

**Privacy Propositions:
notes for a talk at the 2007 Digital Identity Forum, 21/11/07.**

Peter Bradwell
[Demos](#)

Thanks a lot to Dave Birch and Consult Hyperion for asking me to come along and talk this morning.

I'll split the talk roughly into three; firstly, I'll try to give an answer to the question of who I am and where I'm from. Then through talking about some of our research, I'll outline Demos' current thinking around privacy and digital identity management. Lastly I'll hopefully offer some ideas about what kind of thinking could go into designing digital identity management systems.

I'll be talking about why digital identity management is a political activity; and about what it is that has made digital identity management such an important idea and industry in the past years. Digital id management requires some political choices, and the answers to these challenges have to be built out of a reconnection between people's everyday choices and the flows of information that they feed into. It's important because it increasingly affects, for example, what kinds of services people receive; and the opportunities they have open to them.

Digital management is central to this because it helps determine how much people are able to influence the way information about them is used.

I'll be basing the talk around the forthcoming Demos pamphlet called [*FYI: the new politics of personal information*](#), which is going to be launched on 7th December.

Today I will argue that growing connections out from the world of identity management and connecting between people, policy makers and technologists is vital to making digital identity management achieve what it should do.

I'm going to focus on personal information. If we needed reminding why all this is so current and relevant, yesterday's story about HMRC managing to lose the personal details of most children in the UK, and the bank account details for their parents. The media gods have been kind in giving us some food for thought on how important this topic has become.

This is Senator Ted Stevens, who some of you may know made an infamous speech a year or so ago about network neutrality in which he rambled about internet tubes getting clogged up. Im going to do what he should have done, and come clean about what Im not an expert in. I'm no expert in digital identity management - the finer details of the technology and systems that make it up.

But like the Senator there are a few things that I do know a bit about, and I think that means I have something to say about digital identity management.

About Demos...

Those things are social and technological trends, and some ideas about democracy, government and policy.

They are what Demos, which is where I work as a researcher, is about, and I thought it would be worth very quickly running through what Demos is about for those who don't know.

We're an independent think-tank, and a charity. We work with a range of organisations, from other NGOs and charities, government departments, local authorities to the private sector.

We look for long term thinking and solutions across a broad range of areas including families, education, science and innovation, identity, cities, public services, arts and culture, security. And we do a few things that don't really fit into any of those categories. We aim to be accessible and promote public understanding and knowledge of politics and social change.

But it's a virtue to see yourself as others see you I thought it might be useful to start with a few quotes from newspapers about us; the first is from the financial times, and I think we're pretty happy with that. It's quite positive. The second is a little more sceptical about our worth, from the times.

Everyday democracy...

We call ourselves the think-tank for 'everyday democracy', and we're interested in addressing the crisis of democratic legitimacy that politics seems to have befallen. There are a range of depressing statistics about how many people don't vote, and how political parties are hemorrhaging members. But we argue that renewing the political sphere and finding more legitimacy for our democratic system needs more than just bumping up the voting stats and making changes to the formal institutions of democracy.

It means reconnecting individuals and their experiences with the broader public implications of their behaviour and decisions. So we work broadly to think about people's individual decisions in everyday life can contribute to a common good.

That's Demos, and the story we try to tell about Everyday Democracy is one that I'll come back to, as it's really relevant to the problems of personal information that we focused on in the project we recently finished writing up.

It focused on why personal information is valuable; the significance of an increasing reliance on it; and how these map onto the value the public attaches to personal information, and their understanding of it. The broad aim of the research was to think about how to make personal information, and what happens to it, something that people have more of a stake in.

The 3 arguments I'll be making today are...

Firstly - and stating the obvious - we live in a surveillance society. But that's not all bad news. This isn't something that we are subjected to; this isn't just about the whims of a malevolent Big Brother. While we need to guard against what it is that large information handlers do, its important to also focus on the many benefits of being part of an open information society. And to acknowledge that surveillance is as much about how we watch each other as it is something that happens to us.

But there is a tension between empowerment and control. it is impossible to separate the benefits we get from being part of a society rich in personal information, with the challenges and dangers of giving so much information away. because just as sharing more personal information can bring people may benefits, at the same time there is a risk that giving personal information away can mean people have less control over decisions about them.

