IDIS (2010) 3:657–674
DOI 10.1007/s12394-010-0079-2

Public sector engagement with online identity management

D. Barnard-Wills · D. Ashenden

Received: 29 January 2010 / Accepted: 29 October 2010 / Published online: 23 November 2010

Abstract The individual management of online identity, as part of a wider politics of personal information, privacy, and dataveillance, is an area where public policy is developing and where the public sector attempts to intervene. This paper attempts to understand the strategies and methods through which the UK government and public sector is engaging in online identity management. The analysis is framed by the analytics of government (Dean 2010) and governmentality (Miller and Rose 2008). This approach draws attention to the wide assemblage of public and private actors with shared regimes of practice and fields of visibility, as well as to the extent to which individual actors are made responsible for their own identity management. The paper also uses communication and discursive research to examine the potential failings of engagement efforts. Communication theory suggested that the assumption of individual responsibility, alongside linguistic distortions created by this way of understanding the problematic of identity management, complicate and fundamentally limit engagement activity.

Keywords Identity management · Government · Public-sector · Political science · Communication

Introduction

This paper attempts to understand how the UK government and public sector is engaging in the field of online identity management and the form this engagement takes. The individual management of online identity, as part of a wider politics of personal information, privacy, and dataveillance, is an area where public policy is developing and where the public sector attempts to intervene. It is a site of interaction between governments and publics where a politics of information technology is played out. Much of this interaction occurs through public information campaigns. These campaigns attempt to provide advice and guidance to enable individuals to manage better their online and offline identity and the security of their personal information. Issues of engagement

D. Barnard-Wills (✉) · D. Ashenden
Informatics and Sensors, Cranfield University, Shrivenham, Swindon SN6 8LA, UK
e-mail: d.barnardwills@cranfield.ac.uk

around identity management and online security have implications for a range of political and technological debates as technological issues increasingly become part of daily government, as well as daily life. Identity management also impacts upon debates surrounding privacy and consent online, as well as the proper role of states in this field.

Engagement can be understood as getting people to think about the issues or to have them as part of their world view. Engagement is therefore a mix of communication, interaction and interest, with the implication of (at least) a two-way communication process. Engagement is used as an inclusive term to describe the broad range of interactions between people, including a variety of approaches, such as communication or information delivery, consultation, involvement and collaboration in decision-making, and empowered action in informal groups or formal partnerships. The importance of fully exploring the social issues of technology politics was made in a March 2005 Council for Science and Technology (CST) paper which identified the need to, 'stimulate exploration of the interconnections between scientific, economic, social, ethical and environmental issues' (Council of Science and Technology, March 2005a). A second CST paper emphasises the importance of engagement and the link with trust, suggesting that: 'Without an open dialogue on all the implications of better linkages between, and access to, personal datasets, there is a risk that the public will be mistrustful of government's actions'(Council for Science and Technology, November 2005b).

The public sector is here drawn so as to include central and local government, non-departmental public bodies, and independent authorities such as the Information Commissioner's Office. We also include organisations that cross the divide between the public and private sectors, such as CIFAS, the UK's Fraud Prevention Service. This boundary is flexible and fluid. Identity management engagement and communication strategies bring together a wide range of public and private actors. Get Safe Online, the National Identity Fraud Prevention Week and Identitytheft.org.uk all draw together a range of actors in such an assemblage, whilst the ID card scheme, the National DNA Database and the NHS IT system also include a range of actors. There are further actors communicating and engaging in the field of online identity management, including academia, as well as commercial enterprises selling identity management services or technologies.[1] In order to focus upon the logic of public sector engagement, these actors are not the subject of this paper.

The analysis here is framed by Mitchel Dean's analytics of government (Dean 2010) and the governmentality work of Peter Miller and Nikolas Rose (2008). This theoretical approach to the study of government provides a number of perspectives that cast light upon public sector engagement efforts in general, and upon identity management in particular; particularly that government is best conceived of as an assemblage of actors, oriented towards shaping conduct of populations. Government orients towards specific 'problematisations' and makes individuals into responsible actors. The paper also makes use of communication and discursive research in order to examine the potential failings of engagement efforts. We argue that although fundamental, looking at the engagement activities themselves only captures one side

[1] See for example the 'DataPatrol' service provided by garlik.com. for £45 for a 12 month subscription, the service offers 'early warning protection and alerts if your information has been compromised and you are at risk of identity theft and financial fraud.' Galik is by no means the sole actor in this developing marketplace.

of the interaction. It is therefore necessary to examine the impact of these efforts. There is existing research in this and similar areas, but this is limited by the narrowness of the measures used and a number of methodological barriers.

It is hoped that a research strategy including the multiplication of narratives of personal privacy, including online identity management, and presentation of those narratives through multiple vectors might produce alternative ways of conceptualising online identity management that could be incorporated into public sector engagement efforts in a way that satisfies the three demands of verisimilitude, public sector needs, and accessible and effective forms of communication for the diverse variety of the population. A direction for this is outlined at the end of this paper.

Online identity management

'Online identity management' is understood as any attempt to consciously manage or control the "growing mass of information about ourselves and our social or business transactions and relationships that exists in digital form whether stored within commercial or government databases or scattered on the Web in blogs and social networking sites"(Evans-Pughe 2008). It arises from a desire to control personal information in an interconnected online environment. According to Solove "we often don't want absolute secrecy, instead we want to control how our information is used, to whom it is revealed, and how it is spread"(Solove 2007).

