PrimaVera Working Paper Series

UNIVERSITEIT VAN AMSTERDAM

PrimaVera Working Paper 2006-10

Identity management distilled

a comparison of frameworks

Pieter Wisse and Paul Jansen

May 2006

Category: scientific

University of Amsterdam
Department of Information Management
Roetersstraat 11
1018 WB Amsterdam
http://primavera.fee.uva.nl

Identity management distilled

a comparison of frameworks

Abstract

Compelling reasons abound today for emphasizing the relevance of identity management. Enabled by digital information — including communication — technology, people conduct an increasing number of their interactions physically separated in space, yet connected in 'real time.' And 'machines,' especially so-called agents, are making their online contributions by proxy. But then, it's not only the actors directly involved in interaction whose identities should be managed proportionally. Application of information as the very medium of interaction always entails — an attempt, at least, at — object references, qualified in relevant ways. Indeed, more identities to manage.

At this early stage of — digital — identity management, we choose to refrain from any tight definition. It's simply too early. Instead, in this working paper we juxtapose and comment upon several frameworks, all proposed for information management where the concept of *identity* plays a key part. From such a comparison, an already clearer overview emerges of the *varieties* of identity management.

Keywords

Identity management, information management.

About the authors

Pieter E. Wisse (*www.wisse.cc*) is the founder and president of Information Dynamics, an independent company operating from the Netherlands and involved in research & development of complex information systems. He holds an engineering degree (mathematics and information management) from Delft University of Technology and a PhD (information management) from the University of Amsterdam. At the latter university, Pieter is affiliated with the PrimaVera research program in information management.

Paul L. Jansen majored in human resources development at Trinity University, respectively Boston University. His PhD in social & behavioral sciences is from Illinois University. Paul works as a change agent, with a special passion for empowering people to create their learning organization. He has worked for varying organizations, including his own consultancy company.

INDEX

Introduction

We start from our own iDNA-Manifesto.[1] For each article in our manifesto, we're going to discuss how other frameworks have covered the same or similar questions. After we've dealt in depth with all fifteen of our own manifesto's articles, one section at a time, in three additional sections we'll quickly go over each of the other frameworks to see what we may have missed, there. Did we overlook anything of relevance with iDNA-Manifesto? We thereby take the additional opportunity to explain our preferences.

The other three frameworks dealing with identity management in some important way(s) and treated here, are:

— The Laws of Identity,[2] edited by Microsoft's Kim Cameron[3]
— Privacy and Identity Management for Europe (PRIME),[4] prepared by a consortium for the European Community plus Switzerland
— E-Citizen Charter,[5] some guidelines for citizen-oriented government services in the Netherlands.

We do not pretend to present an exhaustive inventory, at all.[6] However, we do believe that these frameworks are now representative for the growing attention given to identity management, whatever it will come to mean.[7]

Please note we're primarily interested in political principles for social equity, i.e. strategy.[8] As will be seen, issues of technological application are clearly included in two of the frameworks we did select for comparison and comments. We've retained Microsoft's, respectively European Community's draft framework because several principles at the level of social organization are suggested, too.

Ownership

As we've announced, for our comparison we simply take one article from iDNA-Manifesto at a time. The first article of iDNA-Manifesto reads:

1. ***Information about the individual (legal) person is the property of that (legal) person***.

Comparing this article to what the other frameworks offer in this respect — actually, to what they don't offer — should already make it abundantly clear that aiming at a closed, invariant definition of identity

[1] We are referring to version 2.1 of *iDNA-Manifesto*. The manifesto originates from Paul Jansen's paper *4891-Project iDNA*.
[2] For our comparison, we've taken the version of *The Laws of Identity* in Word format, dated at February 22nd, 2006.
[3] Cameron keeps an Identity Weblog; see *www.identityblog.com*.
[4] We have oriented ourselves at version 1.0 of *PRIME White Paper*, dated at July 18th, 2005; a list of consortium members is included.
[5] The charter results from a Dutch government project.
[6] We are grateful to Marcus Lasance of MaXware UK for both a first written overview and his subsequent personal communications.
[7] Pieter Wisse develops conceptual grounds with his essay *Semiotics of identity management*.
[8] Therefore we've left out the predominantly technologically oriented Higgins initiative (IBM et al.), for example. We would be interested, though, to position the principles behind such operational platforms.

management is illusory. Whereas iDNA-Manifesto addresses the question of information *ownership* first and foremost, none of the other frameworks even mention the issue. Both The Laws of Identity — here subsequently also referred to as LOI, for short[9] — and PRIME are grounded on the concept of the *user*. We believe that such a foundation for identity management takes too many varying assumptions for granted. For example, LOI and PRIME could be interpreted as to suggest that systems containing person(al) information are simply given. So, it may seem, whatever person information is *registered* by whatever actor —the person in question herself included — lies outside what the framework governs, that is, use.

Indeed, if only actual use counts, why bother with controlling registration? Our idea is that the basic principle(s) of managing person information must,[10] as much as possible at any stage, abstract from technologies in general and systems/tools in particular. Even — or, especially so? — when a person is not a user herself in the sense of actively participating in a digitally facilitated interaction, she needs to be confident of adequate control. iDNA-Manifesto therefore steps outside the, indeed, limited perspective of direct user involvement to state, more generally, an explicit principle for social organization. It helps to avoid an overly narrow bias.

From this broader principle it is easy to recognize the bias of e-Citizen Charter, too. Its hidden assumption is that government institutions each actually own the person information about citizens in their information systems. Now iDNA-Manifesto openly challenges the divorce of ownership from the person 'at stake.' This is not to say that iDNA-Manifesto is objectively right, and e-Citizen Charter evidently wrong. It's fundamentally all about a political choice. A dictatorship would undoubtedly rule that person information is state-owned, period. It is only from establishing different *contexts* for ownership and use, respectively, that subsequent unambiguous differentiation of corresponding behaviors becomes possible.

The political diversity at the global scale makes it hardly likely, if not outright impossible, to arrive at a universally accepted framework for identity management. It pays to become aware of the stakeholders 'behind' a particular framework. Then, as a supplier of tools for information work, it is immediately obvious why Microsoft would hinge its perspective for identity management on so-called users. As a company, it doesn't want to be overly bothered with issues in need of political resolution. But, then again, such issues cannot be avoided. Sooner or later they emerge, which is precisely why we have chosen to address them upfront in iDNA-Manifesto.

At first glance it seems odd that PRIME, too, is oriented at users, rather than at persons. We believe the actual consortium members provide an explanation. With their roots mostly in the technology sector, too, similarities between LOI and PRIME are only to be expected.

---

[9] 'Loi' being the French term for law. ☺

[10] Here, information management would include recording, querying and 'using.'

e-Citizen Charter suffers from the illusion that an official statement by the government about the charter having been formulated independently … from government guarantees a citizens' perspective. No responsible citizen is so easily fooled, of course. Equity doesn't really improve from rhetoric. In fact, trying to make government somewhat more 'user friendly' seems to be aimed at keeping the traditional citizen-government relationship essentially unchanged, that is, government-centric.

