IDIS (2008) 1:135–154
DOI 10.1007/s12394-009-0007-5

Identification practices in government: citizen surveillance and the quest for public service improvement

John A. Taylor · Miriam Lips · Joe Organ

Received: 24 March 2008 / Accepted: 7 December 2008 / Published online: 24 February 2009

Abstract This paper is concerned with the ambiguities and confusions that arise when studies of the 'surveillance state' are contrasted with studies of the 'service state'. Surveillance studies take a largely negative view of the information capture and handling of personal data by Government agencies. Studies that examine Government service providing take a largely positive view of such data capture as Government is seen to be attempting to enhance service provision to individual citizens. This paper examines these opposing perspectives through a series of case studies and concludes that a new understanding and methodology should be brought forward so as to create a reconciliation of these two points of departure for research. The call is for an holistic appreciation of data capture activities by Government so that researchers and public policy makers alike can appreciate and reconcile these competing perspectives.

Keywords Public service · Surveillance · Case studies · Contextual integrity · Appreciation

J. Taylor (✉)
Government & Information Management, Caledonian Business School,
Glasgow Caledonian University, Cowcaddens Road, G4 0BA Glasgow, Scotland, UK
e-mail: jta@gcal.ac.uk

J. Taylor · M. Lips · J. Organ
Oxford Internet Institute, University of Oxford, Oxford, UK

M. Lips
e-mail: Miriam.lips@vuw.ac.nz

J. Organ
e-mail: joe.organ@oii.ox.ac.uk

M. Lips
E-Government, Victoria University of Wellington, Wellington, New Zealand

Citizen identification, surveillance and the quest for public service improvement: themes and issues

Ambiguous confusion in the interpretation of information-intensive government

We draw attention in this paper to a particular case of ambiguous confusion (Rhodes 1981) that has led to a lack of conceptual and interpretive clarity in both the study and the practical policy arenas of information-intensive government.

We develop this theme of ambiguous confusion through an examination of our case study research[1] on identification processes, including forms of identity management, in a variety of settings of 'digital government'. By setting out this case study evidence we demonstrate the information-intensity that characterises the relationship between the modern state and its citizens. In turn, we set these case study findings against what we refer to as a 'Service State' perspective, on the one hand, and a 'Surveillance State' perspective (Lyon 1994), on the other. In so-doing, we acknowledge the largely separate development and orientation of two bodies of academic writing that cohere around these two themes, each of which is profoundly concerned with the application into forms of government service delivery of new information and communications technologies [ICT].

The content of the first of these bodies of writing, the 'service state' literature, has many variants, including studies of access to, and uptake of, forms of 'e-service' providing (eg Hagen and Kubicek 2000; Margetts and Yared 2003); studies of public service innovation and modernisation (eg Bekkers 2007); and, most recently, the development of 'citizen-centric' services and the encouragement of forms of data sharing and database management and development that permit informational integration at the point of the individual citizen in order to improve the service experience of the citizen (Lips et al. 2006; Taylor et al. 2006, 2007; Leben et al. 2006). It is an empirically grounded literature basing its analysis and prescriptive reasoning on research evidence. This academic literature has its parallel too in public policy reporting, reporting that is focussed also on wider issues of citizen-centricity such as the availability, access to, and uptake of, on-line government services, whether they be information services or transactional services and on inter-country comparisons (eg Accenture 2005; Varney 2006).

The 'surveillance society' literature is primarily concerned that new technology developments offer governments, and private companies, affordances (Norman 1999) for 'knowing' citizens and customers in new and more intimate ways than hitherto. Its perspective is on the rapid development of the 'surveillance society', fuelled by inherent capabilities of newly available ICTs that include the ubiquity of information gathering on the activities of individuals; the speed of information gathering and processing; and the embeddedness of computer codes, values and decision making assessments leading to 'social sorting' activities of business firms and governments alike (Gandy 2000; Lyon 1994, 2001, 2003; Graham and Wood 2003; Surveillance Studies Network 2006, 2008). Much of this work has a strong normative basis, one that underpins the advocacy and campaigning stance of

[1] ESRC e-Society Project: Personal Identification and Identity Management in New Modes of e-Government Ref: RES-341-25-0028.

collaborations such as the Surveillance Studies Network. This literature also has its parallel in public policy reporting. The recent report from the Chief Surveillance Commissioner for the UK (2008) and the report of the House of Commons Select Committee on Home Affairs (2008) provide examples, as will a forthcoming report from the Constitution Committee of the House of Lords, expected in late 2008.

In this article we translate this surveillance society perspective into a surveillance *state* perspective (Lyon 1994), one that is concerned with how information-intensive governments are using, managing and implementing new modes of surveillance and, with that, the emergence of new forms of relationship with citizens.

A feature common to each of these perspectives is the centrality of citizen identity. From within a service state approach, identification and authentication procedures are viewed as a necessary precursor to high quality service-providing aimed at the individual citizen, both in on-line and off-line service settings, as we show in our case studies below. From the surveillance state perspective, however, this incipient concern to identify the citizen in many different settings is interpreted as marking a sea change in relationships between citizen and state, one that demands constant and critical appraisal (eg Bannister 2005). Thus, the interpretive schemes of these two sets of observers lead them to opposing conclusions from observation of the same phenomena. Whilst students and analysts of the service state are most likely to stress positive consequences for citizens emerging from new identification practices, for students and analysts of the surveillance state the consequences are most likely to be negative.

Whilst for the purposes of elucidation we present these perspectives as distinctive we note too the growing mutual appreciation emerging between them. That is to say that a growing body of work suggests the need both to accept, and regulate for, an holistic awareness of the co-existence of the desire to enhance public services, on the one hand, and the risks attaching to such enhancement in the form of overweaning public scrutiny, on the other. Such awareness seems to mark out the emergence of a new 'appreciative setting' (Vickers 1965) wherein new regulatory mechanisms, such as a Privacy Council (Bannister 2005), privacy audits (Bennett and Raab 2006), 'surveillance impact assessments' (Surveillance Studies Network 2008) would be introduced into emergent public service relationships between the citizen and government so as to realise a new mode of regulatory optimisation (Vickers 1965).

The main aim of this paper is to add further to this emergent mutual appreciation by presenting case study evidence that works with the concept of 'contextual integrity' (Nissenbaum 2004) as a methodological framework for a new form of regulation in the spheres of digital government, identity management and threats to personal privacy. As Brownsword (2008) argues "the regulators of the 21st century will be smarter than their predecessors. …..while traditional command and control interventions might be attractive to politicians, they are not always an effective or efficient form of response". The subtleties of contextual integrity may well provide for more effective and efficient regulation of the service state, one that avoids surveillance excesses feared by the surveillance studies network, for example, whilst allowing for the realisation of enhanced forms of public service provision.