Identity management differs from concepts of 'impression management' in that it deals with the security of personal information. Online identity management involves not just the 'presentation of self' as discussed in the Goffman-inspired sociological literature (Ellison et al. 2006) but also a (potential) response to a range of threats arising from the proliferation of personal information online. These include but are not limited to: fraud, invasions of privacy, economic harms, discrimination, and exclusion from opportunities (Solove 2008). Reputation can be a key element of identity, and affect our ability to engage in basic activities in society (Solove 2007:31).

We would also differentiate the term from 'identity assurance', the practices through which organisations verify the identity of an individual, and therefore focussed upon institutional rather than individual or social priorities. This approach has origins in information security and regulating access to systems and databases. The Information Assurance Advisory Council defines identity assurance as:

> "A framework of technical, management, policy and regulatory initiatives aimed at preserving the confidentiality, integrity and privacy of identity related data, as well as the availability of information infrastructures and supporting identity management systems." (Information Assurance Advisory Council 2005).

'Online Identity Management' focuses upon the individual level. Finally, using the term 'identity management' also has the benefit of drawing attention to the way in which managerial practices are re-articulated from an institutional frame to be used by the individual upon themselves, and the manner in which the individual is situated as the locus of responsibility; required to monitor, understand and intervene in their own identity. This attribution of reflexive responsibility to the individual is a key feature of liberal governmentality.

Governmentality

Building upon Foucault's work on liberal government, territory and population, the governmentality approach has been developed into a political research perspective beyond the historical and applicable to contemporary political issues. Further, it avoids the functionalist domination of which Foucault's earlier work on discipline has (somewhat erroneously) been accused. Governmentality focuses upon the way that thought is made practical within governing assemblages, and pays attention to the vocabularies and technical interventions of government. Following Foucault, government is understood as the 'conduct of conduct'. This definition plays upon conduct as in 'to conduct oneself' and 'to conduct' as to lead, direct or guide. It encompasses self-direction, guidance and regulation. Government therefore is any attempt to shape with some degree of deliberation aspects of our behaviour according to particular sets of norms and for a variety of ends. Engagement efforts and strategies around online identity management are therefore conceptualised as a particular strategy of government intervention, and a way to influence the conduct of governed populations.

Government is therefore linked to assumptions about how people, as autonomous individuals capable of regulating their own behaviour, should conduct themselves. In this sense, online identity management, as a subset of identity management more broadly, becomes part of positively evaluated conduct for individuals. The various lists of advice, guidance, techniques and strategies put forward in the various engagement campaigns provide this description of appropriate conduct. Following Latour, techno-scientific practice can be a more effective tool of political intervention precisely because it is frequently depoliticised. This should prompt attention to seemingly a-political activity such as OIM communication.

The analytics of government would not consider such guidance an authoritarian move, rather an attempt to direct conduct in the most 'productive' manner. However, this move would be associated with the 'new prudentialism' (O'Malley 1992) in which individuals and families are made responsible for their own risks. Miller and Rose have termed this 'privatised risk management' in which the citizen is 'enjoined to bring the future into the present and is educated in the ways of calculating the future consequences of actions' (Miller and Rose 2008:215). In demonstrating the need to protect themselves from online identity fraud or exploitation, this governmental guidance becomes one of a number of:

> "Instances of contriving practices of liberty in which the responsibilities for risk minimisation become a feature of the choices that are made by individuals, households and communities as the consumers, clients and users of services." (Dean 2010: 214)

This suggests attention to the way that OIM engagement constructs and positions the individual as primarily responsible for managing their online risk.

From the governmentality perspective, the practice of government is seen as an assemblage or as a regime, and not reducible to particular single totality. Critical of traditional theories of the state, government is 'comprised of heterogenous elements having diverse historical trajectories, as polymorphous in their internal and external relations, and as bearing upon a multiple and wide range of problems and issues' (Dean 2010:40). There are a plurality of governing agencies and authorities, and this

perspective supports the wide definition of the public sector used in this paper (Dean 2010:18). The extent of a governing assemblage can be identified from the extent to which regimes of practice are consistent across multiple actors. This paper demonstrates that in with regard to online identity management, there is a substantially consistent regime of practice across government.

Whist it provides a strong basis for analysing the intentions and reasons for the engagements efforts on the part of the public sector, the analytics of government theory cannot, by itself comment on the effectiveness of these efforts, or the extent to which the guidance – the strategies and tactics of identity management – becomes taken up by various groups in society and effectively made part of their conduct. This requires a further examination of engagement efforts and communicative theory, and it is to this that this paper now turns.

Public sector engagement efforts

The benefits of engagement around online identity management are potentially broad. The issue has strong parallels with other issues of science and technology communication and public engagement. The Cabinet Office report 'Transformational Government' identifies the need to, 'Systematically engage with citizens, business and front-line public servants' (Cabinet Office 2005). Issues involving legislation involve engagement through the public consultation exercises by the appropriate government department. For example, the Home Office published a consultation document on identity cards secondary legislation in November 2008, (Home Office 2008) and a response to that consultation in May the following year (Home Office 2009). The government believes that consultation on legislation is in the interests of good government, and informed and rigorous public debate (Office of Leader of House of Commons, http://www.commonsleader.gov.uk/output/Page2449.asp).