Technologies of digital identity management need to be a part of reconnecting individuals to the flows of information around them. The challenge is to make sure that technology helps to build an environment in which people remain connected to the information flows around them. because of the decisions that get made about people on the basis of personal information, there is a responsibility for technology developers and those working in the field of digital identity management to be sure that the tools they are building embody democratically legitimate principles about information use.

So what does this have to do with privacy or digital identity?

Privacy is intimately associated with ideas about how we relate to the people and institutions around us - the kind of things we want or expect to know about them, and them us.

It is often thought about in terms of drawing limits of access - drawing boundaries certain people can not cross. That's a fair metaphor. But focusing on that too sharply can mean that sometimes, discussions about privacy stick too firmly to arguments about putting up barriers and boundaries and safeguards. Part of the value of privacy, however, is that it is closely related to the value of self-determination; and of being able to influence how others see you.

Privacy is not just about whether or not you are seen, or surveilled, or intruded upon.

It's about how those things happen; it's as much about how you are seen.

So three of the concerns around privacy are...

- 1. who 'sees' us, and when;*
- 2. what they think when they do;*
- 3. what they do about it.*

There are some trends that have changed how much control people have over these three concerns:

It is more likely than ever that details about our everyday lives will be available for others to see. Secondly, we are more interested in being part of a world in which that is the case. and finally, the way that other people can influence or decide about what we do has changed.

It's called personal information not just because it is about us, but because it increasingly has significant and very tangible consequences for our everyday lives - the kind of public services we experience, for example.

These aren't all down to the stealing of data or the access to it. This can be as much about the way that organisations *legitimately* use personal data.

The problem of privacy, then, as we see it is that it is now as much about talking about promotion as protection. Privacy also means being able to influence the things that people know about you.

So, what has changed?

Firstly, as I have mentioned, we live in a surveillance society. We've all seen the stats about how many cctv cameras there are filming us going to buy stamps, crossing the road and going back home. - and about passenger information; medical records; and so on.

There are a number of trends driving this. Firstly, security obviously plays a part. That is part of government's continuing desire and need to manage the population. Because of some other changes to how that population looks, such as bureaucracy increasingly relies on, broadly, surveillance.

But equally important is the trend towards services tailored towards the individual - whether it be personalising services in the public sector or customer segmentation practices in the private. Our interactions with institutions searching to provide this personalised service are predicated on them knowing more about us. And that means more 'surveillance'.

This is not only driven by institutions, but the demands of the public too. We enjoy and demand more personal services. We leap to use more convenient online shopping sites. Many people love putting photos of themselves covered in vodka on social networking sites. Further, not only do we live through being watched, but equally we experience a *need* to be seen.

Globalisation has meant much greater flows of people, ideas and culture. In a world marked by transnational flows of people and multiple identities, traditional monolithic identities such as class, race, nationality and political allegiance often overlap or become more complex. Our sense of identity and sense of self are, as a result, less stable. The negotiation of ideas, our sense of self and how people relate to each other has as a result become something of a compulsion - it has become more fraught.

A big part of this story is the proliferation and democratisation of the means of communication. People have greater potential to relay their experiences of everyday life back to each other, and these new ways to communicate serve a broader need. Greater insecurity in the sense of attachment and identity places more importance on the points at which people come to understand themselves, and their position in relation to other people. The fascination with celebrity and the now fading love af-

fair with reality television suggest a culture enamoured of display. Social networking sites like MySpace and Facebook work through a kind of fervent associative clamour, giving people the means to differentiate their 'profile' through the people, music, photos and opinions they connect with.

As well as being something we are subjected to, surveillance, in its broadest sense, is something we are willing to be a part of. And we seem to have the tools and willingness to work out who we are for ourselves.

But does this really mean that more people can take part in what surveillance is for? Does this 'interpersonal surveillance' mean people are busy sorting, judging and responding to the people and ideas around them? The rhetoric of new media, social networking and web 2.0 always suggest so. But there are some problems that mean the reality is at the moment not up to speed with those promises.