If there ever was an illusion, we feel such conservatism certainly qualifies. Pervasive application of digital information technology — technologies, actually, which continue to develop — amounts to qualitative change of society.[11] Identity management, then, is not some side-issue but exemplifies our current social development. It simply follows that the 'quality' of identity management must be strategic, proactive, rather than reactive. The rhetoric of some frameworks for identity management may seem innovative enough. But how they should actually work out, is of course what matters. Such simulations require their assumptions being made explicit first.

Please note that squarely allocating ownership of person information to, as iDNA-Manifesto proposes, the one person concerned doesn't yet suffice to make such ownership unproblematic. Ownership doesn't just simply shift from a multitude of users/holders (traditionally government institutions and companies) to a single subject (the person). It is vital to recognize that information is an irreducible aspect of — symbolic — interaction, i.e. communication. And interaction involves participants, or actors; they are engaged in relationship. What makes the changed information order far less problematic is that it follows that the respective contributions to the interaction count differentially. That is, each actor owns … her 'own' informational commitment.[12] What all actors share, i.e. what is communally owned, is only — a reference to — the interaction in question.

Different others

In article 2, iDNA-Manifesto moves to information use. With ownership firmly established with the person who is the 'subject' of information, she is of course in control of whatever subsequent use. In other words,

2. The person may grant other parties usage rights to pertinent person information.

[11] A. Brate surveys several "visions from the information revolutionaries" in *Technomanifestos* (Texere, 2002).

[12] Each interactional contribution by every actor might constitute a separate context, providing the unambiguous basis for further specifying what her contribution (also read, more generally: behaviour) actually was/is/is expected to be.

It is left as an exercise for the reader to contemplate on, for example, the change of ownership of real estate. What counts as interaction(s)? What person information is involved? Therefore, who owns what information? Who records? Who are potential users? For the requisite method, see *Metapattern: context and time in information models* (Addison-Wesley, 2001) by Pieter Wisse.

LOI's first law is about "user control and consent," arguing that

> [t]echnical identity systems must only reveal information identifying a user with the user's consent.

Again, different perspectives are quite apparent. Our starting point is the person, who may subsequently grant usage right to *other* actors/parties.

LOI, on the other hand, seems to assume that there already exists an information system, managed by some other party. That comes first, and only then does a user give her consent. What the terminology of granting versus consenting suggests, at least we think so, is a significant difference of priority. With consenting, how much is a person really in control? And, by the way, to whom is the information revealed? If it is a matter of the registration holder — who, according to LOI, obviously is not the person herself — informing some third party, i.e. another 'other,' is it actually not ill-directed to call the person a user? For in precisely such an interaction, that is, between other registration holder and other third party, the person about whom information is exchanged is … a non-user.

We also find mention of "identity systems" unnecessarily limiting. It can be replaced in LOI's first law by the more general concept of information systems. And why "identity systems" are predicated as "technical" eludes us. Although, we can guess. It seems that what's behind LOI is the idea that identity management is at most a more sophisticated "system" for controlling access to information resources.[13] The concept of access suggests that the resources are, indeed, owned by someone else, usually a business or government organization, than who-information-is-about. Of course, then it is such an organization 'granting' access to users. That's all perfectly alright. Where it becomes confusing is when changing the label from access management to identity management without realizing the much wider implications of the latter, i.e. *spreading into information management in its most general sense*.

iDNA-Manifesto recognizes the requirement for a qualitatively different paradigm. LOI, however, is still mixing categories, perhaps in the expectation that identity management at the scale of society results from an extrapolation of traditional access control. We believe that's too simplistic. Sure enough, access control includes technical means, and so does identity management whatever it is at whatever scale. But technical aspects are always secondary; it must first of all be clear that granting access to a user-being-the-person-the-information-is-about, that is, the owner *herself*, is qualitatively different from mediating a person's (also read: owner's) consent for information usage by yet *other* parties.

---

[13] Wikipedia carries a lemma on identity management. As consulted on April 21st, 2006, identity management is still narrowly defined as "an integrated system of business processes, policies and technologies that enable organizations to facilitate and control their users' access to critical online applications and resources — while protecting confidential personal and business information from unauthorized users. It represents a category of interrelated solutions that are employed to administer user authentication, access rights, access restrictions, account profiles, passwords, and other attributes supportive of users' roles/profiles on one or more applications or systems."
Our position is that such a definition reflects an inside-out approach that has already reached it limits. With *iDNA*-

The 'old' access control is conceptually a small subset of the 'new' identity management (with the latter, as we argue, fast becoming indistinguishable from information management). As the confusion in LOI demonstrates, though, a framework for access control, only, is inadequate for developing into a framework for identity management in the interconnected world of practically infinite information variety.

PRIME agrees with LOI in its overall orientation. Again, from our starting point of personal information ownership, by mentioning the user it distracts from what essentially needs to be governed. Indeed, PRIME also devotes a principle to "user-informed consent and control," stressing

> the user's informational self-determination: keeping control on which personal data are given to whom and for which purpose.

Once again, such a prescription can only be understood from the assumption that another party must essentially manage the information, thus requiring the user's consent for distributing it to *yet* another party. It seems that the giving of such consent by a person is equated with performing an activity, too, which is digitally facilitated; and using the facilities makes the consenting person … a user, so the assumption probably reads. If so, it should be made explicit that as a user of the facilities, the person is not the — intended — user of the person information which usage by another actor/party she consents with.

Under the heading of "convenient services," e-Citizen Charter stipulates:

> Government makes clear what records it keeps about me and does not use data without my consent.

We would say that merely labeling it a convenience rather downplays the importance of making clear who is really controlling information. Like LOI and PRIME, e-Citizen Charter doesn't put and let the *initiative* etc. lie with the person, not really. It remains a strictly government-centric proposal.

Change seems inescapable. As the traditional holders of person information, government institutions are experiencing increasingly severe operational problems. For without proper, formal distinction between ownership and holdership, institutions are also held one-sidedly responsible for information quality. It transpires that a disproportionate effort is required of any institution to keep information reliable, accurate, etcetera.

We observe that some more enlightened government institutions are becoming aware of the impossibility of 'owning' the quality aspect of what it doesn't really own in the first place.[14] So, they attempt to shift the responsibility for information quality to … the person involved. The person, however, doesn't readily recognize her responsibility, for she is still led to believe that the information is *not* her own, but is owned

---

Manifesto we advocate an outside-in perspective. Then it should come as no surprise that identity management seamlessly integrates with information management.

[14] Companies, understandably, have fewer qualms about enlisting customers etc. for informational contributions to business processes. The information a, say, customer provides, however, 'disappears' beyond the person's control in every company's often plural registers.

instead by some government institution. It should be(come) obvious that the basis for responsibility for quality entails unequivocal — allocation of — information ownership.

We'll have more to say on information quality and who's responsibility it fundamentally is where we encounter iDNA-Manifesto's eleventh article, below.