The first stage of an analysis lies in identifying the activity that the public sector is undertaking in the field of online identity management and public engagement. This overview draws upon a number of case studies; the Information Commissioner's Office, Get Safe Online, www.identitytheft.org.uk, and the National Identity Fraud protection week. Alongside these, we draw upon existing researching into identity cards, the national DNA database and the NHS patient care records launch.

The Office of the Information Commissioner was created by the Data Protection Act 1998. The role and profile of the Information Commissioner increased substantially with the passing of the *Freedom of Information Act 2005*. The office has two main responsibilities, data protection and freedom of information. The ICO holds statutory and regulatory powers but it is not a government ministry or department. ICO sees education and influencing as two of its four main functions (the others being resolving problems and complaints from the public, and enforcement, directed through legal sanctions against those who contravene data protection legislation) (www.ico.gov.uk). ICO has also been heavily involved in efforts to combat identity based crime, as part of opposing exploitation of personal information more broadly, and considers its communication strategy successful (Information Commissioner's Office 2009).

ICO's education and influencing communication objectives related to identity management are: to 'maintain awareness of rights among individuals, encourage

good practice, and maintain 'confidence in organisations' handling of information (among individuals)'(2009:4). ICO is aware of the need to engage with a diverse audience including consumer, youth, ethnic and specialist media (2009:17), and aims to explore the provision of educational materials for schools and young people. ICO's communications budget increased from £700 k in 2004 to £1.5 m in 2009 (2009:35).

ICO's website, publications and press releases present a wide range of identity management strategies and behaviours that the individual is prompted to engage in. These are frequently linguistically addressed to the individual reader – 'you', 'your information'. A number of these are presented in the 'personal information toolkit' (Information Commissioner's Office 2007). Much of this is written in a deontic modality, referring to necessity or obligation and with very few 'hedges'. In effect, this is an authoritative list of positively evaluated conduct, which should be followed.

ICO appears to have (and express) a nuanced view on surveillance. Whilst personal information collection and processing, and potentially privacy intrusive practices are critically evaluated, they are not totally discredited, nor evaluated exclusively in pejorative terms. ICO therefore occupies a position between an unquestioning acceptance of broad surveillance practices (perhaps in pursuit of other objectives such as crime prevention) and a blanket opposition to all surveillance practices. Identity management (or protection individual personal information) is seen as a laudable institutional goal and individual activity.

The Information Commissioner's Office has commissioned annual survey research on its communication activities and understanding of data protection legislation (SMSR 2008). This takes the form of a telephone survey, conducted by a social and market research company. The aim of this research is to gauge awareness of data protection legislation and rights and to understand perceptions of how organisations handle personal data. The conclusion of the 2008 report is that:

> "The public are engaging more than ever before with the issues of data protection and freedom of information – in particular, how they are manifested in everyday society (rather than on a formal, legislative basis). In short, the Acts are becoming increasingly relevant – particularly amongst the young (18–24s) and the upper social classes. The principles behind the Acts are being communicated to the public. And appreciation of the Acts is increased with knowledge and education about them." (SMSR 2008: 6)

ICO believes that awareness of information rights among individuals and organisations is the highest ever; however confidence in these rights is volatile, and low for data protection, with rising concern that people have lost control over their personal information (Ibid:8).

> "The high profile of recent data losses has drawn attention to the importance of safeguarding people's personal information, but it has also damaged public confidence that personal information is well protected." (Ibid:19)

A report for the EU Commission examined the methods used by national data protection supervisory authorities across Europe (including ICO), to promote

personal data protection (European Commission 2007). Promotion is important, as for the Commission the role of DPSAs goes beyond the law and into the creation of a 'privacy culture' to balance the negative aspects of the information society (Ibid:2). The report's authors found that promotion activities take place against a background of lack of awareness, poor knowledge of both individual's rights, and of the existence of the DPSAs (Ibid:3). Compared to best practice (Sweden), the report found ICO lacking in interactive web content, case studies and civic cooperation and exchange, although these methods were not particularly common across Europe. Websites and publications were by far the most commonly used engagement method. The report also found that awareness of ICO was higher among data controllers than among the general population (Ibid:29).

HM government co-founded the online safety campaign, Get Safe Online (www.getsafeonline.org), with HSBC Bank, Microsoft, and the Serious Organised Crime Agency (SOCA). Involved bodies within government include the Cabinet Office, Department for Business, Enterprise and Regulatory Reform, Home Office and the Centre for Protection of National Infrastructure. The Home Office, joined by eighteen partners (with some overlap), sponsors www.identitytheft.org.uk - part of the 'Identity Theft: Don't become a victim' campaign, which includes leaflets and posters.

National Identity Fraud Prevention Week is a 'nationwide effort to help in the battle against identity fraud' (www.stop-idfaud.co.uk). The week, associated website and guides are supported by a range of partners. These include Fellowes (an office equipment retailer), The Metropolitan Police, The Federation of Small Businesses, National Fraud Authority, Equifax, CIFAS, Callcredit, Experian, Association of Chief Police Officers, the Identity and Passport Service, The British Chambers of Commerce, British Retail Consortium, and Royal Mail.

