.

Article 29 Working Party. Work programme 2008–2009 (No. 00393/08/EN, WP 146). Brussels; 2008. Available from <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp146_en.pdf>.

Backhouse J, Halperin R. A survey on citizen's trust in ID systems and authorities. Fidis Journal. 2007;1 (Online). Available from <http://journal.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf>.

BBC. Firms 'give out' customer details. 2008. Online. Retrieved 23 June, 2008, from http://news.bbc.co.uk/2/hi/uk_news/7468491.stm

Bennett R. Plea to ban employers trawling Facebook. The Times. 2008. Available from <http://technology.timesonline.co.uk/tol/news/tech_and_web/article3613896.ece>.

Campbell D. Letter from Duncan Campbell (Fifth Report—Personal Internet Security). London: UK House of Lords Select Committee on Science and Technology; 2007. Available from <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165we07.htm>.

Clout L. Man jailed over Facebook message. The Telegraph. 2007. Available from <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/10/04/nface104.xml>.

Daskala B, Maghiros I. Digital territories—towards the protection of public and private space in a digital and Ambient Intelligence environment (Report No. 22765 EN). Seville: JRC IPTS; 2007. Available from <http://ftp.jrc.es/eur22765en.pdf>.

Davies C. Anguish for mother of suicide girl as 'cyber-tormentor' escapes the law. The Observer. 2007. Available from <http://www.guardian.co.uk/world/2007/nov/25/usa.news>.

DiMicco JM, Millen DR. Identity management: multiple presentations of self in facebook. Paper presented at the 2007 international ACM conference on Supporting group work. Session: Social networking Sanibel Island, Florida, USA; 2007. Available from <http://doi.acm.org/10.1145/1316624.1316682>.

Dinant J-M, Lazaro C, Poullet Y, Lefever N, Rouvroy A. Application of convention 108 to the profiling mechanism. Some ideas for the future work of the consultative committee (T-PD) (No. T-PD(2008)01). Strasbourg: Council of Europe, T-PD; 2008. Available from <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Documents/Reports_and_studies_by_Experts/CRID_Profiling_2008_en.pdf>.

EDPS. The EDPS and EU research and technological development (Policy paper). Brussels: EDPS; 2008a. Available from <http://edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf>.

EDPS. Opinion on the proposed multiannual community programme on protecting children using the Internet and other communication technologies. Brussels: EDPS; 2008b. Available from <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-06-23_Children_Internet_EN.pdf>.

Edwards C, Fieschi C (Eds.). UK confidential. London: DEMOS; 2008. Available from <http://www.demos.co.uk/files/UK%20confidential%20-%20web.pdf>.

European Commission. Communication from the commission on the follow-up of the work programme for better implementation of the data protection directive (No. COM(2007) 87 final). Brussels: European Commission—DG JLS; 2007. Available from <http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf>.

European Commission. Challenge 1, objective 1.4: "Secure, dependable and trusted infrastructures" (Work Programme 2007–2008. Synopsis of R&D Projects.). Brussels: EC DG INFSO; 2008a. Available from <http://cordis.europa.eu/fp7/ict/security/projects_en.html>.

European Commission. The future of the internet. A compendium of European projects on ICT research supported by the EU 7th framework programme for RTD. Brussels: EC—DG INFSO; 2008b. Available from <http://cordis.europa.eu/fp7/ict/programme/futint/>.

European Ombudsman & European Data Protection Supervisor. Memorandum of understanding between the European Ombudsman and the European Data Protection Supervisor. Official Journal of the European Union, C 27/21 Sess 2007. Available from <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_027/c_02720070207en00210023.pdf>

Feijóo C, Maghiros I, Bacigalupo M, Abadie F, Compañó R, Pascu C. Content and applications in the mobile platform: on the verge of an explosion. Seville: Institute for Prospective Technological Studies; 2009.

Felt A, Evans D. Privacy protection for social networking APIs. Charlottesville: University of Virginia; 2007. Available from <http://www.cs.virginia.edu/felt/privacy/>.