Coverage

The third article of iDNA-Manifesto is actually an extension of its second article. It sets rules for what should be covered in an agreement for using person information:

3. ***The person stipulates a usage right, e.g. authorisation, by specifying at least***
   a. the other party;
   b. the purpose of usage and;
   c. the relevant subset of person information.

PRIME provides similar guidance, albeit in a more general vein, calling it "privacy negotiation [and] agreement:"

> [U]sers can negotiate with their transaction partners and conclude an agreement which includes contractual provisions about the privacy rights of the parties involved in the transaction.

We won't go again into the confusion arising from mentioning users, rather than persons. It has been sufficiently dealt with, above.

What comes up as an especially interesting aspect here, are "privacy rights." It may strike the reader of iDNA-Manifesto as odd that it nowhere even mentions privacy. We take the opportunity to explain that we've not at all committed an omission. It's really quite straightforward, too. The complete iDNA-Manifesto is essentially a privacy framework. We've made it so from our first article on, where information ownership is unambiguously allocated to 'the person.' This shift helps to realize that issues of privacy 'only' occur when person information ownership does *not* rest with the person herself. It is precisely the lack of control which calls for privacy measures to acts as counterbalance. iDNA-Manifesto sets the balance on a qualitatively new footing by integrating privacy right from the start.

LOI takes a very neutral stand, here. Referring to "justifiable parties" (fourth law), it refrains from committing itself to any social organization. Instead, it takes a more infrastructural orientation, arguing that whatever is decided upon should be supported. So,

> [d]igital identity systems must be designed so [that] the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

LOI leaves open, both understandable and respectable coming from a technology vendor, what will — come to — count as "necessary and justifiable." The second law, about "minimal disclosure for a constrained use," is related:

> The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

PRIME argues much the same approach with "data minimization and identity management:"

> [T]he basic principle underlying all exchanges is disclosure of personal data on a need-to-know basis only.

Who needs to know, and what is sufficient for the particular need, always remains to be agreed upon.

For e-Citizen Charter, one participant in interaction is always a government institution. The charter doesn't explicitly specify limits to information coverage pertaining to interactions.

Proxies

With its fourth article, iDNA-Manifesto also makes the consistent point of the person controlling her person information:

4. A usage right may include that the other party keeps a register of - a duplicate of, irrespective of the medium - person information.

So, the rule is self-management of person information. Please note that it doesn't matter that such self-management now is, and/or will always be, exceptional *in practice*. It doesn't detract from the practical value of precisely this principle. For it opens the way for, say, other-management of person information to become explicitly rule-governed.

The other three frameworks for identity management under consideration here all remain silent on this point. Above, we've already hinted at hidden assumptions. Actually, e-Citizen Charter is quite outspoken, as soon as its government bias is recognized. For example, where the charter states that a "transparent public sector" implies that

> [a]s a citizen I know where to apply for official information and public services

it is evident that the information is 'officially held,' that is, by government institutions with their information systems. Above (see the final remarks of our discussion of iDNA-Manifesto's second article), we already reported on some government institutions attempting to move away from the dilemma of being solely responsible for information quality. They cannot succeed, however, as long as holdership remains confused with ownership. e-Citizen Charter, too, still seems firmly rooted in the mistaken equivalence of ownership with holdership.

Government ownership of person information is also taken for granted where the charter explains its view of "personalised information:"

> As a citizen I am entitled to information that is complete, up to date and consistent. Government supplies appropriate information tailored to my needs.

What is left unaddressed are the "needs" for the fulfillment of which the person information was collected, kept etcetera in the first place. Most likely, it was not to inform the citizen, but to perform *authorized*

government activities. We've already quoted e-Citizen Charter on "[g]overnment mak[ing] clear what records it keeps about me[.]"

PRIME and LOI differentiate even less than e-Citizen Charter does with respect to information ownership and possible proxies extended for keeping a register of — subsets of — person information. Both of those more business-like frameworks also seem to conflate holdership of a register with ownership of information therein contained. iDNA-Manifesto starts from a precise allocation of ownership. Sub- and consequently, roles — especially including responsibilities! — can, and should, be explicitly differentiated.

Before, technology only permitted isolated information systems. The risk of malgovernance was minimal because what was left implicit was always clear enough for the stakeholders involved with each smallish system as an immediate context, separately. Now that 'everything' potentially connects with 'everything,' a paradigm shift for identity management is mandatory. What worked perfectly well for a singular system, now breaks down under conditions of plurality, variety and so on. No longer can identity management be treated in isolation; the paradigm shift makes identity management an irreducible part of information management.

Recursiveness

A framework should be as consistent as possible for the activities it is supposed to — offer support for — structure. Preferably, therefore, it must be applicable to what it produces, too.

Key products according to iDNA-Manifesto are — agreements on — rights for information usage. Such agreements, in their turn, also take the form of … information. Then, it is only logical to consider whether the framework remains applicable. The fifth article of iDNA-Manifesto makes explicit that it does:

5. ***All granted usage rights become inextricably part of person information.***

Of course, it may be superfluous devoting an article/principle to recursive application. But it certainly helps to raise awareness of, say, levels of conceptualization which require integrated control.

The other three frameworks don't address recursiveness explicitly; in their cases, it's therefore more difficult, to say the least, to evaluate how identity management might function across so-called levels.

Balanced government

We've included LOI, PRIME and e-Citizen Charter for comparison because they supply a contrast that is particularly relevant when recognizing that identity management moves to a qualitatively different order. It is becoming part and parcel of society as a whole, yes, an increasingly international society as far as information exchange is concerned.

e-Citizen Charter represents one side. As we've repeatedly indicated, it presupposes government participation in the interactions for which it was developed as a framework for conduct. On the other side, both LOI and — admittedly, to a somewhat lesser extent — PRIME seem to take their cue from separate private sector organizations. The closest LOI seems to come to acknowledging government involvement is where it mentions "public [and] private entities." Yet upon closer inspection, it turns out that public/private is applied to refer to different regimes of accessibility, rather than social institutions. Government does not at all appear in LOI as issuer of identities and/or privileged user of person information. Likewise, and after all quite surprising considering that the European Community/Swiss government commissioned it, PRIME is also completely silent on government.

iDNA-Manifesto continues from the realization that, say, Internet-age identity management has turned it into an irreducible aspect of social development and organization. At that scale, governments essentially have roles to perform, too. Please note, with social development their roles will even change, identity management providing a clear illustration or even proving the point. It means that a productive framework for identity management should certainly make an effort of sketching — when appropriate, anew — the optimally balanced position for government(s).

We actually consider e-Citizen Charter a failure in this respect. It may justifiably be blamed for its one-sidedness (and for claiming the opposite orientation, which is patently unfounded). But we don't feel that LOI can be blamed for overlooking to include government in a newly balanced position. It still is a framework mainly oriented at private sector organizations, for which it suggests a first upgrade of their traditional access control of information resources. Then again, LOI stands much to gain from recognizing the qualitatively different scale of identity management, i.e. moving toward information management in general, and positioning government accordingly. PRIME seems to suffer from execution by a consortium without sufficient appreciation for the — government — origin of its commissioners.