The Get Safe Online message has a highly similar structure to that of ICO, focusing upon providing educational material and guidance. However, in contrast to ICO and the two other campaigns, GSO is more focused upon online behaviour and internet safety, providing more detailed guidance in this space. As with the other campaigns, this guidance often takes the form of lists of advised behaviour. For example:

> "You also need to be careful about the information you give away about yourself online. For example, be careful about giving away too much information on blogs and social networking sites like MySpace, FaceBook or Bebo. Identity thieves can piece together your identity from public information piece by piece like putting together a jigsaw." (http://www.getsafeonline.org/nqcontent.cfm?a_id=1491)

The website, www.identitytheft.org.uk, states:

> "This website can help you protect yourself, advises what to do if it happens to you and suggests where to get further help. It has been produced in collaboration between the public and private sectors to combat the threat of identity theft." (http://www.identitytheft.org.uk/what-is-identity-theft.asp)

The National Identity Card and register brought into legislation by the Identity cards act 2006 was a key pillar of the previous UK government's strategy on identity

management. The card was promoted as helping to prevent identity theft, an element of government language that had grown from a marginal element in early planning documents (Cabinet Office 2002), to one of the core themes of the government's ID discourse (Wills 2008:175). The UK Identity card and register are contrasted with a 'laisser-faire' response or 'mish-mash of unregulated, potential unsafe systems' for identity management (Byrne 2007). The coalition government formed after the May 2010 elections has rejected this infrastructure and an Identity Documents Bill, intend to repeal the enabling legislation of the identity card is proceeding through Parliament at the time of writing. The new government's language in this area still constructs a threat to 'identity' and it has not removed the element of personal responsibility for identity management. The debates around the identity documents bill have largely focused upon recouping costs of those who had already signed up for a card, with the new government largely unsympathetic to these claims (House of Commons 2010).

Both Get Safe Online and National Identity Fraud prevention week demonstrate the plurality of actors suggested by governmentality models. A regime of practice can be identified where there is a relatively stable field of visibilities, mentalities, technologies and agencies. In this case, the strongly similar sets of advice, 'best practice' and guidance provided by this range of actors in multiple coalitions (with overlapping membership) across the public and private sectors demonstrates this substantial stability. Table 1 maps the occurrence of similar recommended identity management activities across the campaigns and shows the substantial consistency of message that places these campaigns within the same regime of practice.

It is possible to determine the likely impact of these engagement campaigns from existing research. This highlights confusion around conceptual issues, poor reception, a lack of clarity and a general lack of both impact and two way communication.

The ICO communication research found the majority of the public lack confidence in the way that their personal information is protected and handled. Security and passing information on to other organisations were high concerns (ICO 2009:18). Table 2 demonstrates some of the figures from this report.[2] The ICO research is capable of capturing some basic proportions, but is poorly equipped to understand how people make sense of their identity management 'responsibilities'. It highlights an increasing awareness of identity fraud and the malicious exploitation of personal information, and likewise identifies that respondents do not feel in control of their personal information. However, it does not provide any way of moving beyond this, of understanding what such a control would resemble, what individuals want to do with their personal information, or what processes and practices of identity management they would feel capable of, or even of ways in which such

[2] Survey methodology in this field is problematic. Questions based around identity management behaviour are likely to fall prey to social desirability bias. Particular conduct is privileged and approved, and therefore performing this activity is socially desirable and therefore over-reported. This is highly likely to apply to measures of 'concern' where expressing concern about an issue when asked is low cost, and shows an educated, aware and responsible posture. Similarly, issues such as identity management and privacy more broadly can be 'activated' concerns, in that they become a concern when the individual is asked about them, but are not a deeply held concern.

information could be better communicated. The failure to understand the individual within society also needs to be addressed. When individuals described their specific experiences in preliminary focus groups or in related areas, the differences in understanding become starkly apparent and it becomes obvious that individuals have made sense of identity management in ways that were not anticipated by institutions.

Similar differences in understanding and sense making can also be seen in the reaction to the NDNA database. The governance processes surrounding the operation of the NDNA database have taken the issue of visibility of ethical behaviour seriously and have taken steps to ensure that subject matter experts are included in the governance structure. An annual report is also published that outlines processes and makes it clear where errors in processes have been discovered and what is being done to rectify such errors. Finally a relationship is being forged with COREC (Central Office for Research Ethics Committees) so that processes that involve the use of the database, or the records it holds, in new ways are reviewed before they are implemented. In the future there is an intention to develop a web site that is separate from that of the Forensic Science Service so that the general public can post questions about the NDNA database. Despite these steps however, it still seems that there has been a failure to engage and to understand how the public makes sense of the operation of the NDNA database

Furthermore proposals from the NHS for a Care Record Service attracted media interest. These proposals involve moving patients' medical information on to a centralised database system that can be accessed by healthcare professionals in any part of the country. The information will consist of a 'summary care record' giving basic medical information about an individual, allergies and drug reactions. Following a campaign by the Guardian newspaper and an article highlighting the security risks to personal health information that such a database could pose readers were encouraged to write to the Dept of Health and request that their information was excluded from such a centralised database. When reviewing the media and government responses to this issue it seems that a range of inaccurate information has been given. It is not suggested that this has been a deliberate attempt to mislead but that neither side has listened to the other and, in the case of the Dept for Health, information has not been provided in a way that reassures the general public The implication is that the Dept of Health knows what is best for the general public rather than taking the time to listen and engage. Information outlining how personal medical information will be protected under the new proposals is available on the NHS web site but the Dept of Health has to take some responsibility for understanding why their message has not been received by the general public to the extent that a report in the Guardian can start such a significant backlash against the proposals.