Thus, the first proposition informing this paper is that two highly distinctive 'ways of seeing' the same phenomena co-exist, thereby giving rise to forms of ambiguous confusion for academic commentators and policymakers alike. We advance this proposition and develop our analysis only in respect of those parts of

Government involved in the delivery of forms of personal services to the citizen. In this paper, we argue that these service and surveillance perspectives should be brought together, specifically in respect of the provision of public service to the individual citizen where personal information on the citizen is gathered, managed and exchanged in citizen–government relationships. An holistic approach such as this will acknowledge that well produced government services necessarily involve the collection and use of personal information, as service providing in pursuit of high levels of customer satisfaction necessarily becomes more information-intensive. In taking forward this argument we share Nissenbaum's (2004, p101) view when she says:

> Among many privacy controversies that have stirred public concern, a particular set of cases, to which I have applied the label "public surveillance," remains vexing not only because these cases drive opponents into seemingly irreconcilable stances, but because traditional theoretical insights fail to clarify the sources of their controversial nature.

Our second proposition is that the development of new thinking about contemporary public service delivery is urgent. This paper aims to contribute to this thinking by further stimulating mutual understanding between proponents of these distinctive perspectives, understanding from which new theoretical insights may be developed. In advancing this aim we first draw inspiration from Allison (1971) whose classic study exposed the validity, and thereby the pragmatic significance, of examining public decision making through distinctive perspectives. The heart of Allison's argument was that whilst many analysts presumed that governmental decisions were made on a 'rational actor' basis, research exposed equally plausible alternative explanations for particular outcomes, such as the dominance of particular routines and repertoires found in government bureaucracies or the internal politics of government organisation. Moreover, Allison pointed to the possible negative consequences that can occur as a consequence of the perspective taken. Thus, from a scientific point of view, to take a wholly rational actor perspective, for example, seems to violate the central scientific concern with 'falsification', for it ignores much evidence that points to the validity of other perspectives. More importantly from the point of view of practical outcomes, such a perspective may prove purblind to the likelihood of unintended consequences arising from the decision taken. Only if all available perspectives are given consideration can outcomes be fully assessed and built upon.

Extrapolating this reasoning to the concerns of this paper, we argue that analysts of public services delivery on the one hand and the surveillance state, on the other, must address their respective perspectives if these scientific pitfalls are to be avoided. The normative basis for so much of the surveillance state and society literature appears to the authors here to lead ineluctably to an interpretation of much techno-governmental activity as surveillance and is thereby not amenable to falsification. The gathering of detailed empirical evidence, some of which is presented here, must be allowed to enrich this debate. Rather than being assumed *a priori* as surveillance [in the negative sense of that term], because of the affordances embedded in the technical capabilities of ICT systems, it must be subjected to detailed assessment of both its surveillance and service enhancing content.

Thus we ask:

- How strong is the science base for these distinctive perspectives on contemporary, information-intensive government, including their amenability to refutation?
- Can these perspectives be conjoined in an holistic appreciation and assessment of the dilemmas of information-intensive government?

Case study research

In the research project that has provided the empirical basis for this paper we chose to explore the application and utilisation of a variety of emerging identity management [IDM] systems in different government service domains. An integral element of this focus upon IDM was a detailed exploration of the informational relationships between these service domains and citizens. In that exploration we examined what new information was being captured; the management and flow of information in government service provision to the citizen; and policy and managerial dimensions of the application and use of IDM systems in emerging service relationships. Moreover, as this research project had no direct empirical antecedents, we were particularly interested in enabling deeper, broader and empirically informed understanding of the relationship between IDM systems and the nature of citizenship.

We used case study research methodology to bring a depth of both historical and contemporary understanding to our work aimed at enhancing reliability, enrich our subsequent analysis and theoretical development, and enhance too the generalisability and 'transferability to policy and practice' of the research findings (Walsham 2002; Seale 1999). For each of the case studies, we undertook an academic and policy document literature review as well as c15 semi-structured interviews with key individuals at operational, strategic and policy levels. We gained further insights on the strategic and policy context through semi-structured interviews with experts from the IDM industry and national policy makers in the field of IDM and/or digital Government; two focus group meetings with policy makers and user group representatives respectively; and an international-comparative IDM policy seminar with policy makers and experts from Canada, the US and the UK.

Eight case studies were completed from various parts of UK government, each of them having a different primary "technological access point" for the citizen. In each of them design and implementation choices about identification, authentication and identity management were already made (e.g. Internet Portal, smart card, mobile communications, CCTV). In undertaking these case studies we gained further empirical understanding both of existing information capture, management, flow and assessment within a variety of service relationships, and upon information resources that are being sought as new digital relationships are forged. Other variables designed into the study included different policy and service domains; differentiated institutional settings; and the sensitivity level to be attached to the capture and use of personal information in those different governmental arenas.

In this paper we outline four of the eight case studies of IDM applications in use in emerging transactional public service relationships, that we have conducted.

These studies have been selected because they resonate readily with the questions that are central in this paper. These are studies in:

- Satellite monitoring of offenders on license under the management of the Probation Service and with the support of the Police Service.
- Automatic number plate recognition [ANPR] undertaken by Police Forces.
- On-line application for a provisional driving licence under the management of the Driver and Vehicle Licensing Agency (DVLA)
- E-benefits claims procedures undertaken by the central Department for Work and Pensions [DWP] and local authorities responsible for housing benefit.

Case study 1: satellite monitoring

Offenders are selected for satellite monitoring through a mixture of computerised 'prisoner sorting', with points accumulated for types of offence, levels of apparent risk etc. and probation and police staff discretion. Once selected, a representative of the private company involved in data management and project coordination visits the offender immediately following release from prison. An ankle tag and a tracking device are fitted to the subject. At times when data subjects are away from their dwelling, the tracking device will be detected by up to four satellites, in which case identification is considered '3-dimensional', or by fewer than four satellites in which case the identification is considered '2-dimensional'. At its most precise the location of the subject can be down to 2 m of accuracy.

The tracking device stores this locational information and then transmits it *via* the GSM network to a database managed by the private company, where mapping software plots the movements of the subject. The maps (Fig. 1 below) are periodically despatched at designated intervals to selected probation and police officers *via* secure email. Under initial plans [though this aspect has yet to be implemented] offenders with an 'exclusion zone' built into their license were to be subject to real-time alarms triggered at the control room when satellites detect that the offender had strayed into such a zone Probation officers were to be able to use this information to ensure that offenders are not breaching the condition of their licence, for instance by entering exclusion zones or missing probation appointments.

