EUROPEAN COMMISSION
JOINT RESEARCH CENTRE

Institute for Prospective Technological Studies
Information Society Unit

Minutes from the eId and Law Workshop
Regulatory and legal aspects of electronic identity

Brussels, 15 May 2009
Avenue de Beaulieu 25
Building BU25, Room 0/S 5

Participants (participants' initials used in text)

Laurent Beslay	European Data Protection Supervisor
Anna Buchta	EC DG INFSO B1
Ian Brown	Oxford Internet Institute, UK
Ramón Compañó	EC DG JRC IPTS
Jos Dumortier	University of Leuven, Belgium
Anssi Hoikkanen	EC DG JRC IPTS
Michal Hrbaty	EC DG INFSO C1
Samoera Jacobs	Fedict, Belgium
Gloria González Fuster	VUB, Brussels, Belgium
Ronald Leenes	University of Tilburg, Netherlands
Wainer Lusoli	EC DG JRC IPTS
Yves Poullet	University of Namur, Belgium
Giovanni Sartor	European University Institute, Florence, Italy
Dirk van Rooy	EC DG INFSO F5
Wout van Vijk	EC DG INFSO F5
Thilo Weichert	ICPP Kiel, Germany

Objective of the Workshop, *A. Hoikkanen, IPTS*

Roundtable introduction by all participants

Session 1: Definition of the Problem

Background on the regulation challenges, *W. Lusoli, IPTS*

Trends, drivers and challenges to current regulation. Experts addressed the following questions:

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

J. Dumortier

JD mentioned a project concerning interoperability he is running at present and a project related to health. There is a need for coherent, structured discussion in the field of identity (mentioned initiatives in the field, including FIDIS, MODINIS); there is a need for clear terminology and focus, a common language. Some problematic concepts of this type include identity, identifiers, and partial identities. Additionally, it is *dangerous* to define identity in abstract terms, without bedding down, as different rules apply in different contexts, pending practical implementation in private and public sector (as in the case of health). JD's overall impression, supported by evidence, is that if we take a general view, 'law does not deal with identity per se' (this is not true, however, if we move down to specific applications and fields). Therefore stating the need for a reform of the regulatory framework may be *dangerous*: this needs time to reach down, it is counterproductive to constantly modify and criticise current regulation, and technological neutrality is necessary. What may be required is a sort of translational legal science, whereby abstract principles are made more understandable in practice by integrating perspectives, and possible solutions, from other domains (JD gave an example of how this can be done from the medical domain).[1] In the case of eId, this would imply, looking at cryptography on the one hand and at value embedded design on the other hand (as an example of the translational paradigm of combining different perspectives; for more details see the attached link).

I. Brown

IB is involved in many studies concerning eId, including a study for DG INFSO, a study for JLS and several studies for the UK government. IB took a governmental perspective and described the extent to which public authorities in the UK handle citizen personal data (a 'database state'). States are not only controlling citizens, government behaviour may spread into business; through its purchasing power and through demand side regulation, the state has the capacity to dictate de facto standards in relation to personal data handling (and setting a moral precedent based on the following argument: we have more data than we need, but we will use them appropriately). However, it is generally unclear what are the benefits for the citizens of increased surveillance; there is limited evidence of the impact of these technologies on security (especially in the case of national security, as profiling is not a reliable method for predicting rare events), but also in other fields, the impact of increased surveillance needs to be measured. Conclusions from his presentation were that the UK is a model for how not to do e-government; it is dangerous to allow large centralised databases to proceed in the hope that they will later be ruled illegal (as has happened in a few cases); and governments need to build privacy into systems by design at a much earlier stage.