The normalising of surveillance and our reliance on personal information multiply and change the places and spheres in which people can learn things about us, and where they can potentially come to make decisions about us. That means that as well as being about us negotiating for ourselves our sense of self, the way this happens gives others more of the raw material of more traditional surveillance and control - personal information. That makes it more likely that they can take decisions about us without our consent or knowledge.

The mobile phone

For example, how many people realise the ways that they are being, and can be, surveilled when they use their mobile phone? This is a new set of information that can be used to make judgements about us, or be used to tailor a service or response around those judgements. It is a new context in which we have to consider the kinds of inferences others can make about us. The mobile phone is a great example of the disconnect between our social, everyday experiences of the way our digital identities are so important to many of us, and an institutional sense of our digital identity.

They are often personalised visually - with stickers, scratches or covers. They take photos and videos and sounds from our everyday life. And they play the music, ringtones and voices we associate with. All those things transmit messages about who we are. they are messages we feel we have a lot of control over. most people have a feel for the fashions and trends and norms of this process. Its something we can influence.

But there are other messages we transmit - less colourful, noisy and creative, perhaps, but just as influential in determining how people understand who we are. There are a host of new contexts in which we have to consider how it is that people see and understand us. At the moment, the most important disconnect in terms of privacy is that between the ease with which we have taken to these tools of personal convenience and communication and creativity, and the flows of information they feed in to. That is a problem.

We care...

It is important to say that these complaints about privacy aren't just limited to the whining of privacy advocates or social policy wonks.

People care about privacy:

90% worry about organisations keeping personal information secure

60% believe they've lost control over their personal information

94% are concerned that organisations sell their details without permission.

And in the Oxford Internet Survey, 70% of respondents felt that going online endangers the users privacy.

There's also no shortage of media interest. Yesterday was particularly notable. Similar stories appear every few days. They often reference public sector information gathering, but increasingly acknowledge the blurring lines between private and public databases.

For our research, we spoke to people of all ages as part of our focus group work, and yes. They do care. From the older users who were broadly more fearful about the idea that it is easier to find out about them, to younger participants of the research who often expected the kind of control over what they share so freely to be matched by control over what happens to it once it's out there, or surprise at the the consequences of being so open.

But we're not sure why...

So, we care. But - we're not really sure why. That's because it can be difficult to follow the new contexts in which we are sorted and judged, and the sorts of influence different people have over us, the accountability those people are subject to.

The way that institutions gather and use information can be opaque, and difficult to grasp. Though people are beginning to understand how their information, with or without their knowledge, is used and what the implications are, that understanding is marked by ambiguity. The findings from our research suggest that this stems from an ambiguity around the consequences, responsibilities, accountability and control associated with the use of personal information.

Underneath the surface of our acquiescence to consumer convenience and choice are serious issues of power and control. Because of these ambiguities, in the individual risk assessments people take, convenience is often more heavily weighted than the vague notion of control or privacy. As personal information has become one of the key ways that judgements are made about people, so the concern is that without real engagement in how that happens those are decisions that lie further away from individuals they concern. The problem is that its difficult to figure out where influence lies; and more narrowly where influence over personal information policy can be exerted.

These ambiguities stems from merging roles of private and public private sector. This is perhaps the most important factor in the development of personal information use. This has served to exacerbate the questions of power, responsibility and coercion in both.

It coincides with an increase in demand for good quality, comprehensive data, and competition among data suppliers, making connectable information about every aspect of an individual's life easier to come by than ever before. Personal information has become, as a result, less easy to segment in terms of what is relevant for public or private sector purposes.

So: we're not really sure about how all these changes have impacted on who sees us and why it matters. That helps to explain why it is easier to point to statistics about how 19 nectar cards are swiped every second in the UK than it is substantial public outcry over a world reliant on personal information.

Privacy is political

Privacy, then, is political because it is about figuring out where this influence lies. It is about making sure that it doesn't get lost beyond the reach of the individual it influences.

It should be about making sure that everyday behaviour does not get disconnected from the decisions that influence people and exert power over them. Just because the idea of direct control over our behaviour has increasingly lost purchase, it doesn't mean coercive power doesn't still exist. Not being able to connect to the specific information practices and policies contributes to this fear.