Returning to iDNA-Manifesto, its sixth article pronounces government as a privileged user, and possibly holder, of person information:

6. A government institution obtains usage rights by law.

Short as it is, this article refers to 'the workings of democratic government.' The process of government should guarantee equity. So, whatever government institution should not — be able to — unilaterally determine its right to usage of person information, or whatever information, for that matter. The laws governing information usage by … government are created through democratic process, with due regard for (legal) persons (see article 1 of iDNA-Manifesto) who are lawfully represented.

One way of looking at article 6 is to consider it as a reformulation of the manifesto's article 2. There, it is the person-as-individual who grants usage right. Here, in article 6, the person-as-collective essentially agrees usage rights with herself. In order to exempt the government from individually negotiated

agreements, one for each combination of person and authorized government task, article 6 allows for a sort of collective bargaining, of course within the overall political and legal framework. So, it is not that individual agreements are simpler etc. than collective agreements. They are just different, especially as far as the process is concerned through which they are arrived at.

Of course, individual agreements should also at least comply with the legal framework for social conduct.

Emphasis

The formal distinction, with iDNA-Manifesto, between information owner and possible other party as holder of a register, allows for specifying additional conduct:

7. ***No additional permission is required for the person to inspect the usage, when applicable including how registers are kept, of their person information by the other party.***

This extends article 4, where it says that another party may be granted the right to keep a register of person information. It has been given separate expression in the manifesto because we felt the need for emphasis on the related right to inspection by the information owner. Please note that article 7 does *not* cover inspection of, say, application. When application is called active usage and 'just' holdership would be known as passive usage, it is the latter we're dealing with right now.

LOI and PRIME do not explicitly recognize holdership as a separately derived role in information management. It follows, really, from their implicit assumption, i.e. taking identity/information systems as given and erecting the framework from that point on, only.

How e-Citizen Charter compares is treated further on, where we present the manifesto's ninth article.

Social equilibrium

A risk for social stability is the generation of frustration. People become frustrated when something they feel that they rightfully own, is actually — actively made and kept — unavailable. Having to make an effort to claim what is theirs in the first place is already repulsive. Next, being treated offensively amounts to adding insult to injury.

When ownership is respected, as it should, trust grows. On the balance, more actors profit and civilization as a whole develops.

Taking the concept of the information society seriously, means giving fundamental attention to information ownership. It is currently the frontier for continued social development. So, ownership must be strengthened by additional measures.

As owner, the person also has the fundamental right to learn how her person information has been applied by another person, company or government institution. She should not be bothered with administrative

hurdles. Instead, the relationship must be reversed. The person should no longer have to make a request. The user — and please note how we use the word 'user' differently from LOI and PRIME — is liable to report on usage. As the manifesto's eighth' article proposes:

8. The other party periodically, without the person's explicit request and for each transaction, accounts for the usage of person information to the person in question. The reporting frequency has been determined in the usage agreement.

Identity management is not just some improved instrument. It is fast becoming a key infrastructural ingredient for social-political dynamics. From this — again, qualitatively — widened perspective it follows that behavioral feedback must also be addressed by a viable framework.

Traditional information management is far removed from sustainable equilibrium; it favors some actors at the expense of others, with individual persons usually being exploited.

A fair 'deal,' we've already said so, is always also in the long-term interest of parties who are now shortsightedly holding on to unqualified privileges.

How does e-Citizen Charter fare as far as preventing frustration and promoting trust are concerned? For example, it advocates that

> [g]overnment ensures multi channel service delivery, i.e. the availability of all communication channels: visit, letter, phone, e-mail, and internet.

Fine, the choice is to some extent left to the citizen. She can choose what comes — as we would say — as least inconvenient, also considering that "service" is of course a euphemism most of the time when interacting with government. Most interactions are about compliance with government rules, rather than the person being at the receiving end of some freely chosen service. Even for social benefits, service is a misnomer. When a person is entitled to a benefit, we find it degrading to call it a government service.

iDNA-Manifesto is about information management in general, while e-Citizen Charter 'only' refers to citizen-government interactions. Given its limited perspective, e-Citizen Charter does indeed put the burden of reporting with the actor who is using the person information, for

> [g]overnment keeps me informed of procedures I am involved in by way of tracking and tracing.

Our reluctance consists in not quite understanding what "tracking and tracing" involves. When it is the government who tracks and traces, subsequently informing the person without her having to make a request, we gladly acknowledge correspondence to our manifesto's eighth article. However, we would like handles added for operationalization. It's precisely why in our article 8 we mention 'details' such as "for each transaction" and "reporting frequency."

Alarming, then, is how e-Citizen Charter treats "trust and reliability:"

> As a citizen I presume government to be electronically competent.

Who is actually expressing a principle, there? Coming from a citizen, it makes sense to require the government to account for its activities. Why should the citizen give her government the benefit of the

doubt? So, it seems reasonable to conclude that some government official took the opportunity with e-Citizen Charter to avoid liability, instead.

And what to think of the typical reassurance that

> [g]overnment guarantees secure identity management and reliable storage of electronic documents[?]

It begs the question what identity management is. When

> [a]s a citizen I can file ideas for improvement and lodge complaints[,]

it is called "considerate administration" by e-Citizen Charter.

Why is it necessary to prescribe that

> [g]overnment compensates mistakes and uses feedback information to improve its products and procedures[?]

Shouldn't that be perfectly normal, already? What does e-Citizen Charter add with such "quality standards"?

Voluntary feedback on actual information use is absent from LOI. PRIME states the requirement

> that individuals stay aware of the scope of use of their personal information by their transaction partners[.]

Again, we would like to see included what the general terms of such awareness are. For example, are "transaction partners" under an active duty to report? From such a vague statement as PRIME offers, operationalization is not yet sufficiently directed.

Keeper's accountability

We have already explained how iDNA-Manifesto considers holdership an aspect of usage, i.e. passive usage, but usage nonetheless. Our ninth article is designed to secure regular reporting on such passive usage, too. The (other) information holder must, of course, we believe, report to the information owner:

9. If the other party (also) keeps a register for the person information, an account must be included in the periodic report to the person. The reporting period has also been determined in the usage agreement.

As article 7 of iDNA-Manifesto extends its article 4, article 9 can be seen as an addition to article 8. It serves to make explicit a necessary emphasis.

When LOI and PRIME don't provide for reporting on active usage, that is, by the user, it more or less follows that rules for reporting on passive usage by the holder are equally missing. However, relying on "user consent" is far too limited a guarantee from the perspective of the person involved. Again we emphasize that "user" is a misnomer, there. It is usage, including holding, by some *other* actor than the person whom the information used/held is about, why control loops needs to be — more — tightly closed in favor of the person. Please note that in the information society, *we are all persons* especially in this respect.