---

[1] http://en.wikipedia.org/wiki/Translational_medicine

R. Leenes

There is a distinction between the state-allocated identity, which is valid and useful for identification and authentication, and the socially emergent, multiple identity, which has to do with representation of the self. The former can be referred to as eId, the latter as eId (note the use of capital letters). Two projects that embed these logics are STORK and Primelife, which describe different logics, lessons and challenges. These include profiling, data protection of interoperable government-allocated identities and, importantly, the fact that governments are pressing on with their plans in the face of increasing evidence of technical problems (both interoperability and "hard" technical problems). There are significant issues in implementing interoperable eId-eId systems in terms of content (When to ask for it? How long should it be valid for) and in terms of relying party information (how much, in what language?).[2] Also, liability and responsibility are unclear outside the state's border (and in two and multi-sided markets, for eId). RL also mentioned the fact that people don't have a single identity, but a number of separate, partial, identities, and people want to keep their partial identities separate from each other, given that identities represent different characteristics of theirs. RL also argued that profiles are a part of a person's identity. Furthermore, there are issues with incrementalism (incremental development of technology, which limits innovation because you follow a certain track of technological development instead of questioning first principles), data maximisation rather than minimisation, and fragmentation of the systems in use.

G. González Fuster

GGF touched upon and further specified some of the issue already emerged in the discussion, especially in relation to the fitness of the data framework and its applicability across borders. Moreover, there is lack of clarity concerning the role of supervisors outside their national remit, and an almost complete lack of research on data protection rights across borders. Further, data protection authorities have different access mechanisms, there are significant differences in the way national legislation posits access in specific domains / in relation to specific activities (supporting JD's point); in addition, data protection authorities are not responsive to user-generated challenges and feedback from non-national interested parties. This is linked to the question of citizen trust in the system (that is again different). This further leads to the question whether there is a need for a more consistent European approach in relation to practical privacy and data protection issues.

G. Sartor

GS began with a mention of the fundamental *right* to identity, i.e. the right to be identified as a particular individual and the right not to be misrepresented. Identity has a direct impact on trust, because you do not always know the true identity of your counterpart in a given transaction. Trust and reputation are crucial in new environments, not just to ensure compliance with regulation. Service-oriented architectures (SOA) and Web3.0 will create new challenges to regulation, as they will confer systems ways to identify 'on behalf of' owners. Both trends exacerbate web2.0 trend of data maximisation, rather than minimisation.[3] This growing tension also applies to other 'identity' principles, such as purpose and unlinkability, which become more complex to manage in such environments; one possible solution is the embedding of the principles directly in the new architectures to come. In this respect, one important problem is personal data fragmentation; fragmentation is both a resource (if it enables privacy and enables limited identities) and a challenge (as it may create market dynamics of oligopoly on people's identity and de facto standards).This led to a discussion of centralisation vs. decentralisation: we generally assume that decentralisation is better (safer, more

[2] This resembles Google's current stance on maximising transparency in online advertising.
[3] FIDIS work on profiling argues the same case.

efficient, etc.), for instance due to a smaller likelihood of the system being abused later on if there are several different stakeholders, but this is not necessarily the case in practice.

T. Weichert

TW touched upon many of the points discussed by other participants. In addition, identity theft and other mishaps / misrepresentation of one's privacy and personal data (profiling, dossiering, and lack of purposefulness) are important challenges not mentioned so far. Correct regulation of eId does not only need to capitalise on opportunities, but also help avoid risks. In this respect, privacy by design implementations is a solution. TW stressed the importance of data minimisation, both through technological and legal means. More generally, we need to posit the idea of 'identity protection' as a regulating principle; does identity protection exist, and does it need to be regulated. In this case, there is a need to understand whether identity protection pertains to member states or to the EU, as there seem to be competing and overlapping areas of competence.

Y. Poullet

There is a need for a typology of eId and a structured discussion about the risks of different identifiers. The major threat in the future will be coming from identity being linked to objects, raising new issues concerning what is personal data, and what is personal identity data (Internet of things as a challenge). In this respect, context will matter even more than today (here converging with JD). A second challenge relates to infomediaries: private gatekeepers (such as the ISPs, Google, Facebook) of people's personal data that have a significant degree of control eating into areas which were previously opaque (such as the case of nominal e-ticketing, in which identity tags are attached to transactions that were previously anonymous). These gatekeepers have an overview of how you act with different companies and Internet sites and in different contexts. Anonymity, one underlying principle of privacy, has long been recognised as a social value. YP emphasized that even though data minimisation is important, we must go beyond: more possibilities for anonymous transactions must become available than there currently are. On the one hand, we need mechanisms that allow 'switching off' identity. On the other hand, this increasing intrusion invites regulatory action concerning companies' value propositions, which need to be transparent and the benefit of which should be clearly stated and measurable (linking to IB thinking). This should be well received by companies, as what they really care about is what we want, not who we are.