Moreover, probation officers use mapping information as an evidence base to assess the lifestyle and habits of offenders so as to aid the rehabilitation and resettlement process.

Furthermore, the police have also become interested in this offender location data for crime detection and prevention purposes. Police officers learning of a newly reported crime are now able to check that crime against the *modus operandi* of those subject to satellite monitoring. In these instances, police officers are also able to request retrospective mapping information from the private company. Such maps, as shown at Fig. 1, contain both locational and temporal data. The Police Service use these data to eliminate or associate these tagged data subjects from or to a specific crime. Access to these data by the Police Service is enabled through a clause in the Data Protection Act [29: 3] which permits data sharing deemed necessary to criminal investigation. Such data has already been used to convict at least one offender through a court of law.

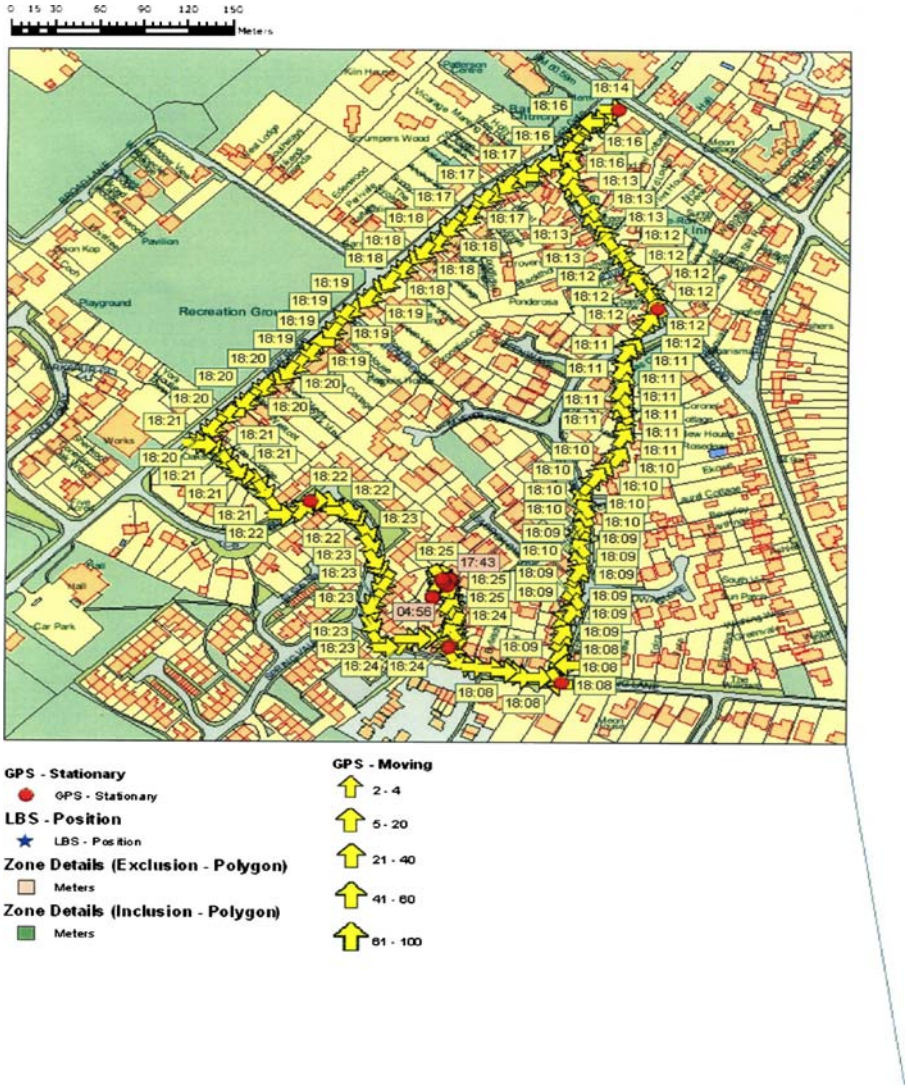


Fig. 1 Satellite monitoring and mapping

Case study 2: automatic number plate recognition

Since 2003 our case study English Police Force has employed Home Office provided Automatic Number Plate Recognition (ANPR) cameras, mounted in police vans and patrol vehicles, to read number plates of passing vehicles. The cameras are mounted at both the front and rear of the vehicle and are able to read up to 3,000 Vehicle Registration Marks (VRMs) an hour for vehicles travelling up to 100 miles per hour. Whilst the front camera has normal colour image capabilities, the rear camera is fitted with infrared; the latter is more effective at reading number plates (e.g. if they are dirty or obscured) whilst the former is required to show the colour of

the car. Number plate information is then matched against a number of datasets in an attempt to detect and reduce crimes and misdemeanours. The case study Force hopes to enlarge the scope of its activities through connection to local authority CCTV systems and other networks, such as that of the Highways Agency. This expansion was not occurring during the period of the research. Moreover, the Association of Chief Police Officers announced plans in 2005 to develop a National Data Centre to house and analyse ANPR information from all police Forces. The National ANPR Data Centre will collect and collate ANPR reads from all Forces, and are likely to keep all reads for at least 2 years. It is likely that retrospective analysis will be developed to generate stronger evidence upon which future police activities can be based. This planned warehousing of national ANPR data is also expected to produce vehicle profiling to aid criminal investigation.

Home Office research has indicated that those who have committed traffic or vehicle-related offences are significantly more likely to have committed mainstream criminal offences than other road users (Rose 2000).

The ANPR system relies on access to a variety of public and private sector databases, such as those held by the DVLA (information on those vehicles that have no road tax, on disqualified drivers etc), the Police National Computer (lost or stolen vehicles), the Motor Insurance Database (uninsured drivers) and local police intelligence (PA Consulting 2004). Patrol vehicles do not have a direct link to the PNC or to the Force's control room. Rather, the on-board ANPR computers have data from these sources periodically loaded onto them.

'Hits' flash onto the screen real-time showing colour coded matches in the various databases used, which connect vehicles on the road with potential crimes and discrepancies. The hit rate is reported as less than 2%, thus most vehicles pass through the camera systems without any action being taken; however the National ANPR Data Centre will collect and store both 'hits' and 'non-hits' from Forces for designated periods of time..

Once a hit occurs, officers in the case study Force make a judgment about whether to pursue the vehicle. This pursuit is most likely to occur where more than one hit had occurred across the multiple databases involved. In addition to this reactive aspect of ANPR the system employed allows for proactive investigation of a vehicle through its VRM. If, during the course of patrols, officers spot what they consider to be a potentially suspect vehicle, they can deliberately position the camera equipment so as to take a reading from that vehicle. The equipment also permits officers to key in the VRM of a car they suspect but are not able to capture through the camera. Furthermore, staff in the Force control room can radio a VRM of particular importance so that officers can monitor the vehicle's passage through the system.