Frean A. Every child in school numbered for life. The Times. 2008. Available from <http://www.timesonline.co.uk/tol/news/uk/education/article3359931.ece>.

Gantz JF, Chute C, Manfrediz A, Minton S, Reinsel D, Schlichting W, et al. An updated forecast of worldwide information growth through 2011 (IDC White Paper). Framingham, MA: IDC; 2008. Available from <http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf>.

Google. Annual Google communications intelligence report (Google white paper No. February 2008). Mountain View, CA: Google; 2008. Available from <http://www.google.com/a/help/intl/en/security/pdf/cir_08.pdf>.

Gunther O, Spiekermann S. RFID and the perception of control: the consumer's view. Commun ACM. 2005;48:73–76.

Gutwirth S. Privacy and the information age. Oxford: Rowman & Littlefield; 2002.

Hammarberg T. Strong data protection rules are needed to prevent the emergence of a surveillance society (Viewpoint No. 26 May). Strasbourg: Council of Europe, Commissioner for Human Rights; 2008. Available from <http://www.coe.int/t/commissioner/Viewpoints/080526_en.asp>.

Hammond, E. No place to hide. Financial Times. 2007. Available from <http://www.ft.com/cms/s/0/f6182bc8-85e4-11dc-b00e-0000779fd2ac.html>.

Hansen M, Schwartz A, Cooper A. Privacy and identity management. IEEE Security & Privacy. 2008;6(2):38–45.

Hildebrandt M, Koops B-J. A vision of ambient law (Deliverable No. D7.9). Tilburg and Brussels: FIDIS Network; 2007. Available from <http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf>.

Hogben G. Security issues and recommendations for online social networks (ENISA Position Paper No. 1). Heraklion, Crete: Enisa; 2007. Available from <http://enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf>.

Hustinx PJ. The role of the European Data Protection Supervisor in the EU Framework for Data Protection. Paper presented at the Polish Parliament, Warsaw, 26 May 2004. Available from <http://www.giodo.gov.pl/plik/id_p/77/j/en/>.

Kirkpatrick M. Is Google's social graph API a creeping privacy violation? 2008. From http://www.readwriteweb.com/archives/google_privacy.php

Koops B-J. A survey on legislation on ID theft in the EU and a number of other countries (Deliverable No. D5.1). Tilburg University: FIDIS Network; 2005. Available from <http://www.fidis.net/resources/deliverables/forensic-implications/>.

Kuneva M. Key challenges for consumer policy in the digital age (Speech No. 08/347). London: Roundtable on Digital Issues; 2008. Available from <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/08/347&format=HTML&aged=0&language=EN&guiLanguage=en>.

LaRose R, Rifon NJ, Enbody R. Promoting personal responsibility for internet safety. Commun ACM. 2008;51(3):71–76.

Leenes R, Graux H, Meints M, Rost M, Zuccato A, Delaitre S, et al. ID-related crime: towards a common ground for interdisciplinary research (Deliverable No. D5.2b). Tilburg University: FIDIS Network; 2006. Available from <http://www.fidis.net/resources/deliverables/forensic-implications/int-d52b000/>.

Liberty Alliance. Release of IAF and IGF drives standardized identity assurances and policy-based data and privacy protection across identity-enabled applications and networks; 2008. Retrieved 24 July 2008, from http://www.projectliberty.org/liberty/news_events/press_releases/liberty_alliance_marks_policy_and_privacy_milestone_for_identity_enabled_enterprise_and_web_2_0_applications

Maghiros I, Rotenberg B, Elliott J, Birch D, Ford M, Whitcombe A. Overcoming barriers in the EU Digital Identity Sector (JRC Scientific and Technical Reports No. EUR 23046 EN). Sevilla: EC JRC IPTS; 2007. Available from <http://www.jrc.es/publications/pub.cfm?id=1533>.