Roundtable discussion: definition of the problem

- There are at least **two ways of understanding eId**, state-allocated and user-chosen (but mediated by the industry) (RL, others); there is a need for further definition of terms, focus, what is meant by identity (JD), there is no common language across sectors (one would be needed). The problem s compounded by policy-makers' misunderstanding of the issue, linked to a generational dimension.
- These are linked to **two different understanding of identity rights** (if any exist, independently): the right to be identified (and the limits of it: privacy and data protection); and the right of one person's identity not to be misrepresented (the more challenging novelty). (GS) The claim of the existence of an underlying right to identity is far more complex for data that is not controlled by the individual (e.g. by governments and companies) and that is not unique (proliferation). Correct representation (contextual integrity), based on autonomy, may be the underlying principle in both circumstances.
- Experts mostly discussed the first perspective, rather than the second. There is an agreement that **eId will drive eId**. Argument is that however much data governments hold does not matter, what matters is the way data is used (i.e. according to OECD principles). The main problem is the **application** of the

principles underlying different pieces of legislation (minimisation, proportionality, unlinkability), as even the systems being considered and designed today clearly do not conform to them. For instance, personal data centralisation / fragmentation are both a problem and a solution; there is a need to find a balance between identity efficiency and protection in scalability. The 'privacy by design' approach is a possible solution in this respect (IB). There are **increasing monopolies** in the eId market, however **without single eId market regulation**. Experts argued that the Commission needs to make sure that MS and EU institutions are dealing with citizens' data correctly and transparently, as the only regulating bodies. Companies start making the same argument, nowadays (data availability does not matter); but are businesses getting the same level of scrutiny? It is also important to discuss which identity is used in which situation; e.g. private/public might be one useful distinction (RL), and the data you should provide should most likely be considered your personal property (GS). Also, there may be **collusive behaviours** between governments and companies on the covert release of citizens' data (sometimes, as in the US, for money); this create an economy of personal data which erodes privacy. Rules that openly oversee such transactions would work best. There should be in-built guarantees that the data will be used responsibly, e.g. via state control (JS), or through the user being able to decide how his data will be used (IB).

- One of the main problems is the standard **implementation** of data protection legislation; difficulties are related to inefficiency of data protection supervision (Art 29 with limited powers, data protection authorities are differently proactive, and could be more so across the EU), the inexistence of a single market for eId, and great **disparity** in national implementation of identity-related legislation, across members states and sectors; more than has been previously argued. Almost nothing is known, for instance, about **data protection across national borders** (in the form of comparative studies or similar). The biggest obstacle is **compliance** of MS and companies with existing principles enshrined in existing legislation, which is quite comprehensive. Compliance and its **enforcements** by data protection authorities are key problems of today, which are made visible by technological developments. Finally, not all revolves around data protection, as **consumer protection and social discrimination** are significant components to consider in the regulatory discussion (not only personal data at stake: consider consequences, impacts and benefits, as argued above).
- Identity is necessarily linked to **trust** and societal acceptance, as we don't know whether people are misusing our own personal data (GS, YP, others). On the one hand, there is **very limited if any societal discussion** on these topics, outside a few countries; certainly not at EU level. On the other hand, there is a strong need to link whatever implementation of eId and eId to measures of benefits for citizens and society; need to do **impact assessment**; what are citizens exchanging their personal data for? In exchange for what? Under what assumptions? It was argued that data collection could be justified by the added public security (GS), but on the other hand UK courts did not accept this argument (IB).
- Technologies like web2.0, SOA with Web3.0, internet of things and cloud computing will **generate further challenges** to the existing framework as they further enhance data maximisation vs. minimisation, confer systems ways to identifying people, reduce possibilities for non-nominative transactions, link identity to objects and create further data fragmentation (which may then be data mined).

Session 2: Solutions to the Problem

Solutions along the Technology – Regulation Continuum, *W. Lusoli, IPTS*

Interactive Session, *all participants*

Participants' views addressing the following questions:

What – if any – are the solutions? What is the (likely) impact of these solutions? How difficult would it be to implement them?

Who are the stakeholders involved? What should they do?

Which are the research priorities? How can the IPTS contribute?