Where there is *prima facie* evidence of an offence, an officer takes one of two courses of action. Officers may take the suspect to the local police station for formal identification and further questioning or charging. Alternatively, police officers may award a Fixed Penalty Notice for offences deemed minor.

Case study 3: on-line driving licence application

An applicant for a licence enters the 'Government Gateway', the managed environment for Government on-line transactional services in the UK, almost

certainly through first of all accessing the citizen-facing web-site Directgov (direct.gov.uk). The applicant inputs standard identity data—surname, initials, date of birth and 3 year address history. These details are then electronically matched against existing driver databases. If no match is produced (very likely in the case of an applicant for a provisional licence), the applicant continues the transaction and a new record is created. Equally, the applicant can proceed if a match is found (i.e. the applicant has been positively identified in the DVLA database) so long as these records do not preclude progression (e.g. he/she is not a disqualified driver). Having gone through this in-house matching system the applicant's details are automatically and in real time transferred to the data management company Experian. Using name and address history in particular, Experian seeks to match the applicant's details against a host of public and private sector databases.

The purpose of this 'third party' involvement of Experian is to validate, verify and authenticate the identity of the citizen making a licence application. Experian systems run personal information from the applicant against the Credit Application Previous Searches (154 million records) and Address Links (252 million records) databases, for example, seeking as they do so the agreed level of validation for the particular service that is being provided. In the case of an application for a provisional driving licence three or more corroborations are needed for name and address and two or more corroborations on the date of birth or an equivalent combination of these factors. This is the ***validation*** aspect of the check.

In addition a ***verification score*** is assigned to an applicant, which is an outcome of a further data matching exercise that seeks to corroborate biographical details that only the applicant is likely to know and which again are to be found in other databases, such as Mother's maiden name or some other 'secret'.

Finally, all of these data are distilled into an ***authentication index*** with each applicant receiving a specific 'trust score'. This final score, indicating the strength of the applicant's 'digital footprint', is heavily influenced by the perceived quality of the databases within which the matching process occurs. Customer databases such as those of the main clearing banks are given higher salience in the authentication process than those of mail order companies, for example. Only when the trust score reaches the pre-ordained level can the applicant proceed to a successful conclusion of their on-line application. The trust score arrived at is not therefore a judgment of creditworthiness but a risk assessment attaching to the degree of certainty that the identity of the applicant is an accurate one. In the Experian methodology the highest possible trust score is 99. A citizen coming on-line to transact with Government may appear in any of the deciles that this scale allows, therefore, and will only succeed in any particular transaction if the trust score is at or above the level set for that transaction.

Case study 4: e-benefits

Since 2004 a unitary local government in England has been using an 'e-benefits system' in respect of claims for housing and council tax benefits. Here, claimants are visited by an official who conducts a face to face interview, usually in the claimants' home, to determine the precise level of allowable benefit. The official uses a tablet

PC loaded with specific e-benefits software; personal details are loaded onto the PC as well as information about claimants' living arrangements, income, bank account details, savings, assets and other benefits being claimed. Once this data has been inputted the software calculates the benefits that can be claimed. The claimant must at the same time produce specified paper documents such as passport, driving licence and pay-slips as proof of identity. Both the claimant and the official sign off the claim using an electronic pen and the document is then sent on as an email attachment to the Government office, *via* a wireless network. This process offers advantages to both claimant and Government, through reducing time and work effort involved in claim processes.

Following this initial registration and successful acceptance of the benefits claim, the claimant is then assigned into a particular 'social' category by the DWP at national Government level, a categorisation that determines the frequency and intensity with which the claim will be reviewed. These categories are derived from matching between a database containing details of detected overpayments of £5 or more 'due to claimant error or fraud' and housing benefits data from the particular local government. In building up the model for categorisation, the characteristics of the claimants who had overpayments were then compared to the characteristics of claimants without overpayments. From that data matching process, an approach that the DWP refers to as 'logistic regression', a risk score is produced for the claimant that is used as a predictor of the likelihood of error or fraud in the claim. The lowest risk categories are in the pensioner groups and the highest risk categories are in working age claimants, with a specific subset of single parents living in private landlord accommodation being the highest risk of all. These social categorisations are sent to the local government with recommendations attaching for their claim review regime. DWP data suggest that where a claimant is in a risk category of more than 10% chance of error or fraud, the number of positive 'hits' from the review process is 25% compared to those in low risk categories (less than 5% chance of error or fraud) where the positive hit rate is 3%. Thus it is assumed that the local authority will place highest priority within its claim review process to citizens from within the highest risk categories. Indeed, local governments responsible for conducting this process of claim review are subject to a performance management regime that determines the level of central financial support for the administration of the service being provided.

Interpreting the case study data

Our first proposition guiding the direction of this paper, as we stated above, is that two distinctive 'ways of seeing' the same phenomena co-exist: the service state and surveillance state perspectives. Moreover, we argued that the co-existence of these perspectives gives rise to forms of ambiguous confusion between academic research communities, for commentators and for policymakers alike. In this section of the paper we go back to the case study descriptions above through each of these two lenses, explaining, as we do, how, simultaneously, we can interpret the data as the service state in action, on one reading, and as the surveillance state in action, on another.

Empirical evidence of the service state

In addition to conducting case study research for the four studies described in this paper, interviews were undertaken with a range of key individuals involved in policy and strategy on the cross roads of public service provision and the introduction of new IDM systems. We have used the content of this set of interviews to distil the 'Whitehall perspective' on the public service agenda being pursued. Underlying each of these themes, and giving force to them, is the relative failure of e-government in the UK as measured against key indicators developed for international comparison (Accenture 2005; Cabinet Office 2005, 2006) and as 'measured' too, anecdotally, by Ministers asking, for example, why the Financial Services sector and other commercial enterprises appear to have been so comparatively successful in transforming their service delivery channels, bringing their customers into new cost effective electronic digital relationships. It is clear from our work that senior government officials are under pressure to perform more effectively than hitherto in the delivery of new forms of public services, in particular within the overarching theme of 'citizen-centric government'. This theme of citizen-centric government informs the Service State perspective and will be discussed further below.