Both LOI (law 3: limited disclosure) and PRIME (need-to-know basis) state important constraints, but the design for a genuinely systematic order is still rudimentary. This is not to say that iDNA-Manifesto is

already well-rounded as far as integrated control mechanisms are concerned. It would be too much to expect, actually, at this early stage of awareness of overarching relevance of identity management. iDNA-Manifesto does, however, clearly recognize how checks and balances for identity management are essentially social-psychological in nature, requiring a correspondingly widened perspective. So, when PRIME argues that

> evidence [must be] retained during the transaction [as] the reference against which potential disputes can be evaluated,

how are responsibilities for retaining such evidence allocated? Testimony to PRIME's potential for more mature socially oriented guidelines is its insistence that evidence

> represents the reference against which potential disputes can be evaluated.

iDNA-Manifesto was drawn up from information ownership as the core concept. When an asset — in this case: person information — is used by another actor, what basically happens is that it is applied beyond the immediate control of the owner. The question of securing social order then becomes one of, say, compensating the owner for such loss and subsequent lack of control. So, for equity, in turn the — real! — users also relinquish some autonomy. Their obligation to report on usage/holding to the owner is meant to re-establish an operationally viable social balance.

Referring to e-Citizen Charter, we've already mentioned its call for "reliable storage of electronic documents." What really counts, of course, is the person's practical access to her person information. It certainly helps, according to e-Citizen Charter, that

> [g]overnment ensures that my rights and duties are at all times transparent.

Better still,

> [g]overnment makes clear what records it keeps about me and does not use data without my consent.

What such "quality standards" make us wonder even more, though, is that e-Citizen Charter seems to draw from the assumption that a citizen is strictly defined in relation to government. Again we apply the wider perspective of society, where every person is always a citizen. It means that "standards" or whatever cannot remain limited to person-government interactions. Instead, they should 'govern' all interactions with aspects relevant for the public domain.

From its regretfully limited perspective, e-Citizen Charter proposes:

> As a citizen I am able to compare, check and measure government outcome. Government actively supplies benchmark information about its performance.

In the information society at large, too, a person should be generally awarded such 'powers' for all her interactions with some — potentially — public aspects. Arguably the most important role for government is to protect the person's rights of integrity, also when a government institution was not directly involved in the original interaction. What should now be acknowledged, and formalized accordingly, as an irreducible aspect, too, of personal integrity is person information.

Just different, not separate

Article 6 of iDNA-Manifesto, "A government institution obtains usage rights by law," could be so densely expressed because workings of democratic government, including a balanced legal framework, are assumed. In fact, in this sense iDNA-Manifesto is more succinct than, especially, e-Citizen Charter. For the latter actually restates much that is not at all specific to the occasion for which it was drawn up, i.e. government aiming at digitally facilitated interactions — calling them "services," for the occasion — with 'personal' members of the public (also bypassing companies and other statutory organizations in their dealings with government, leave alone in — information — society at large).

Where article 6 establishes government participation as a special case for primary usage of person information, another additional article argues for government's special case for reporting on usage, holding included:

10. How a government institution accounts for usage of person information is decreed by law.

Likewise, it doesn't at all mean that government is exempt from reporting (and, through lack of reporting, effectively from liability …). Article 10 of iDNA-Manifesto 'only' puts forward that aspects of management of person information/identity, such as covered for accountability in general by its articles 7 up to 9, require particular procedures etcetera, too, when a government institution is involved with using/holding. In fact, in several respects accountability of government should be expected to be ruled (far) more strictly.

For comparing iDNA-Manifesto with e-Citizen Charter, it is of course logical to single out article 10. We want to offer a general comparison, though. That is why we have already dealt with e-Citizen Charter's approach to accountability, above, where we made comments starting form the manifesto's articles 7, 8, and 9. We oppose the self-limitation, only recognizable from a wider perspective such as iDNA-Manifesto provides, of e-Citizen Charter to "government services" to private persons. Management of person information — and why not also call it identity management? — can only be organized properly at the scale of overall society. What also becomes recognizable, then, is government's special position for which, indeed, some correspondingly special arrangements are necessary. Government is not apart from society, but an essential, constituting part of it. Ultimately, it calls for *international* cooperation.

Interdependency

From its first principle of information ownership, iDNA-Manifesto's nine subsequent articles are mainly occupied with safeguards for the owner. The idea is that information usage/holding by another actor than the person herself entails, by definition, a loss of control which should therefore be compensated for.

Dependency, however, hasn't just shifted in one direction, only. Any other actor has now also become dependent on the person-as-information-owner. Social equilibrium requires acknowledgment of pertaining duties on the owner's part. The owner, therefore, cannot just enter agreements for usage. The other-actor-as-user should be able to trust the person information made available for usage, also meaning that the owner is formally liable when — and here we use the words with precision — agreed-upon quality standards are not met.

11. ***The person is responsible for the quality of information subject to usage agreement(s).***

Again, we emphasize that such a provision can only be made to work consistently from an unambiguous ownership principle. Nowadays, person information is held by all sorts of organizations without the person herself being able, practically anyway, to exert any control. Such a fundamental imbalance effectively makes the organization, if not formally responsible, at least spending huge efforts for achieving some adequate measure of information quality which essentially lies outside its control.

As we've already mentioned, some government institutions have started to — consider to — re-engineer processes. They seek to involve the person (more) directly in the quality assurance of … her person information. We argue strongly that they can only succeed from an overall redesign of checks and balances, sharing in the constitutional point of departure of *person* ownership of *person* information. Simply put, organizations all over have to give up the false idea of owning person information in order to gain what is really 'use'ful.

LOI, PRIME and e-Citizen Charter all address some issues that could be classified as promoting quality. Nowhere, though, is the person's direct responsibility summoned for the quality of her person information itself. iDNA-Manifesto departs from the — still implicit —assumption made elsewhere that the framework can profitably start from existing circumstances. Yes, person information is indeed often used nor held by the person herself. How it will evolve, iDNA-Manifesto abstracts from. But whatever arrangement — for democratic society — can only be consistent when information ownership rests with the person herself. Then, also in principle, she may decide that only she herself keeps a register of her 'own' person information. We emphasize that this is not just idle theory. For at least this fundamental right makes it clear that any different arrangement constitutes some, say, outsourcing which needs to be formally agreed upon.

Nature of framework

We hope it has already become clear that we put great emphasis on a framework's operational relevance. So, how can it — be made to — really work when, as our eleventh article prescribes, the person is

responsible for information quality?[15] That's far too general a statement for practical purposes. On the other hand, with exhaustively detailed instructions it wouldn't be a framework any longer, but a blueprint. And blueprints … don't really work. They don't, anyway, at the scale of the whole of society or with qualitatively changing variety. A framework for identity/information management is even concerned with qualitatively changing society.