It's impossible to separate the benefits of living in an open information society from the challenges that come with giving away so much personal information. There is a tension between empowerment through information and control by it. This tension is embedded in a society which thrives on everyday surveillance. From personalising services, to consumer research to social networking, our interactions with people and institutions are increasingly mediated through, or involve, personal information. And with that comes the promise of more grassroots negotiation of identity, but the dangers of traditional forms of surveillance and control.

Phil Collins and the Turner Prize

As part of his 2006 Turner Prize display, the artist Phil Collins set up a working office under the name 'shady lane productions' in Tate Britain's exhibition space. He and his staff worked nine 'til five researching 'the influence that the camera exerts on the behaviour it seeks to record'. Their work drew on the experiences of people who have suffered from the compelling draw but often unseemly aftermath of involvement in reality television.

The focus of the exhibit was the power of others' eyes, and the ways that our behaviour changes before them. But the office itself stood within a high-profile, popular art competition. The lives of those within it became the subject of visitors' inquisition – visitors who were asked simultaneously to interpret the meaning and value of the piece itself while comprehending the significance of the job, behaviour and reactions of 'shady lane' staff.

People stared and peered in, looking for answers from the office workers. Gallery attendants and closed-circuit television oversaw the public's reactions. Seeing all were the judges of the competition, charged with ascribing the institutional value of the exhibits, the public's views left on walls of postcards accumulated at the end of the show.

In the gallery, there was no escaping the watching; just inferences about the power that different people hold while it is happening.

Part of the focus of Collins work was the force that other people's eyes hold - to interpret what they see about us in a way they choose.

Its a great diagnosis of our culture today. Because it illustrates how there are many different spaces in which we are seen and judged, and the angst which we feel in trying to figure out what that means.

That problem is something that digital identity management can be part of solving.

Personal information and the way it is used matters politically, and democratically, because it is intimately connected with how we are seen, represented and treated by the people, organisations and institutions that hold influence and power over us. It influences the 'space' that we have to decide and negotiate who we are. It grows in significance, but it becomes more difficult to control, in an era in which people so readily give away their information in exchange for the immediate and social benefits of sharing details about themselves; where institutions increasingly rely on it; and the consequences of its use or misuse are growing in significance if not clarity.

By sharing personal information we risk surrendering control in the longer term by leaving ourselves open to judgement by different groups in different ways. The drive to personalise or tailor services, which is shaped by those judgements, can lead to differences between what people experience and have access to. This can mean a narrowing of experience, can lead to social exclusion, and has significant implications for how we live together as a society.

Privacy is politically important because the way we value it, design for it and legislate for it embeds an individuals ability to influence what people think about them; and how institutions 'see' and understand and respond to them.

The meaning and value of personal information

So on the one hand, openness and a rich information society gives people the chance to negotiate their own sense of self; through things like myspace; with their mobile phones. With their t-shirts or their friendship group. But on the other there is a risk other people have the means to make those decisions for us.

At the heart of this is the tension between institutional and individual claims.

A good parallel is the music industry. On the one hand, the proliferation of music is a good thing. More easily exchanged music from and opinion about a band is a good thing. More exposure, more fans, more buzz, more gig sales, more shared culture. On the other, however, the proliferation of means to share, experience and discuss music happens out of the reach of those who claim to own the rights to it.

That means a tension between the organisational interests of the record labels and artists, with those who argue for the social and cultural benefits of democratised means of music production and distribution.

Music has both a value, and a broader meaning. And as with these other 'tradable' intangibles like music, personal information also has both a value and a meaning. The value may be easier to barricade and form rights around, but the meaning of personal information is something that requires much more open and fluid negotiation. It can sometimes feel difficult in the case of music and pop culture to make the case for a situation in which the rights of a few impact too strongly on the broader benefits other claim - the rights of the music industry make more sense to the courts and juries involved than less tangible arguments about 'free', bottom up culture.