Derived from extensive research interviewing we identify five elements within citizen centric government, each of which can be identified as a goal within some or all of our case study examples. The first of these elements is ***joined up government [JUG]***, a hardy perennial in the discourse of British Public Administration (Bogdanor 2005; Hood 2005). Internal reports made available to us in the conduct of our research reveal how remote the realisation of JUG remains in British central Government, as officials at the centre of the e-government effort lament their inability to persuade Government departments to engage with the necessary information sharing that can join services at the point of service delivery and consumption (Office of the e-Envoy 2004). It is clear too that the centre of the Whitehall e-government effort has had insufficient authority to counter this centrifugalism of the wider Whitehall system. As one insider advised:

> The levers that need to be pulled to achieve the objectives of transformational Government are not yet available. There are so many Departmental reviews, performance indicators, separate budgets etc that are being managed by separate parts of Government that fragmentation seems inevitable.

An illustration of the case for alignment, much cited by central officials and to be found in some detail in the recent Varney Report (2006), is that of the 'Dealing with Bereavement' work currently being led by the Pensions Service, operating under the purview of the DWP. Government research suggests that there are up to 44 interactions that a bereaved citizen might need to conduct with Government (Regulatory Impact Unit 2005). Thus, although increasing evidence suggests that inter-agency data sharing is becoming more accepted, particularly at local, multi-agency, operational levels of administration (6 et al. 2005a, b; Bellamy et al. 2005), at the highest levels in Whitehall there remains uncertainty and reluctance about so-doing.

From our cases we see a number of examples of joining up government that lead to enhanced service providing. The first of these is from the satellite monitoring

study where the Police Service access to Probation Service data leads to new capabilities in criminal detection. A second example is the joining up of the DWP and local authorities through the development of a new evidence base for benefits claims leading to reductions in error and fraud.

The second and third elements within the theme of citizen-centric government are '***ease of contact***' and the provision of '***personalised service***' for the citizen. From our cases we identify the procedure for on-line application for a driving licence, set out above, as an example of ease of contact. Here we have one of few examples in UK government of a fully transactional service being available on-line, '24x7'.

The best example of a service being provided that affords both ease of contact and personalisation from the four cases outlined here is in e-Benefits. This service is brought to the home of the claimant, time consuming copying and posting of identification documents is averted and the individual's personal entitlement to benefit assessed on the spot.

Our fourth element under this theme of citizen-centricity is '***equitable enforcement***' of public service, including the enforcement of citizen entitlement. The cases of ANPR and e-Benefits provide strong examples of the search for greater equity in these service arenas.

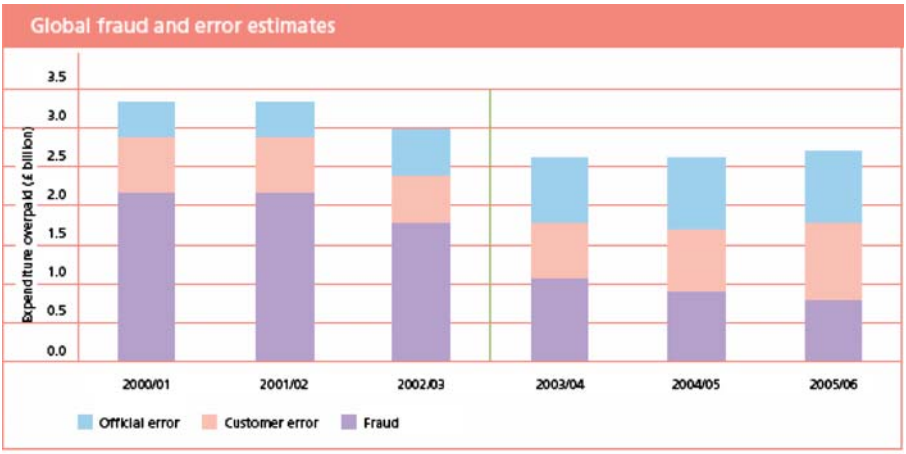
It was estimated in 2004 that one in 20 motorists does not pay insurance, thereby adding an estimated £30 to the average bill of compliant motorists, and that 1.75 million vehicles (5.6% of all those registered) do not have valid road tax (Greenway 2004, pp 7 & 10), adding to the tax burden of those who pay. Since then DVLA has announced that road tax evasion was estimated to have reduced to 3.6% short of the maximum possible income, close to its target of 3.4%. This reduced figure of 3.6% equates to £147 million in lost revenue (DVLA 2006, p95). ANPR was cited as a major contributing factor in this decreased evasion (DVLA 2006, p12).

A further illustration of a new equity of service provision emerging around the use of ANPR comes directly from our work. A number of our interviewees emphasised that the ANPR methodology is pushing the inaccuracies and prejudice based 'suss' interventions of the Police Service away and replacing them with firm, evidence-based reasons for stopping the motorist.

In the case of e-Benefits, we see in Fig. 2 below the cost to government of overpayments, whether by error or fraud.

The total annual loss to government due to benefits error or fraud is estimated at £2.5 billion. In 2005 the Housing Benefit overpayment was estimated to be £580 million (DWP 2006, p2). We can see in Fig. 2 that levels of fraud have been reducing in the period covered. DWP states that its data matching and risk profiling processes form a major part of the DWP's policies to reduce the levels of fraud and error as well as their success in doing so (DWP 2007, p18–19). In 2004/05 data matching processes run by the DWP led to 65,353 incorrect housing benefit claims being identified (DWP 2005, p11).

Finally, we use the satellite monitoring study to illustrate the fifth element within the theme of citizen-centric government; that of ***affording enhanced public and personal protection***. From this case we can observe three aspects of this protection. First, the prisoners under licence being monitored are both frequent and persistent offenders, and some are considered dangerous; it is estimated that persistent criminals, who make up 10% of all offenders, are responsible for 50% of



Source: DWP,2007,p8

Fig. 2 Total overpaid benefit expenditure from 2000/01 to 2005/06. Source: DWP 2007, p8

all crime (Home Office 2001). Evidence gathered during the pilot study shows those prisoners being monitored in this way are re-offending much less than would be the case were they fully released into the community. Secondly, as we describe above, satellite monitoring may be used to enforce exclusion zones for particular prisoners. Thus, previous victims of violent or other crime by these criminals can be better protected from them by the introduction of an 'electronic cordon'. Thirdly, satellite monitoring contributes to processes of offender rehabilitation and can be seen, as a consequence, as an effective protective device for the monitored criminal too.

Empirical evidence of the surveillance state

In their recent report to the Information Commissioner for England, the Surveillance Studies Network (2006, p4), define surveillance as "purposeful, routine, systematic and focused attention paid to personal details". In the case study descriptions set out above in this paper we see each of these adjectives in play in respect of the focus on personal data by State agencies. Each of them provides examples of where the collection and use of personal data is indeed goal-centred, routinised and systematic. Formal goals include those through which we have analysed the services being provided above. Data collection, as with all administrative activity both past and present, has become a matter of routine in the organisations concerned and these data are collected systematically through procedures laid down. Such is the generality of this definition of surveillance that already our cases 'demonstrate' the existence of the surveillance state, it would seem. However, further in their report the Surveillance Studies Network offers up numerous other perspectives on the Surveillance Society that provide the prospect of greater specificity in understanding what is meant by 'surveillance' as well as the possibility of empirical testing. It is to some of these perspectives that we now turn so as to analyse our case study data

from this surveillance perspective. The perspectives we address here are '***social sorting***'; '***function creep***'***and*** '***data sharing***' [which we bring together]; and the '***blurring of public private boundaries***'.