The European Commission report recommends that data protection authorities develop a more practical and pragmatic approach to engagement. This includes avoiding paternalistic language and promoting citizen inquiry, alongside making best use of the mass media and targeting the education sector (European Commission 2007:49–51). This may however ignore fundamental problems with the message that is being communicated. From an examination of

the language used to outline online identity management it is perhaps possible to understand why this failure to engage occurs. The fact that the language of identity management does not engage was noted by the Information Commissioner; Richard Thomas stated that the language surrounding the protection of 'personal information .... is not particularly attractive'. He notes that from research carried out by his office that 'Only 10% of the population in this country understand what a data subject is. Most people think it's a subject you study at school'(Thomas 2005).

'Identity theft', which drives much of the discourse in this area, is also a heavily contested term. It is problematic in that references to identity theft may intimidate and confuse the search for potential political or infrastructural solutions (Barnard-Wills 2009:355). The articulation of identity as something that can be stolen misrepresents financial crime, as identity theft is most frequently credit fraud (The Identity Project 2005). Government statements that identity theft costs the UK £1.7 billion per annum conflate a number of different types of crime, the majority of which should not be considered identity fraud (Bryne 2007). These practices are the circumvention of security practices – therefore 'online identity management' is instead individualised interaction and negotiation with security processes put in place by others, with complications arising from technological legacies, an increasing number of users, and resource allocation decisions. These are the complex interactions described by Dewey as arising from the 'machine age' in politics, increasing indirect consequences of actions (Dewey 1999).

The CST highlight the concept of, 'citizens *owning* their own data' (Council for Science and Technology, November 2005b) and argues that for most individuals this is an idea that is 'too remote from people's own experiences for them to engage with it'. It could be suggested that it has not been made sufficiently clear to them at an individual level what this means. When questioned, individuals found it 'difficult to formulate definitive views on the more specific issues' surrounding the sharing of personal data. As a result of this there is a lack of understanding about how the public make sense of what they are told about identity management which is likely to complicate matters. Another outcome of not understanding background expectancies is described in the CST paper when participants in focus groups felt, 'powerlessness that greater sharing of personal data by government would happen anyway' (Ibid:29)

Research into government initiatives where public consultation has been undertaken suggests a failure to learn from past lessons. In the case of Radioactive Waste Management it was observed that a valuable lesson had been learned and that, 'Since 1997 there has been a change in approach and the issue has been redefined: from a technical challenge to be solved by engineers, to a social challenge that science and technology can help to solve'(CST March 2005a:3).

This was reiterated in the 'Report on the Surveillance Society' which states that 'returning to the social science is helpful' in understanding the impact on society but the report also acknowledges that this is not an easily accepted argument and that 'it has proved difficult to persuade policy-makers of the salience of the *social*

dimensions' of issues such as privacy (Surveillance Studies Network 2006:38). In spite of the CST's recommendation that, 'If government is to develop the capacity to use dialogue effectively it needs to develop a corporate memory of past experience that will enable collective learning' (CST March 2005a:14), it seems that information sharing programmes have yet to build on this and continue to place the technical challenge at the forefront of consideration.

Failing to engage the public risks distancing the public from government action; decreasing trust in public sector activity; and increasing opposition to activity in this field. On a social level, a failure of public sector engagement could leave individuals exposed to harm arising from the widespread sharing of personal information, or unable to make informed choices. The CST paper discusses the, 'decline in confidence, which may be part of a wider trend of disengagement from government' (CST March 2005a:3). The paper outlines an explicit framework for encouraging public dialogue and argues that this should be done, 'earlier and more deeply' than in the past. While government may argue that it has attempted to engage in public dialogue there are many indications that these attempts have failed. The 'Report on the Surveillance Society' provides the example that 'in the UK the clarity about the primary purpose of the proposed national ID system is a key issue'(Surveillance Studies Network 2006:16). In spite of this, anecdotal evidence from senior practitioners in the security arena and from project teams involved in the Government ID card programme has demonstrated a failure in attempts to persuade the public to engage in such discussions.

Problems of engagement

We move now from a practical critique of existing engagement efforts to a more substantive political critique of the model of engagement, supported by returning to governmentality and communication theory.

In Mikhail Bakhtin's concept of centripetal and centrifugal forces, language pushes back on the social world, describing the relationship between the social world and language as a two-way struggle (Maybin 2001:65). The centripetal force is the discourse of authority which stems from social institutions and this is in constant conflict with the centrifugal force of individual discourse which is determined by the individual's experience of their place in the social world.

The centripetal discourse of authority can fail to engage with the centrifugal discourse of the individual. The Council for Science and Technology's case study of GM Food, highlighted the importance of public debate - providing the government allows the outcomes to influence its actions (CST March 2005). Undoubtedly dialogue between government and the public is vital but the implication here is that engagement must be a dialogic process. The centripetal and centrifugal forces of language feed off each other carrying them both forward but this will not happen if there is no engagement between them.