Marcus JS, Carter K, Robinson N, Klautzer L, Marsden C, Reidenberg J, et al. Comparison of privacy and trust policies in the area of electronic communications. Bad Honnef: wik-Consult/RAND Europe, CLIP/CRID/GLOCOM; 2007. Available from <http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/final_report_29_02_08.pdf>.

McKenzie R, Crompton M, Wallis C. Use cases for identity management in E-government. IEEE Security & Privacy. 2008;6(2):51–7.

NA. MySpace to consider additional protection measures. Biom Technol Today. 2008;16(2):12. Available from <http://www.sciencedirect.com/science/article/B6W70-4RW4JMJ-R/2/b7f4e82fa94d194c597938dda7f356e2>.

OECD. The Seoul declaration for the future of the Internet economy. Seoul: OECD Ministerial meeting; 2008. Available from <http://www.oecd.org/site/0,3407,en_21571361_38415463_1_1_1_1_1,00.html>.

Palen L, Dourish P. Unpacking "privacy" for a networked world. Paper presented at the SIGCHI conference on Human factors in computing systems; 2003.

Pascu C. Social computing: a monitoring and trend analysis (IPTS Exploratory Research on Social Computing No. Draft Deliverable 1). Seville: European Commission JRC; 2008.

Pascu C, Osimo D, Turlea G, Ulbrich M, Punie Y, Burgelman J-C. Social computing: implications for the EU innovation landscape. Foresight. 2008;10(1):37–52.

Rodotà S. Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali. Riv Crit Dirit Priv. 1997;4.

Rodotà S. Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione. Rome-Bari: Laterza; 2004.

Rössler B. The value of privacy. Cambridge: Polity; 2005.

Rundle MC, Blakley B, Broberg J, Nadalin A, Olds D, Ruddy M, et al. At a crossroads: "Personhood" and the digital identity in the information society (STI Working Paper No. 2007/7). Paris: OECD; 2007. Available from <http://www.olis.oecd.org/olis/2007doc.nsf/ENGDATCORPLOOK/NT00005D0E/$FILE/JT03241547.PDF>.

Squicciarini A, Mont MC, Bhargav-Spantzel A, Bertino E. Automatic compliance of privacy policies in federated digital identity management (HP Technical Report No. HPL-2008-8). Bristol: Hewlett-Packard; 2008. Available from <http://www.hpl.hp.com/techreports/2008/HPL-2008-8.pdf>.

Story L. How do they track you? Let us count the ways; 2008a. Online. from http://bits.blogs.nytimes.com/2008/03/09/how-do-they-track-you-let-us-count-the-ways/?em&ex=1205294400&en=8662840-b2e462d04&ei=5087%0A

Story L. To aim ads, web is keeping closer eye on you. N Y Times. 2008b. Available from <http://www.nytimes.com/2008/03/10/technology/10privacy.html?_r=2&hp=&oref=slogin&pagewanted=all&oref=slogin>.

The Gallup Organization. Data protection in the European Union—citizens' perceptions (Flash Eurobarometer Series No. 225). Brussels: EC—DG JLS; 2008. Available from <http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf>.

Thomas S. The end of cyberspace and other surprises. Convergence. 2006;12(4):383–92.

Thomas R. Freedom of information and privacy—the regulatory role of the information commissioner. London, Centre for Regulated Industries: ICO; 2008. Available from <http://www.ico.gov.uk/upload/documents/library/freedom_of_information/notices/cri_lecture_jan08.pdf>.

Tufekci Z. Can you see me now? Audience and disclosure regulation in online social network sites. Bull Sci Technol Soc. 2008;28(1):20–36.

Williams C. First 'Facebook harassment' defendant cleared—friend request not proved. The Register. 2008. Available from <http://www.theregister.co.uk/2008/03/27/facebook_birmingham_harassment_cleared/>.

Workman M. Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. J Am Soc Inf Sci Technol. 2008;59(4):662–74.

Zimmer M. The externalities of search 2.0: the emerging privacy threats when the drive for the perfect search engine meets web 2.0. First Monday. 2008;13(3). Available from <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2136/1944>.