Evidence of ***Social Sorting*** activities by Government agencies is especially evident in the case studies on applying for a driving licence and e-benefits claimants. We have written elsewhere about how we interpret these findings as examples of social sorting (Taylor et al. 2007).

The gathering literature on social sorting draws attention to ways in which Government agencies are collecting, managing and applying new information resources so as to categorise or 'sort' citizens into both socio- and geo-demographic categories in a variety of service providing arenas (e.g. Lyon 2003; Graham and Wood 2003; Nettleton et al. 2004; Burrows et al. 2005). The existing though newly developed on-line application for a provisional driving licence, to be generally available later in 2007 as a channel for all driving licence applications, provides a particular variant to the general theme of social sorting. This case illustrates a different approach to sorting based on 'trust profiling' of citizens and giving rise to what we have termed '***layered citizenship***' (Taylor et al. 2006, 2007). As authentication processes such as the one described above in this case become more commonplace so their effect is to locate citizens differentially in their trust score category. The 'top' layer will consist of those with a strong 'digital footprint', or high levels of validation and verification because of the consistency of their identity data in highly trusted data sources. Below that are other citizenship layers where the trust profile assigned to the individual is scaled at the level determined by the authentication process.

Our second example of citizen sorting, that of housing benefits claimants, uses data held within government to assign a benefit claimant to a socio-demographic category that has a pre-assigned, statistically driven, risk score attaching. Thus, the sorting process is not used 'horizontally' to assign a level of certainty to personal identity, as in the first example above, but to identify the level of trust that can be assigned to the claimant in respect of likely error or fraud in the claim being made. In our research we refer to this as 'vertical sorting'. As evidence based risk assessment processes, such as the one described above in this case of e-benefits, become more commonplace so the effect is to locate citizens differentially on the trust that can be assigned to them as claimants.

At Fig. 3 below we illustrate these two sorting activities by placing them on a single matrix. Here the surveillance perspective is at its most potent. The rows of the matrix represent the trust layers to which we refer in the case of on-line application for a driving licence. The columns of the matrix represent the vertical sorts to which we refer in the e-benefits case. Drawn together in a hypothetical scheme as we do in Fig. 3 we can see how citizens can be assigned to cells within the matrix, cells which, if we follow the arguments of the surveillance perspective, may well impact upon the life chances of the individual (Lyon 2003).

Four examples of '***function creep***' ***and*** '***data sharing***' emerge from within our case studies. First, with satellite monitoring, information primarily aimed to aid probation staff with the resettlement and rehabilitation of offenders is being increasingly used by police officers, as we set out above. Here, the purpose of mapping data has shifted, or crept unexpectedly towards one where crime detection,

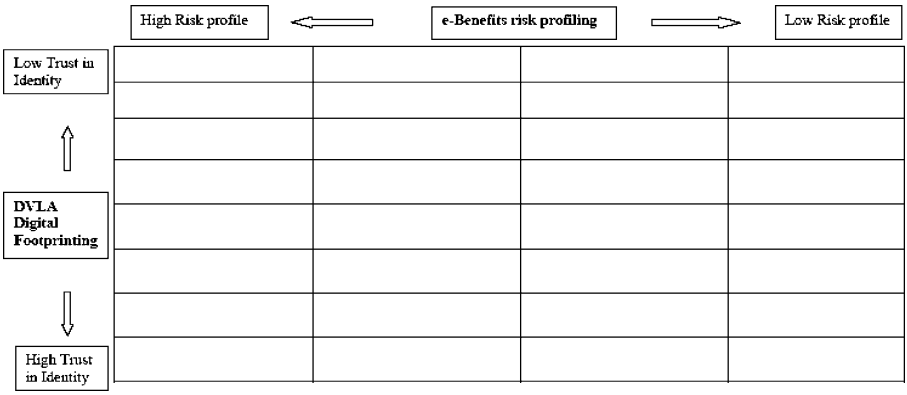


Fig. 3 The citizen in the matrix

prevention and prosecution were placed alongside the original Probation Service objectives.

Secondly, ANPR includes real time searching of a variety of data sets originating not only from the police and DVLA but from private sector sources also, as in the case of the Motor Insurance Database. The case study Force was continually developing relationships with other organisations in the hope of accessing new data, whilst the National ANPR Data Centre was set to arrange access to a variety of data sources for all Forces.

Thirdly, following the 'digital footprint' portion of the online provisional driving licence service, the DVLA use an established data link with the Identity and Passport Service to obtain digital passport photographs and signatures of existing passport holders for use on the production of driving licences. Applicants have to input their passport number for this aspect of the service to be used and can opt out by using another certified paper photograph. However, the application has to be completed offline should this second option be chosen by the applicant.

Fourthly, in the e-benefits case, the DWP are able to match local authority housing benefit applicant data with a variety of data sets held by the Department which provide indications of fraudulent or erroneous behaviour to be fed back to local authorities. For instance, database checks are made using the National Insurance Number of the applicant against death registers (fraudsters may use the details of dead citizens to claim benefits—known as 'NINO hijacking') and other benefits records. Furthermore, by converting the National Insurance Number to the corresponding Unique Tax Reference number, the DWP are able to check various Revenue and Customs databases (including 'P45', 'P46', Savings, Tax Exempt Special Savings Account, Construction Industry and other databases). Statistics drawn from the data matching exercise are used to inform the risk profiling operations of the DWP.

Two examples can be used to demonstrate the '***blurring of public private boundaries***' in service delivery. Firstly, Experian, the information management company, have become closely involved in online applications for driving licences. The main section of the 'layering' process described above, where decisions are made as to whether to permit applicants to complete the application process online, is conducted by Experian. The Government Agency involved, the DVLA, only reacts to the digital trust score

presented to it. The involvement of Experian is hidden from the point of view of on-line applicants, who are not explicitly made aware of the digital footprint process.

Secondly, a private security company has been closely involved in the satellite monitoring case. As well as supplying and fitting the tagging and tracking equipment, the company monitors the movements of offenders, deals with technical issues and plots, stores and sends digital maps to Probation and Police Service contacts. The private company in question is effectively the custodian of mapped data, to whom police and probation officers apply for further information such as retrospective mapping.