The sociologist Howard Garfinkel spent time researching the methods individuals use to make sense of what others say and do. 'Any conception of social action is incomplete without an analysis of how social actors use shared common-sense

knowledge and shared methods of reasoning in the conduct of their joint affairs' (Wetherell et al. 2001:50). We all think we are talking about the same thing until it is too late. The transmission model of communication fails precisely because the lack of a feedback from receiver to sender means it is difficult to understand how the individual makes sense of what is heard about information sharing. Garfinkel's experiments demonstrate the importance of understanding how social context sets up expectancies about what is said and why and what is meant. As the 'Report on the Surveillance Society' points out 'what spells 'efficiency' for one person spells 'social control' for another and 'this is particular true for strongly personalised systems like ID records retrieval' (Surveillance Studies Network 2006:33). We can see from this example how important it is that we understand how individuals make sense of what they are being told about identity management.

There is a tension in these campaigns, excepting the Information Commissioner. They present the individual as responsible in a way which occludes the architectural choices behind an environment of substantial gathering, sharing and processing of personal information. In many ways this economy of personal information (Lace 2006) is what makes the 'identity' of the individual valuable and thus require efforts to secure it. Get Safe Online sums up this responsibility in the following way. The focus is primarily upon the individual protecting themselves.

> "Online safety is as much about behaviour as it is about technology. Fundamentally, it is about assessing risk and deciding what to do about it. You are the only person who can guarantee your own safety online." (http://www.getsafeonline.org/nqcontent.cfm?a_id=1143)

ICO discourse does not construct a vision of the world in which it is possible to do away with or prevent privacy invading practice. Rather ICO seeks to

> "mitigate the negative effects of surveillance by promoting privacy friendly approaches, influencing stakeholders, developing relevant tools and increasing the confidence of individuals in exercising their data protection rights" (Information Commissioner's Office 2008:20)

Dean draws a distinction in this thinking between active citizens, capable of managing their own risk, and targeted populations (disadvantaged groups, the 'at risk') who require government intervention in the management of risks (Dean 2010:194). Applying this to online identity management, we can see a drive to present active citizens with a range of strategies and techniques to manage their 'identity risk' as part of their daily conduct, whilst the national identity card has been discussed in terms that suggest that it plays an interventionist role in identity management – protecting those parts of the population that are unable to protect themselves, for lack of resources or technological skills (Byrne 2007). Torin Monahan has referred to this responsibility for security in terms of the 'Insecurity Subject' produced by the intersection of security cultures and surveillance infrastructures, and carrying a responsibility to be both reflexive and self-surveilling (Monahan 2010).

OECD regards citizen engagement as involving citizens in decision making (OECD 2009). This does not appear to be the case in online identity management in any real sense of deciding the identity management 'architecture'. Individuals are

presented with a situation and then presented with a range of strategies to protect themselves from risk in that situation. There are public panels and expert panels associated with the identity card system, but the link to direct online identity management is limited. It cannot be considered engagement if it is not two-way, and certain decisions are presented as fait d'accompli – especially those decisions that are depoliticised through being embedded in technological architectures. Wynne's examination of the interactions between expert and lay knowledge suggests that when 'expert' institutions impose prescriptive models upon groups, these are often found wanting. This leads to alternative risk assessments using different frameworks and alternative sources of evidence. This alternate framework also often includes critiques of the methods and motives of the expert institution (Wynne 1996). The governmentality perspective, especially that of Miller and Rose, suggests attention towards the centres of authority in governance – the voices that carry authority within a particular discourse (Miller and Rose 2008:20). Currently with identity management these centres of authority are the broad assemblages of government, and the architecture of online identity management is predominantly presented as a technological fait accomplis and engagement with these models is only legitimation after the fact.

Moving forward with engagement

To summarise the previous, engagement fails when it assumes a transmission model of communication, ignores lay or public perceptions, and when it presents technological fait d'accompli. Presenting mitigation strategies for appropriate conduct within an environment cannot be considered engagement. Adopting appropriate responses to these problems is primarily a political act. However what can assist with a more active engagement is a better understanding of existing models of online identity management. Our approach towards engagement uses a theoretical framework derived from the discourse theory work of Glynos and Howarth, which emphases the importance of starting with contextualised self-interpretations of subjects involved in a discursive space (Glynos and Howarth 2007).

Glynos and Howarth set out a discursive research strategy and theoretical approach based upon post-structural presuppositions and ontological framework, a development of Laclau and Mouffe's work in political discourse analysis (Laclau and Mouffe 1995). They attempt to negotiate the distinction between positivism and non-generalisable hermeneutic approaches. Their goal is to allow research in the social sciences that is explanatory, critical, and incorporates an appropriately political dimension. They offer an account of politics highly linked to contingency. Politics includes, but is not limited to the public contestation of practices and norms. Taking inspiration from hermeneutic approaches, all meaningful social science explanations must pass through the contextualised self-interpretations of subjects. However, this is not in itself sufficient as subjects are not fully aware of world. Explanations need to show how self-interpretations are contingent, and how they are sedimented, focusing attention on the 'ignoble origin' forgotten as self-understanding is lived out. In this sense, to understand how elements of public

engagement efforts become sedimented in everyday discourse. All practices and regimes are discursive entities. This makes understanding meaning central. All objects (including people) have their identity conferred upon them by particular systems of meaning (or discourses). Regimes are constellations of practices, pulled together by a discourse. Any field of discursive social relations is marked by radical contingency, that is to say that identities are inherently unstable and achieving a full, stable, identity is impossible. There is always an outside that cannot be re-absorbed by an identity. The regime of practices in this case becomes the practices of identity management that are encouraged by the public sector as well as the communication practices of the public sector itself.