But arguing for this open attitude in the realm of personal information and identity - where the ability to challenge, debate and construct new meaning around our relationship to other people is fundamental to a functioning democracy - should be easy. This is a theme Laurence Lessig has consistently drawn out; and in a talk in New York earlier in the year, he discussed how the same arguments about free culture - that we need the ability to access the currency of popular culture - apply to politics, too - we need to be able to critique, think about the people, ideas and politicians and their ideas as openly as possible.

So it should be easy to argue for and create an environment in which people have a strong stake in debating how personal information is used. Because decisions made on the basis of it play an increasingly important role in shaping institutional responses to people, and therefore influencing important policy areas like service provision, or the state's role in responding, for example, to social inequality.

But at the moment it is not. Too often, despite the rhetoric of convenience and empowerment around the information society, the institutional or organisational benefits outweigh the claims of individuals.

We do not expect to exert full control over what is said, known or thought about us. Bits of information are needed about us by others, usually governed by principles or rules about when and where it is appropriate for people to have access to that information. When we want to buy a house, the bank lending us the money to do so might run a credit check - the information fed to them is the basis on which they can make a judgement about the kind of people we are. Less instrumentally, people need to share and learn about others; to share thoughts and feelings to build a sense of understanding of the world around us. Usually, there are means of redress if a person believes another's opinion is incorrect or damaging in some way.

There are some serious benefits to allowing others to use and share personal information, from better health care, safer places, cheaper clothes and more efficient public services to the connections we can make socially or culturally. But at present people are too far removed to wield any serious influence over where and how limits and regulation work.

people need the ability to influence those decisions and policies. because people's worth and value is going to be shaped increasingly by the things that their personal details say about them. the way that

information singles us out has serious implications for our experiences. so being able to reconnect with those decisions is becoming increasingly important.

Digital identity and politics

'Digital identities' – either the ones we actively help produce or the identities held in electronic form by institutions – are increasingly as intimately a part of these processes as people's offline selves. Personal information is the raw material for this, and DIM offers a simple question: how do we think we should prioritise claims over how personal information is managed? But that simple question isn't actually that simple at all. Because of the problems I mentioned earlier it is more likely at the moment that institutional - private and public - interests will dominate the voice of individuals.

In October 2007 the All Party Parliamentary Group on Identity Fraud warned of the dangers of people's fervent desire to use social networking sites. Our loose lips in the informal connected realm see us freely displaying our phone numbers, addresses and birthdays. The group recommends that government play a role in deepening people's understanding of the dangers of carelessness in what we show to whom, and in explaining just how useful and valuable personal details online can be to fraudsters.

Why is digital identity management so important to this? Crucially, the connections between the more organic understanding of identity and the institutional understanding are missing in the parallel debates about the social values of technology and bureaucratic identity. Importantly, with the increasing interdependence between on- and offline worlds many people's 'digital' and 'real' identities are barely separable. But it is difficult to make the connection between a general willingness to use technology to build incredibly personal profiles and reflections online, and the more technical understanding of what our 'identity' is. Connecting our social identity with 'identity' in a more technical sense – the details businesses and institutions see and interpret – is difficult. How we use technology is important in this process – rather than digital identities being separate from our 'real' self, for many of us they are more and more important to how we build a sense of who we are.

What has been difficult to reconcile so far are the everyday interactions from which information about us is passed to others, and the long or short term implications of giving away that information. As I mentioned with the ideas around everyday democracy, democratically legitimate practice extends to the clarity of connections between our decisions and behaviour and the broader implications of it. Those connections are lost in the case of personal information. And that matters, because there are serious consequences of not having a sufficient stake in this - for how people are seen, managed, governed and provided for.

So digital identity management embodies unavoidably political decisions regarding public services, government intervention in inequalities and the state's role in managing the population. The tools that get designed around personal information use can make it more or less likely that policies around those issues lie in the hands of individuals and the public rather than institutions. Because technology can connect people's individual decisions and behaviour to the processes through which decisions about them are made - by connecting them with the flows of information around them and placing the individual at the centre of it.

The questions to be answered are: how heavy do we want the rights of individuals and institutions to be? Giving too much power to the 'owner' of the personal information would be too constrictive, just as giving too much to the data holder – the e-retailer, the marketing firm, the government – removes the element of negotiation. Different technological 'architectures' allow information to flow in different ways. In the way technology is designed, there is an opportunity to embed the level of control an individual has over their personal information. In the choice between the top-down and bottom-up models lie these questions of control, autonomy and power. The choices are bound up in broad political challenges associated with information, openness, and the role of government.