The aim of the interactive session was to devise a list of the policy options, their potential impact and the feasibility of the implementation of each. Policy options were first elicited in a brainstorming session; this resulted in 17 possible policy options.

Possibly the most important one emerging from the policy issue generation phase, is **enforcement of current legislation**. Another very important issues (JD) is the **layering of regulation** on eId in data protection directives (DPD) in specific fields (such as health), where specific legislation / regulation is invited on top of general provisions. This runs counter to attempts at systematisation; on the other hand, it could provide a good rationale for standardisation / understanding of what is specific of each field and what is common (beyond intentions, in practical implementation in MS).

The role of the EC and EU were noted as a large client for many of eId related companies; based on this, the Commission could exert significant regulation on privacy and data protection via its buying power (i.e., only buy into best standards). And / or persuade MS to act likewise at the procurement stage on eId.

Also, it was noted that 'identity', electronic or otherwise, is **not** Community Law. Identity can be discussed (and has been discussed) under different headings to address the issues (JD noted several instances where the Commission pushed in this direction, e.g. the eServices card); this is problematic, unless Community Law is changed.

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

b. Enforce EU regulation towards members states (infringement procedure). (Currently member states do not enforce existing regulations equally efficiently.)

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

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

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

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

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

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

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

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

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

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

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

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

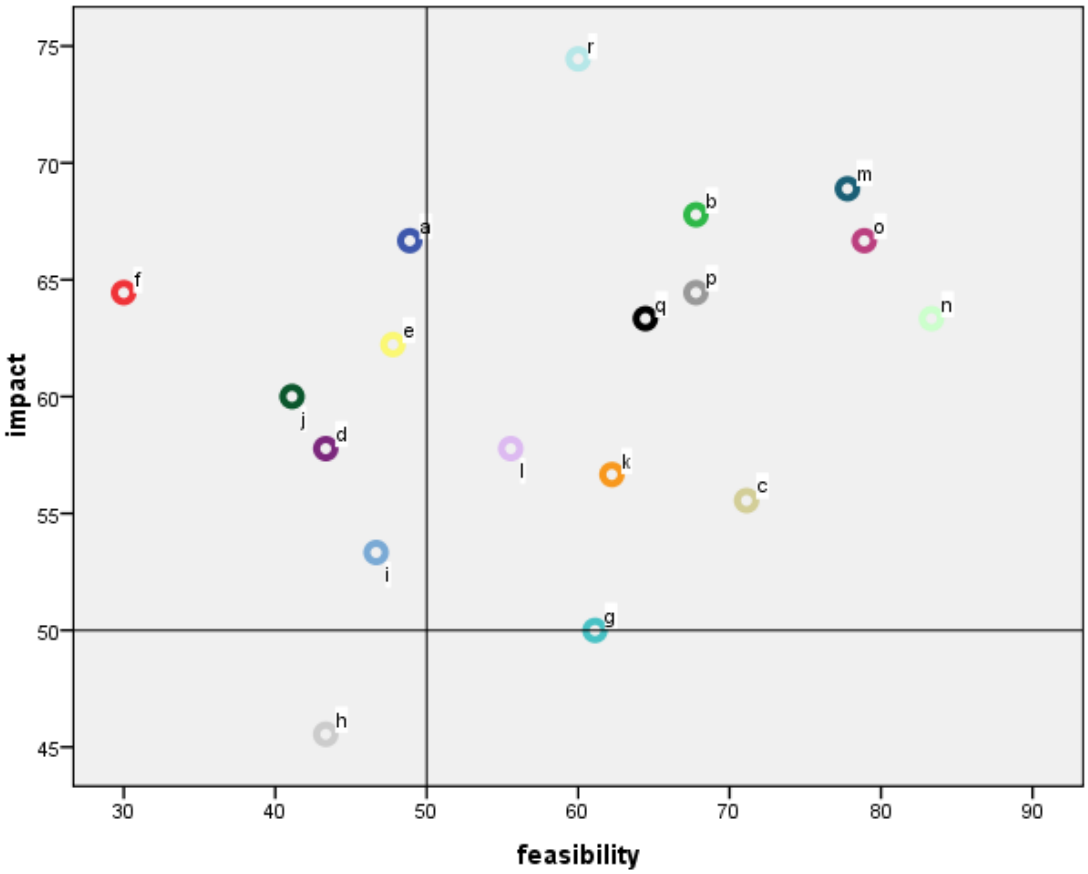
o. Recommendations as a suitable tool (e.g. identifiers).