This contingency is highlighted by any moment where a subject's mode of being (which is generally habitual, and non-reflexive) is disrupted; when identities and existing discourses fail to make sense of the social space. The contingency of the social is revealed to the subject, who must then deal with this somehow. The subject can either acknowledge and act upon contingency or deny and conceal it. This can be done politically, or socially. In this case, contingency occurs when identity practices and their supporting discourses fail to work, or to make sense of the world.

Glynos and Howarth's approach is amenable to incorporating other theoretical traditions and research perspectives, even those with differing ontological presumptions. Such theories require returning to the original questions and problems addressed in the development of those theories, deconstruction to find the weaknesses, ambiguities and exclusions in the theory, a commensuration process that reworks the theoretical concepts to make them compatible with discursive ontology, and a re-articulation of the theoretical concepts. In this sense it can encompass other socio-psychological theories to account for why particular ways of understanding privacy and identity security may have greater purchase than others.

Conclusions

This paper has examined contemporary UK public sector engagement efforts around the complex socio-technological issue of online identity management. Drawing upon governmentality analytics suggested attention to the plurality of actors with shared regimes of practice and fields of visibility, as well as to the extent to which individual actors are made responsible for their own identity management. Communication theory suggested that this assumption, alongside linguistic distortions created by this way of understanding the problematic of identity management, complicate and fundamentally limit engagement activity. Whist much of this is a practical issue, we have set out the first principles of an appropriate engagement strategy for online identity management; understanding (so as to respond better to and incorporate) existing public understandings of the space through a inductive qualitative research strategy.

Appendix

Table 1 Table of advice from identity management campaigns

Advised activity	ICO	Stop-idfraud.co.uk	Get safe online	Identitytheft.org.uk
Beware of unexpected requests for personal information, ask for phone number and call back	x	x	x	x
Keep cards safe		x		x
Keep note of emergency numbers				x
When giving personal information, make sure cannot be overheard				x
Watch cashiers when purchasing		x		
Pay attention to billing cycles		x		
Check statements when arrive for unfamiliar transactions	x			x
Contact creditors if bills arrive late				
Don't throw away bills, receipts, bank statements, unwanted post				x
Shred all documents	x	x		x
Invest in a powerful cross-cut shredder		x		
If passport or driving license lost contact issuer immediately				x
Report all stolen documents to issuer	x			
Get credit report	x	x		x
Monitor credit report regularly	x	x		
Get credit report 2–3 months after moving house				x
Keep your documents in a safe place	x	x		x
Consider storing valuable financial documents with your bank				x
Limit number of personal documents you carry	x	x		x
Protect/monitor post		x		
Secure postbox	x	x		
Be extra careful in multiple occupancy dwellings		x		x
Inform all relevant organisations when moving house	x	x		x
Security patches and up-to-date anti-virus		x		
Firewall and anti spam software	x			
Visit get safe online		x		x
Don't use same password/PIN for several accounts	x			x
Keep passwords safe				x
Choose strong passwords			x	
Be careful using public computers	x			
Do not click on web links unless confident genuine				
Block unwanted spam			x	
Use a modern web browser			x	

Table 1 (continued)

Advised activity	ICO	Stop-idfraud.co.uk	Get safe online	Identitytheft.org.uk
Be careful about information posted on social networks			x	x
Use a mail forwarding service after moving house		x		
Use royal mail 'keepsafe' service if going away		x		
Consider using mailing preference service to limit junk mail				x
Ask post office for advice on secure postage of personal documents	x			
Protect the identity of the recently deceased				x
Contact CIFAS	x			

Table 2 Proportion of UK public

Showing concern about issue of protecting people's personal information	94%
'Very concerned' about issue of protecting people's personal information	71%
Believe they have lost control over the way their personal details are collected and processed	68%
Believe organisations handle details they collect you in a fair and proper way	47%
Aware of ICO	23%

References

Barnard-Wills D. The articulation of identity in discourses of surveillance in the United Kingdom. PhD Thesis, University of Nottingham. http://etheses.nottingham.ac.uk/850/; 2009.

Byrne L. Securing our identity: a 21st century public good: speech by Liam Byrne MP, the Minister of State for Immigration, Citizenship & Nationality, to Chatham House. http://press.homeoffice.gov.uk/Speeches/sc-identity-21st-century, 19th June 2007.

Cabinet Office. Identity fraud: a study. London. Available online: http://www.statewatch.org/news/2004/may/id-fraud-report.pdf, 2002.

Cabinet Office. Transformational government: enabled by technology. Available online: http://www.cabinetoffice.gov.uk/media/141725/strategy-workfile.pdf, 2005.

Council for Science and Technology. Policy through dialogue: informing policies based on science and technology. Available Online: http://www.bis.gov.uk/assets/bispartners/cst/docs/files/whats-new/05-2180-policy-through-dialogue-report.pdf; 2005a, March.