Admitting to some arbitrariness to what should, may, etcetera, be optimally included, and what not, we chose to add precision to iDNA-Manifesto's eleventh article succinctly as follows:

12. Upon receiving a signal by any other party of faulty person information, the person immediately applies correction.

This article recognizes that information involves communication, and therefore relationship. And only in the design for the process of relationship does operationalization find relevant direction. A truism, yes, but it takes all participants to develop mutual trust.

Of course, such an article begs the question as to who ultimately decides on what counts as "faulty." We argue, in principle, that the digital nature of much of present information technology doesn't basically alter that question. As far as the legal framework is independent of particular technologies, it should therefore be relied upon to provide mediation and, when necessary, binding judgment or verdict.

Once again, article 12 of iDNA-Manifesto reflects a perspectival turn when compared to the other three frameworks under consideration, here. e-Citizen Charter is actually most outspoken that the person — labelled citizen — does not herself keep a register of (her) person information. Government institutions do, as can be read from e-Citizen Charter's "quality standards." Consequently, those institutions expend effort for information quality. It's called "considerate administration" when

> [a]s a citizen I can file ideas for improvement and lodge complaints. Government compensates mistakes and uses feedback information to improve its products and procedures.

Upon some closer inspection, what e-Citizen Charter specifies there is indeed the opposite of the manifesto's article 12. For on the basis of our article, the charter's particular quality standard can simply be rephrased as:

> Upon receiving a signal by a [citizen] of faulty person information, the [government] immediately applies correction.

It certainly sounds service-oriented. But is it? Underlying such a behavioural rule is still a muddled concept of information ownership. Talk about faulty, the regular foundation is still missing from those frameworks for erecting the flexible, dynamic infrastructure for the information society.

---

[15] The concept of quality is especially variable, i.e. contextually differentiated. Realizing the naïvely realist nature of our position, we here mean with quality the correspondence between fact and information. Naïve realism can be seen as an assumption for guiding social conduct. The idea of correspondence grounds practical liability, accountability, and so on.

PRIME explicitly mentions "the user's informational self-determination," but also fails to ground it on ownership, leave alone to move to — some specific — consideration of equitable roles that participants are required to perform for productive informational interactions.

Toward reconstruction

The person is invested with information ownership. So far, iDNA-Manifesto's articles have equated ownership with more or less unqualified rights for a person to at least hold and use her person information herself. However, socially that's not sufficiently balanced. For example, as a house owner cannot 'just' do as she likes with her house, an information 'owner' can also be constrained even though she always formally owns all of her person information.

The constraining power resides with government only, which is less one-sided than it may seem. We've already pointed out that government-as-process is quite different from government-as-object. Here, we're once more referring to the former, i.e. the democratic process through which any social constraint is ultimately a self-constraint. As iDNA-Manifesto puts it:

13. ***The person's control over their person information may be restricted. Any restriction always has a legal basis.***

Our mere reference to "legal basis" should be sufficient to include the 'normal' legal framework.

It's again interesting to see how opposing assumptions show through in the other frameworks. We repeat that iDNA-Manifesto starts from the person's unqualified control, and subsequently applies constraints. Most recognizable in e-Citizen Charter, unqualified control is assumed for government institutions. Next, constraints are added for those institutions. Please note that, at this point anyway, the charter seems only concerned with government-as-object.

We don't want to ridicule e-Citizen Charter's attempts at balancing the informational relationship between citizen and government. However, it cannot practically succeed from starting at the wrong end.

We can only guess why e-Citizen Charter omits whatever restrictions. Doesn't it fit in well with promoting government's service orientation?

For LOI, as might be expected at this stage, constraining the person's control lies outside its scope. It can only enter, rather, enlarge the scope after the issue of information ownership has been recognized. An organization is, we believe, still seen by LOI as the prevailing power. Then, identity management only seems to require some mitigating measures. LOI, and the same applies to PRIME and e-Citizen Charter, offers suggestions for strengthening the position of — here and there mistakenly called — the "user," while leaving the predominance of the traditional information holders essentially intact.

Of course our society doesn't come to a halt. Such frameworks may serve for some time, even when inadequate for the long run. Eventually, though, a qualitative shift in perspective is inescapable. In the

seventeenth century a civil philosophy of physical property originated, enabling accelerated social development. We are convinced that now a fundamental reconstruction is required for a civil philosophy of informational property.

Trust chains

Trust is often not just dialogically established, i.e. merely between two immediate participants in interactions. Especially when specialists make contributions, for example one specialist using information 'discovered' by another, they may even distrust the person as layman. She shouldn't interfere with … what essentially is her own information. And/or knowledge is deemed harmful to her.

We avoid making a radical choice as far as our framework goes. So, we accept that in some cases specialists cannot, or do not want to, perform adequately when they are (too) dependent on the person whose very information they're using, or even producing. We do make the provision, once again, that setting such limits to the person's control must be legally authorized, or even prescribed. Or, in the wording of iDNA-Manifesto:

14. The person designates a trusted party for controlling their restricted person information. The trusted party has been formally certified for its intermediary role (reflecting the requirement trust in social trans-/interactions).

Again, we draw special attention to the relational character of using and holding information. When the person cannot control some of her own information, at least let her be able to choose her intermediary for dealing with specialists and the like. But, then again, for the sake of reaching some social balance — more realistically, actually, for the sake of not straying too far from socially workable relationships for 'complex' matters, too — an intermediary should be recognizably accountable; as a certified professional, an intermediary's continued livelihood is dependent on 'trustworthy' performance.

We've already come a long way from iDNA-Manifesto's first article. Our fourteenth article reflects the insight that informational relationships usually involve more than 'just' the actors who seem immediately involved. A particular interaction often requires a host of preconditions in order to proceed successfully. Therefore, any viable framework for identity/information management also gives directions for *infrastructure*.

With iDNA-Manifesto, we've abstracted from, say, technical aspects of infrastructure. We've concentrated instead on more durable 'elements' necessary for behavioral feedback, resulting in improved social balance. Prominent elements are (legal) person, other party, government-as-object, government-as-process, intermediary and some further differentiations such as owner, user[16] and holder.

[16] Not to be mistaken with how LOI and PRIME apply the concept of user! For clarification, see throughout this paper.

Especially LOI contains a strong infrastructural flavor, but it remains limited to some technical aspects. We'll return to infrastructure where we go over LOI, PRIME and e-Citizen Charter to see what we might have missed in iDNA-Manifesto.

Eventualities

An intermediary as introduced in iDNA-Manifesto's fourteenth article is only eligible as such for a particular subject area, for example medical. It's not that the person is held to be generally unaccountable for her actions, but the intermediary serves the purpose of keeping the person at some distance. It leaves specialists 'free' to register what is person information, too, but what for legally supported reasons they prefer to keep from the person herself.

The final article of iDNA-Manifesto (version 2.1) addresses the eventuality that a person is, indeed, not accountable:

15. ***Upon formal declaration of the person's contractual incapacity, rights and duties concerning their person information, too, fall to their legal representative(s).***

With the person's death, the eventuality of course becomes a 'dead' certainty for which article 15 equally provides. None of the other frameworks considered here explicitly deal with a user's (LOI and PRIME) or citizen's (e-Citizen Charter) possible incapacity for controlling her own information. But those are facts of life, too, with social consequences; a framework for identity/information management should make appropriate allowances from within its boundaries.