Towards a holistic appreciation of information-intensive government?

We have looked separately at these two distinctive interpretations of many aspects of contemporary government, the Service State and the Surveillance State, and shown how the data we have captured on citizen identification processes in government can be interpreted in each of two ways. Now, as we turn towards a proposed holistic appreciation of these two perspectives we return to the questions asked at the beginning of this paper, the first of which were 'how strong and amenable to refutation is the science base for these distinctive perspectives on contemporary government?'

Our answer to these first questions lies primarily in the work of Graham Allison, set out in brief earlier (Allison 1971). A fully scientific approach to understanding the service-providing activities of contemporary government implies, firstly, that each of the competing perspectives should be drawn together in a rounded analysis of those activities of Government relating to service provision. What we have seen, however, is that research on e-Government largely ignores the surveillance perspective, focussing instead on managerial issues of on-line service design and uptake, for example, whilst research on State surveillance largely ignores the services perspective. Reference is made in this surveillance literature to the 'beneficial' aspects of surveillance (e.g. Surveillance Society 2006, p2) but no evidence from research is brought forward in this literature to demonstrate these purported benefits. Secondly, we argue that a scientific approach to public surveillance is not possible without a clearer, tighter and more restricted definition of the meaning attaching to surveillance, one that lends itself to empirical testing. Currently, as we have seen in this paper, definitions of surveillance are drawn so broadly as to include most of the information-related activities of the corporate and government sectors alike, particularly in respect of their development of customer- and citizen-centric services. We do not propose a specific definition of surveillance in this paper though we do advocate that one should be brought forward that is clearly limited in its scope, one that speaks specifically to the personal service-providing activities of Government and one that allows for empirical testing. Our judgment is that such a definition will derive inductively from the proposals and procedures that we set out below.

Our second question at the beginning of this paper was 'can these perspectives be conjoined in a holistic appreciation and assessment of the dilemmas of modern government?' We have established that it is our judgment that to fulfil the requirements of scientific research they must be equally considered; but can that be done?

Here we turn, briefly, to the work of Vickers (1965), Nissenbaum (2004) and derivative work from Barth et al. (2006) to show that it may be possible to move closer to the holistic perspective for which we have called. It is our judgment that

taking on an holistic perspective such as this will provide a basis for the conduct of privacy and surveillance audits for which some are calling (Information Commissioner 2004; Bennett and Raab 2006; Surveillance Studies Network 2008). We set out our preferred, holistic, perspective in the five sequential points below:

- First, there must be an acceptance that in both studying and administering the personal service-providing areas of government, such as those examined in this paper, scholars and public officials accept the presence, in those areas, of differentiated informational dilemmas for both government and the citizen.
- Secondly, there should be acceptance that the extant universalism of privacy- [and surveillance-] protecting principles should be tempered through a recognition that solutions to privacy and surveillance dilemmas need to be found in the particular situational logic of a policy setting. Although this may already be the emergent situation *de facto* it should become a *de jure* reality.
- Thirdly, and following Vickers (1965) we should interpret a policy setting as an 'appreciative setting'. Writing before institutionalist perspectives were articulated, Vickers, nonetheless, provides such a perspective when he describes an appreciative setting as a "set of readinesses to distinguish some aspects of the situation rather than others" (Vickers 1965, p68). Such an appreciative setting is inhabited by professionals pursuing specific roles: roles that are guided by the norms and values of the setting as well as by informational principles that exist within that setting. Thus the specific context of any policy setting should be interpreted as a particular set of roles, norms, principles and values. Following Nissenbaum (2004), such contexts have 'integrity' for they represent relatively settled practices and procedures that make up the situational logic to which we refer in the second of these five points.
- Fourthly, and a further aspect of these practices and procedures, the 'principal & agent' roles of the official and the citizen can also be interpreted as occurring within both 'informational norms' that, in effect, regulate what personal information is captured, and 'transmission principles' that, in effect, regulate how such information flows between actors. This information nexus between the State and the citizen, which has also been built up over time, represents a further and crucial aspect of 'contextual integrity' (Nissenbaum 2004).
- Fifthly, specific policy settings should be investigated against this contextual integrity. Where it can be shown that extant norms and principles of personal data capture and flow are upheld in a new technologically-mediated environment, then we should not deem such an environment to be surveillance, in the negative sense of that word. Where new forms of technogically mediated relationships between the citizen and the State that violate 'contextual integrity' are brought into place we have a *prima facie* case that may be termed 'negative surveillance', one that should become the subject of audit.

Application and conclusion

The case studies that we have set out here provide a possible proving ground for the ideas set out in the section immediately above. We do not have the space in this paper to test those ideas to the full but we can point up key aspects of them that bear

upon the degree of contextual integrity resident in our case studies. To do so, we now turn back to these five points immediately above, offering brief evidence and analysis on each of them from our case studies.

First, we have shown in the breadth and depth of the public service domains that we have examined in our case studies the "informational dilemmas" that exist within them. For each of them, apart from the Satellite Monitoring study, there exists, for example, a fundamental dilemma between enabling ease of contact to a service for the citizen, on the one hand, whilst exercising due diligence in the form of risk assessment on that same citizen, on the other.

Secondly, we have shown, in particular through our examples of 'function creep and data sharing', how situational logic is already being applied within the context of the formal instruments and principles of fair information practices [FIP]. In other words these totemic principles of FIP are coming to have less and less meaning in the practices of government and commerce, as more and more avoidance is practiced and formal exclusions are permitted in recognition of the logic of specific service-providing situations.

Thirdly, we have seen how each of the policy settings related to our case studies is inhabited by different professional groups [Probation Officers, Police Officers; Local Government Benefits Officers; Civil Servants], each with their own norms, values and principles. We know from this and from previous research (Bellamy and Taylor 1996) how these norms, values and principles serve to individuate service domains rather than collectivise them. Thus from our work we argue that the structures of the State continue to be informed most strongly by the centrifugal forces of professionalized environments rather than an oft-assumed, quasi-monocratic centripetal forces of a Government.

Fourthly and fifthly, we must address the degree of contextual integrity residing in each of these cases and with it the presentation of *prima facie* cases for privacy and surveillance auditing. Here we must ask 'does the capture of personal information in these cases transgress the accepted norms of the citizen-State nexus and does any subsequent flow of personal information similarly transgress these norms?' It is here that we see most to investigate in our case studies, from both privacy and surveillance perspectives. Whilst the capture of basic personal information in these studies seems to us to be broadly commensurate with long-standing professionalized public practice, it is in the ***flow*** of personal information in some of these case studies that we find most to question. Thus, for example, in the driving licence case study, personal data is flowing from the citizen into a third party provider of authentication services without the knowledge of the citizen applicant. In the e-benefits case study, personal data flows through the algorithms of the DWP and the applicant for housing benefit assigned a socio-demographic category without their knowledge, a categorisation process that may involve the risk of subsequent 'false positive' identifications and threats to life chances (Lyon 2003).