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

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

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

After the policy options were listed, each participant was asked to rank every option on a 1-10 scale in terms of feasibility and potential impact. The scores given by each participant for each option were added up and mapped on two axes (feasibility – impact). As 9 people participated, the scores for each policy option range between 0 and 90; the resulting graph is presented below. Finally, this graph was discussed within the group, and it was agreed that the graph represents fairly well the group consensus view of the different policy options and their positions relative to each other.



The solution seen as having the largest impact, though not the easiest feasibility of all solutions proposed by the experts is **societal discussion** and acceptance of identity implementation (**r**); a democratic process of acceptance was almost unanimously seen as legitimising eId in Europe. This has more to do with the active involvement of citizenship in the understanding and definition of personal data, privacy and user control than with education and awareness raising.

A second cluster is visible regarding **soft legal-technical regulatory solutions**, based on Best Available Techniques for identity: anonymous identity, cryptography, DRM, guidelines for compliance, and Commission Recommendations as a suitable tool (e.g. on identifiers) (**m, n, o**). These, largely based on soft regulation and persuasion, are seen as offering a good balance between impact and chances of implementation at the present time. These include solutions that keep personal data separate, allowing data control *on behalf of* citizens, rather than *by* citizens (which could carry problems, due to increasing responsibility in the case of a lack of skills). However, best available techniques (BATs) need to be seen as clearly linked to compliance; therefore not BAT in general but BATs that then generate compliance with specific eId regulation (in the way this is intended in the IPTS elaboration of BATs). In this context, IPTS should possibly look into the behavioural issues regarding the acceptance of different types of soft solutions. The fact that Standardisation solutions, not necessarily EU level, (technical: privacy seals, ISO for IDMS) get a much lower score on impact identifies a need for a debate on what the aims and benefits of standardisation (legal, technical) are in the field of eId.

A third cluster of policy options includes **compliance-inducing regulations** (**b, p, q**), such as drafting of industry Codes of Conduct (for specific fields) to create level playing field and for risk management, again needing support and approval from consumers (e.g. recent RFID recommendation); support for elaboration of standards (regulatory: W3C, pling, etc); and enforcement of EU regulation towards members states

(infringement procedure). All these solutions need to point at a more focused Commission at addressing the 'grey' area surrounding the implementation of existing regulations (industry, MS). The latter item was seen as a tried and tested and well understood way of ensuring MS activity in a given field, and as such relatively easy to implement.

Still valuable in terms of impact but less feasible are enforcing regulation outside the EU, and, more in general, standardizing implementation of applications of DPD + consumer protection in Europe and elsewhere (**a and e**).

What experts think will be of **lesser impact and feasibility is bridging regulation across Directives** (**f, h, i**); this includes setting eId regulation as infrastructural, like the eSignatures Directive; creating an eId package relying on existing tools (as for the Telecoms reform Package); or creating new, supra-national legislation on eId (via the Regulation route). Although the latter would have a greater impact, this is rated as the least feasible option under discussion.

Suggestions for IPTS activities. Overall, it was noted that the eId debate promoted by the IPTS fully falls in the wider debate on 'better regulation' currently being held within the Commission and EU institutions more widely.[4] One option for the IPTS is to function as an eId observatory, to chart developments in the field, as observation activities are currently spread over many DGs and Units. Also, as there is a problem of governance in dealing with the privacy / data protection industry (witness the recent case of the expert group), JRC IPTS could possibly act a trusted third party in mediating with industrial players on this topic. For example, we could find out about the business models, privacy policies and other relevant aspects of the relevant industrial players, especially those that infringe the existing rules (suggested by TW). Additionally, the IPTS should become more active in the behavioural and economic aspects of eId, which were deemed by the experts to be very challenging but worth the effort. Practical topics we should investigate include cloud computing (not IPv6), identity in relation to search engines, and anonymity both as a principle and as a technology.

[4] http://ec.europa.eu/governance/better_regulation/index_en.htm