The Laws of Identity

This paper has so far faithfully followed the order of articles in iDNA-Manifesto. For every article, we've looked at three other frameworks aiming to structure identity management in particular and/or information management more in general. We should now correct, at least somewhat, the bias inherent to our approach at comparing frameworks. So, for the next three sections we'll just go through each of the other frameworks, reporting on what didn't come through yet from the iDNA-Manifesto's perspective. Are there more relevant differences to explain? he first of the other framework that we investigate for such differences is LOI. We've already referred to LOI's first three laws, that is,

1. user control and consent
2. minimal disclosure for a constrained use
3. justifiable parties.

The fourth law is about

4. directed identity,

accompanied by a summary as follows:

> A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

As we've indicated, LOI applies the concepts of private and public with respect to the tightness of control over who qualifies as the other party in — potential — interactions. Information, then, is public when — as LOI calls her — the user doesn't exert any proactive control; anyone can have access, and subsequently use etc. the publicly available information. With private access, the user retains proactive control.

iDNA-Manifesto proposes the concept of agreement on usage rights. Thus, it abstracts from how to provide optimal support for — the great variety of — the agreements. On this issue, LOI and iDNA-Manifesto are clearly occupied with different conceptual levels.

More or less the same conclusion may be drawn when considering LOI's fifth law, entitled

> 5. pluralism of operators and technologies.

It says:

> A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

We even advocate strongly that an "identity system" is a both integral and integrating aspect of infrastructure for informational interactions. Given its, by definition, "universal" scope, technical pluriformity simply follows. It makes law 5 more of an acknowledgement, than a design principle.

With iDNA-Manifesto we're positively concerned with the functional level of informational interactions. Technical aspects of infrastructure can, and certainly will, display a variety while leaving functional integrity intact.

LOI sixth law, too, takes technical infrastructure as its point of departure. At least, that's how we understand

> 6. human integration

as described in LOI:

> The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine-communication mechanisms offering protection against identity attacks.

Leaving aside our confusion about identity system (as mentioned in the first five of LOI's laws) and now suddenly "identity metasystem," it is clear that the person must be accommodated … as "user." And by the way, what LOI requires for a/the universal identity (meta)system is not at all specific. Those are obvious requirements for any infrastructure. We won't repeat this observation, but it equally applies to the seventh law of the LOI framework which demands a

> 7. consistent experience across contexts

for which the following short explanation is supplied:

> The unifying identity metasystem must guarantee its users a simple consistent experience while enabling separation of contexts through multiple operators and technologies.

What we especially appreciate about LOI's law 7 is its emphasis on contexts. In fact, in an earlier version of iDNA-Manifest we had two articles under the heading of infrastructure, stating that[17]

> unambiguous differentiation according to context and time systematically guarantee information security.

We decided against retaining it for the current version, i.e. version 2.1. Semantically fundamental as the requirement is, we believe it detracts from emphasizing first principles for social equity in informational interactions. We called our framework a manifesto because we want to make explicit a political orientation. But, yes, infrastructural integrity can only be arrived at, and kept, from recognition of pervasive reconciliation between informational differences and similarities. So, we completely agree.[18]

Privacy and Identity Management for Europe

Principles, laws, or whatever, don't appear numbered in PRIME's framework. From our analysis of PRIME we've gathered four principles to guide identity management. As with LOI, starting from iDNA-Manifesto we've already referred to PRIME's first three principles

1. user-informed consent and control
2. privacy negotiation, agreement and dispute handling
3. data minimization and identity management,

in PRIME's case only leaving its fourth principle for our additional consideration. Its deals with

4. accountability

[17] Translated from the Dutch-language original text. The "security" is meant to cover aspects such as accuracy, integrity, reliability, flexibility and so on.

[18] One of this paper's authors pioneered contextual differentiation; context as a recursive function of object and relationship guarantee disambiguated reconciliation. See *Metapattern: context and time in information models* (Addison-Wesley, 2001) by Pieter Wisse. See also his paper *The pattern of metapattern*, in: PrimaVera, working paper 2004-01, Amsterdam University, 2004. Elsewhere (in a short, Dutch-language text), introducing the idea of civil information engineering as a new, much-needed discipline, Wisse calls the infrastructure for informational interactions an infrastructure *sui generis*. In fact, especially identity management exemplifies that the informational infrastructure should not just support but actually includes conceptual order as its very foundation. Were we to draw up a manifesto for civil information engineering, too, indeed we would make contextual differentiation its first principle.
The idea of another manifesto, one for civil information engineering, can help to clarify *iDNA-Manifesto*. In the latter, we've tried to keep out how supporting instruments may, or should, function. *iDNA-Manifesto* concentrates on human social behavior; we abstract from technologies. And now we can also point out how *The Laws of Identity* occupies a position somewhere between *iDNA-Manifesto* and — how we currently think about another manifesto for — civil information engineering.
Coming back to informational variety itself, metapattern allows conceptual precision for modelling, say, comprehensive differentiation. Metapattern-as-method is formally grounded on semiotics which it even extended

and prescribes that

> disclosure of personal information [must be commensurate with] reliable and accountable transaction processing [and] legal compliance.

This principle, too, demonstrates an assumption that is still opposed to our explicit allocation of information ownership in iDNA-Manifesto. We don't need such an article on accountability because our framework squarely places ownership with the (legal) person whom the information is about. It simply follows from her ownership that she is free to disclose her own person information, entering into usage agreements (with a default agreement valid when no conditions are explicitly formalized). Some later articles in iDNA-Manifesto limit her freedom in order to secure social balance. But still, the *principle* of personal information firmly stands.

PRIME never mentions information ownership, but seems to start from the assumption that person information resides beyond control by the person herself. Then, indeed, freedom to disclose person information doesn't follow at all. What is the legal basis for another actor to hold person information in the first place?

PRIME, as does LOI, for that matter, jumps in half-way. It takes current practice for granted, where indeed organizations all over keep a register of all sorts of person information. Instead, iDNA-Manifesto tackles problem analysis of identity/information management sufficiently close to the origin, that is, where the (infra)structural solution becomes feasible.

e-Citizen Charter

Are there any "quality standards" that we didn't treat yet from following the order of iDNA-Manifesto's articles? Out of e-Citizen Charter's ten principles, as we'd prefer to call them, so far we've commented upon the first nine:

1.choice of channel
2. transparent public sector
3. overview of rights and duties
4. personalised information
5. convenient services
6. comprehensive procedures
7. trust and reliability
8. considerate administration
9. accountability and benchmarking.

---

into so-called subjective situationism (*Semiosis & Sign Exchange: design for a subjective situationism, including conceptual ground of business information modelling*, Pieter Wisse, Information Dynamics, 2002).

e-Citizen Charter's tenth principle is titled

> 10. engagement and empowerment.