Council for Science and Technology. Better use of personal information: opportunities and risks. Available online: http://www.bis.gov.uk/assets/bispartners/cst/docs/files/cst-reports/05-2177-better-use-personal-information.pdf; 2005b, November.

Dean M. Governmentality: power and rule in modern society. 2nd ed. London, Thousand Oaks, Delhi: Sage; 2010.

Dewey J. The public and its problems. Athens: Swallow Press & Ohio University Press; 1999.

Ellison N, Heino R, Gibbs J. Managing impression online: self presentation processes in online dating environments. J Comput-Mediat Commun. Available online: http://jcmc.indiana.edu/vol11/issue2/ellison.html (accessed 25/07/10); 2006; 11:2. Article 2.

European Commission. Final report: evaluation of the means used by national data protection supervisory authorities in the promotion of personal data protection. Directorate General Justice, Freedom & Security. Available online: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_kantor_management_consultants.pdf. Accessed 19/07/1010; 2007.

Evans-Pughe C. Engineering digital identity. Eng Technol. 2008;3(10):16–18. 7-20th June.

Glynos J, Howarth D. Logics of critical explanation in social and political theory. London: Taylor & Francis; 2007.

Home Office. Identity Cards Act Secondary Legislation: a consultation. London: The Stationary Office. Available online: http://www.ips.gov.uk/cps/files/ips/live/assets/documents/NIS_Legislation.pdf; 2008.

Home Office. Identity Cards Act Secondary Legislation: a response to the consultation. London: The Stationary Office. Available online: http://www.ips.gov.uk/cps/files/ips/live/assets/documents/09-05-06_Identity_Cards_Act_Secondary_Legislation_a_Response_to_the_Consultation.pdf; 2009.

House of Commons. House of Commons Public bill Committee on the Identity Documents Bill 2010-11 Available online: http://services.parliament.uk/bills/2010-11/identitydocuments/committees/houseofcommonspublicbillcommitteeontheidentitydocumentsbill201011.html; 2010.

Information Assurance Advisory Council. IAAC Position Paper on Identity Assurance (IdA): towards a policy framework for electronic identity. Available online: http://www.iaac.org.uk/Portals/0/identity_management_paper_v1-7.pdf; 18th October 2005.

Information Commissioner's Office. Personal information toolkit. Available online: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/toolkit.pdf (accessed 25/07/10); 2007.

Information Commissioner's Office. Data protection – protecting people: a data protection strategy for the Information Commissioner's Office. Wilmslow: ICO; 2008.

.Information Commissioner's Office. Strengthening our position: ICO communications and external relations strategy – three year plan 2009–12. v2.2. http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/cer_strategy_2009_2012_v2.2_final.pdf (accessed 19/01/10); 2009.

Lace S. Glass consumer: life in a surveillance society. Bristol: Policy Press; 2006.

Laclau E, Mouffe C. Hegemony and socialist strategy. London & New York: Verso; 1995.

Maybin J. Language, struggle and voice: the Bakhtin/Volosinov writings. In: Wetherell, M., Taylor, S. & Yates, S. (eds). Discourse Theory and Practice: a reader. London: sage; 2001.

Miller P, Rose N. Governing the present: administering economic, social and personal life. Cambridge & Malden: Polity Press; 2008.

Monahan T. Surveillance in the time of insecurity. New Brunswick, New Jersey and London: Rutgers University Press; 2010.

OECD. OECD Studies on public engagement. Focus on citizens: public engagement for better policy and services. OECD Publishing; 2009.

O'Malley P. Risk, power and crime prevention. Econ Soc. 1992;21(2):252–75.

SMSR. Report on the findings of the Information Commissioner's Office Annual Track 2008: individuals. Hull: SMSR. http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_tracking_individuals_final_report2008.pdf, 2008.

Solove DJ. The future of reputation: gossip, rumour and privacy on the internet. New Haven & London: Yale University Press; 2007.

Solove DJ. Understanding privacy. Harvard: Harvard University Press; 2008.

Surveillance Studies Network. A report on the surveillance society. Information Commissioner's Office, 2006.

The Identity Project. The identity project: an assessment of the UK Identity Cards Bill and its implications. Version 1.09. LSE Department of Information Systems; June 2005.

Thomas R. Information sharing: information rights. eGov monior. Online http://www.egovmonitor.com/node/3721, 28th November 2005.

Wetherell, M., Taylor, S. & Yates, S. (Eds.) Discourse Theory and Practice: A Reader. London: Sage. 2001

Wills D. The United Kingdom identity card scheme: shifting motivations, static technologies. In: Bennet C, Lyon D, editors. Playing the identity card: surveillance, security and identification in global perspective. London: Routledge; 2008.

Wynne B. May the sheep safely graze? A reflexive view of the expert-lay knowledge divide. In: Lash S, Szerszynskis B, Wynne B, editors. Risk, environment and modernity: towards a new ecology. London: Sage; 1996.

Websites:

www.cifas.org.uk
www.getsafeonline.org/nqcontent.cfm?a_id=1491
www.identitytheft.org.uk/what-is-identity-theft.asp
www.ico.gov.uk
www.stop-idfraud.co.uk/