They directly affect whether people are empowered or controlled by information. And they are also, crucially, bound up in how responsibility is balanced between individuals, institutions, organisations and the state. So digital identity management is essential in helping to place people at the centre of an information society, and to offer democratic engagement.

The way personal information is legislated for and designed for influences the 'space' that we have to decide and negotiate who we are and how we feel. It grows in significance, but becomes more difficult to control, in an era in which people readily take advantage of consumer convenience; where we flock to the engaging tools of social networking; where identities form along unpredictable lines, with unpredictable consequences; and where the state apparently has less of a claim to influence, determine or manage them.

These are questions that technology on its own can not answer.

Digital identity management is essential in helping to place people at the centre of an information society, and to offer democratic engagement in it. These problems obligate people designing technology to ground their work in a focus on engaging with the public, and developing links between their practice, people and policy makers.

PROPOSITION ONE

The work of digital identity management needs to be in the simple language it deserves. One of the established principles of data protection is that personal information gathering should be done on the basis of informed consent. But given there is a sense of information asymmetry – much greater knowledge on one side of the interaction than the other. People are often unaware of, and not invited to engage in, the context in which decisions about information use are made. So far, data protection law has not in itself provided adequate means for democratic engagement with these principles beyond the redress offered through norms regulated by the Information Commissioners' Office.

the complexity of language and technical details associated with dim can be off-putting. DIM is often seen through the lens of technical possibility, meaning that discussions of people's practical and everyday aspirations – how they want to use technology – become secondary, overshadowed by technological boasts about decentralised or centralised networks or splendidly complex cryptography.

It is a failure if the language and practice of identity management or data protection is too complex for non-technologists or non-experts to understand, because this process is fundamental to the way that institutions, businesses and other people find out about who we are and decide how to react to us. This is going to be increasingly true, as technology becomes ever more central in mediating 'relationships'.

PROPOSITION TWO

DIM shouldn't be seen, as sometimes it seems to be, solely through the lens of technical possibility. As a bridge between people, policy-makers and technologists, there needs to be much greater emphasis on collaboratively shaping what it is technology does. It is answering some long term questions about the relationship between people and institutions that hold influence or power over them.

There is a responsibility for technology developers and those working in the field of digital identity management to make tools that embody democratically legitimate principles about information use. A body such as the ICO should be given the remit and resources to lead open discussions and debate to help build more secure, effective and appropriate technology for personal information. Part of this means that tech companies need to be better at making themselves be seen as legitimate part of the debate, rather than just interested in selling product. The key point is that there needs to be a much more engaged relationship between the people building digital identity management systems, the public, and policy makers who make demands about where people's information should be used.

I am my information

Having more information available to more people – quicker, easier to access and on demand – means that personal information has become a more important commodity than ever before. For this reason an open debate about information policy and practice, that engages the public, industry and representatives across government, cannot just happen on data protection and identity fraud grounds. A democratic approach to personal information means finding clear limits and rules on information use. That needs to be based on a sharper understanding of the role of the state, connected to an openness about the sorts of information it will need to perform it. That, in turn, rests on a longer-term debate about the sort of support and interventions people want and hope for in future, personalised services.

We casually leave trails of information behind ourselves. But data and facts retain a significance well beyond the convenient transactions they may have been generated by. Here, the personal becomes political. Democratic policy on personal information, then, means maintaining the spirit of collaborative openness that information technologies promise. To achieve that, we need collective rules about when and where individuals have the right to control, or influence, the use of the information that increasingly determines their worth.

So, that's about all. Thanks a lot for listening, I hope some of it was useful.

We'll be launching the pamphlet that talks about all this in a little more detail on December 7th 2007 - you're all most welcome to come along. Just drop an email to demos_fyi@demos.co.uk. We have Information Commissioner Richard Thomas, columnist Bill Thompson and comedian Nathalie Haynes joining us so it should be a great event.

Thanks very much.