It says:

> As a citizen I am invited to participate in decision making and to promote my interests. Government supports empowerment and ensures that the necessary information and instruments are available.

What we make of it is that government rhetoric is only thinly veiled. Of course it sounds hospitable to extend an invitation to citizens. You're most welcome! But then, who is doing the inviting? Such a statement carries the implicit assumption that power one-sidedly resides with government-as-object. Out of self-interest, government apparently feels now 'forced' to act in a more enlightened manner. Act? As a proposed charter, they're still only words. Anyway, government retains its traditional power claim. For at best, government thus bestows a favor on 'its' citizens. Extending an invitation even serves to solidify the 'other' as the stranger. With an accepted invitation, the 'other' moves herself to a territory where she is expected to comply.

Ultimately, identity management is about the individual. Social psychology teaches that a person is constituted, as a human individual, by her social relationships. However, e-Citizen Charter doesn't really start from the person, subsequently positioning her socially. It continues to argue from the government-as-object position, instead, rather deserving the label 'e-government charter.'

The future of iDNA-Manifesto

We find it has been a worthwhile, extremely productive exercise to compare frameworks, all dealing in some way(s) with identity management. It transpires that different frameworks reflect various interests. Where such interests are in conflict, it shouldn't come as a surprise that corresponding frameworks don't match.

As the major 'bone of contention' we recognize the issue of information ownership. It needs to be resolved explicitly, formally, etcetera, in order for information society to continue to develop as civilization. With iDNA-Manifesto, we've made the radical choice for personal ownership, subsequently adding provisions for securing social balance.

Both LOI and PRIME seem to us ambiguous. That's quite understandable for LOI. It has been published, at the minimum with an outright authorization from a leading information technology company, Microsoft. It may therefore be concluded that LOI reflects how Microsoft sees its market(s) develop, with LOI also an attempt at influencing direction. Then it becomes clear that LOI's "user" is not credited for

making buying decisions for Microsoft's current and future products and services.[19] What we find interesting, though, is that LOI and iDNA-Manifesto are not necessarily incompatible. Actually, what we've learned ourselves from comparing these two frameworks in particular is that convergence is simply feasible when aspects are grouped at — what are usually called — levels. Keeping iDNA-Manifesto's predominantly political orientation intact, LOI adds some principles on infrastructure including 'the human use of infrastructure.' The other way around it's difficult to expect LOI being extending to include overt political commitments. We should remark, however, that abstaining from a choice … is always a choice, too. For it tends to reinforce the status quo. A commercially validated framework such as LOI may therefore be expected to change its — remaining to be implicit — assumptions only in the wake of consolidated political change. Of course, new business opportunities may be recognized in iDNA-Manifesto. Are they sufficiently interesting to have an impact on — a framework such as — The Laws of Identity at shorter notice?

PRIME's ambiguity is … double. On the one side it extrapolates concepts from traditional access control, i.e. where access is organized one isolated information system at a time. On the other side it takes an infrastructural stand. As with LOI, those opposing approaches are not properly aligned. The result is a framework without necessary and sufficient consistency.

Another ambiguity concerns the gap we recognize between what undoubtedly was a politically inspired commission to design a framework and its subsequent depoliticized execution by a consortium more representative of competitive technology suppliers. Political savvy in the sense of proposing a coherent vision of social organization in the information society would certainly have been a bonus with LOI. It cannot be blamed at all for side-stepping political commitments. For PRIME however, given its stakeholders we feel it is a level that it even should have addressed primarily.

Of course, we're only too happy to suggest iDNA-Manifesto as the framework at the level of social-political guidelines. We propose that PRIME and iDNA-Manifesto can also be made compatible. Before the attempt is made, we advise that LOI and PRIME are merged; PRIME seems already moulded after LOI, so that's an easy first step (conceptually, at least).

e-Citizen Charter has really disappointed us. Upon closer inspection, it's far removed from what it promises at first glance. But are e-Citizen Charter and iDNA-Manifesto incompatible? They are impossible to align, converge and so on for as long as the implied assumption on information ownership opposes what the latter's first article specifies, that is, we repeat,

---

[19] Yet, we also venture to disagree, though, because Microsoft earlier championed, at least commercially with astounding success, the personal revolution in the use of information technology. Lowering prices, software quickly became a commodity, allowing individual citizens to make their own buying decisions. Wouldn't it make obvious sense, then, especially from Microsoft's perspective, to place *The Laws of Identity Management*'s next version on a personal footing, too?

> [i]nformation about the individual (legal) person is the property of that (legal) person.

What we really don't find realistic is that the ownership title as implied by e-Citizen Charter is formalized for a democratic information society. Admitting to our own bias, a framework for identity/information management can only acquire consistency when starting from the radically practical idea of ownership of person information by … the person. From such a first principle for the information society, e-Citizen Charter can be easily redrafted. What it advocates for citizens, and of course we agree with redressing balance, is then given a solid foundation.

Do we expect to publish additional versions of iDNA-Manifesto? No, not in the near future, anyway. We would like to see it taken up as inspiration for making other frameworks — increasingly more — compatible. We feel confident that iDNA-Manifesto can serve precisely that purpose as it now stands. It supplies a vantage point for recognizing informational variety irrespective of scale. The essence of identity management is diversity across the information society.

references

Brate, A., *Technomanifestos*, Texere, 2002.

Cameron, K., *The Laws of Identity*, 2006, see *www.identityblog.com*.

Europe, *PRIME White Paper*, version 1.0, 2005, available at *www.prime-project.eu*.

IBM et al., *Higgins*, see for example *spwiki.editme.com/HigginsIntroduction*.

Jansen, P.L., *4891-Project iDNA*, 2005, in Dutch, available at *http://www.pauljansen.eu/materiaal/4891%20-%20Project%20iDNA.pdf*; for an English-language abstract, see *http://4891.pauljansen.eu/EnglishAbstract.html*.

Jansen, P.L., and P.E. Wisse, *iDNA-Manifesto*, version 2.1, 2006, see *http://www.pauljansen.eu/materiaal/iDNA-Manifesto.pdf*.

Lasance, M., *ID Management/IMS - Identity crisis?*, in: European Communications, 2006, available at *www.eurocomms.co.uk/features/features.ehtml?o=1446*.

Netherlands, *e-Citizen Charter*, see *www.burger.overheid.nl/actueel/?id=712*.

Wikipedia, *Identity management*, available at *en.wikipedia.org/wiki/Identity_management*.

Wisse, P.E., *Metapattern: context and time in information models*, Addison-Wesley, 2001.

Wisse, P.E., *Semiosis & Sign Exchange: design for a subjective situationism, including conceptual ground of business information modelling*, Information Dynamics, 2002.

Wisse, P.E., *The pattern of metapattern*, in: PrimaVera, working paper 2004-01, Amsterdam University.

Wisse, P.E., *Semiotics of identity management*, in: PrimaVera, working paper 2006-02, Amsterdam University, 2006.