The challenges that we raise in this paper both for academic researchers and public policy makers, are manifold, yet, it seems, there has been little inclination to recognise them in a more holistic way. Whether the citizen is to be viewed as a risk to be managed, and thereby an object for surveillance, or a consumer deserving the best possible public service, it becomes clear from our research that evidence on information-intensive methods of citizen identification contributes *prima facie* to the simultaneous upholding of each of these two distinctive perspectives.

We wish to move debate and practice on from the seeming irreconcilability of the different perspectives set out here and towards an holistic and considered understanding of public service provision and surveillance, deriving from close attention to policy contexts as appreciative settings within which 'contextual integrity', and breaches to it, can be identified. Such understanding will produce practical routes and reconciliations between naïve optimism about the roles of Government and the dark spectres attaching to them, alike.

References

Accenture. Leadership in Customer Service: New Expectations, New Experiences. London: Accenture; 2005.

Allison G. Essence of Decision: Explaining the Cuban Missile Crisis. Boston: Little, Brown & Co; 1971.

Bannister F. The Panoptic State: Privacy, Surveillance and the Balance of Risk. Information Polity 2005;10(1&2):65–78.

Barth A, Datta A., Mitchell JC, Nissenbaum H. 'Privacy and Contextual Integrity: Framework and Applications' in *Proceedings of the IEEE Symposium on Security and Privacy*, May 2006.

Bekkers V. Modernisation, public innovation and information and communication technologies: The emperor's new clothes? In Information Polity 2007;12(3):103–7.

Bellamy C, Taylor J. 'New Information and Communications Technologies and Institutional Change; the case of the UK Criminal Justice System' in *International Journal of Public Sector Management*. 1996;9(4):51–69.

Bellamy C, 6 P, Raab CD. 'Information risks and joined-up government' in: Lips M, Taylor JA, Bannister F, editors. Information polity: the international journal of government and democracy in the information age (special issue entitled Essays on risk and trust in the internet era: issues for governance, democracy and regulation; 2005.

Bennett C, Raab C. The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge: MIT; 2006.

Bogdanor V (ed). Joined up Government. Oxford: Oxford University Press; 2005.

Brownsword R. Rights, Regulation and the Technological Revolution. Oxford: Oxford University Press; 2008.

Burrows R, Ellison N, Woods B. Neighbourhoods on the Net: Internet-Based Neighbourhood Information Systems and their Consequences. Bristol: Policy; 2005.

Cabinet Office. Transformational Government: Enabled by Technology (cm 6683). London: HMSO; 2005.

Cabinet Office. Transformational Government: Implementation Plan. London: Cabinet Office; 2006.

Chief Surveillance Commissioner. Annual Report to the Prime Minister and Scottish Ministers. London: The Stationery Office; 2008.

DVLA. DVLA Annual Report and Accounts 2005–06—available at http://www.dvla.gov.uk/media/pdf/publications/anual_report_and_accounts2006.pdf; 2006.

DWP. Reducing fraud in the benefit system: Achievements and ambitions—available at www.dwp.gov.uk/publications/dwp/2005/fsu/reducingfraud.pdf; 2005.

DWP. Fraud and Error in Housing Benefit April 2002 to September 2005—available at http://www.dwp.gov.uk/asd/asd2/fraud_hb/HBR_Report_Jul06.pdf; 2006.

DWP. Getting welfare right: Tackling error in the benefits system—available at www.dwp.gov.uk/publications/dwp/2007/error_strategyPDFs/error_strategy_report.pdf; 2007.

Gandy O. 'Exploring Identity and Identification in Cyberspace' in *Notre Dame Journal of Law, Ethics and Public Policy* 14; 2000.

Graham S, Wood D. 'Digitizing Surveillance: categorization, space, inequality' in Critical Social Policy. 2003;23:2.

Greenway. Uninsured Driving in the United Kingdom—a report to the Secretary of State for Transport. London: DfT; 2004.

Hagen M, Kubicek H. One_Stop Government in Europe. Bremen: University of Bremen; 2000.

Home Office. Criminal Justice: the Way Ahead (cm 5074). London: HMSO; 2001.

Hood C. 'The Idea of Joined-Up Government: A Historical Perspective'. In: Bogdanor V, editor. Joined up Government. Oxford: Oxford University Press; 2005.
House of Commons Home Affairs Committee. A Surveillance Society? Fifth Report of the Session 2007–8; 2008.
Information Commissioner. The Identity Cards Bill—the Information Commissioner's Perspective December 2004—available at www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/id_cards_bill_-_ico_perspective_dec_2004.pdf; 2004.
Leben A, Kunstelj M, Bohanec M, Vintar M. Evaluating public administration e-portals. Information Polity 2006;11(4):207–25.
Lips AMB, vander Hof S, Prins JEJ, Schudelero AAP. Issues of On-line Personalisation in Commercial and Public Services Delivery. Nijmegan: Wolf Legal; 2006.
Lyon D. The Electronic Eye: the rise of surveillance society. Cambridge: Polity; 1994.
Lyon D. Surveillance Society: monitoring everyday life. Buckingham: Open University Press; 2001.
Lyon D (Ed). Surveillance & Social Sorting: privacy, risk and digital discrimination. London & New York: Routledge; 2003.
Margetts H, Yared H. Incentivisation of e-Government. UK National Audit Office, Session 2003–4 HC1267. London: The Stationary Office; 2003.
Nettleton S, Burrows R, O'Malley L, Watt I. Health e-types? An analysis of everyday use of the Internet for health, Information, Communication and Society. 2004;7(4).
Nissenbaum H. 'Privacy as Contextual Integrity'. Washington Law Review. 2004;79(1).
Norman DA. Affordances, Conventions and Design. Interactions 1999;6(3):38–43. ACM.
Office of the e-Envoy. UK Government Gateway Product Roadmap Review. London: Office of the e-Envoy; 2004.
PA Consulting. Driving Crime Down: Denying Criminals the Use of the Road. London: HMSO; 2004.
Regulatory Impact Unit. Making a Difference: Bereavement. London: HMSO; 2005.
Rhodes RAW. Control and Power in Central-Local Relations. Farnborough: Gower; 1981.
Rose G. 'The Criminal Histories of Serious Traffic Offenders' Home Office Research Study 206—Home Office Research, Development and Statistics Directorate available at www.homeoffice.gov.uk/rds/pdfs/hors206.pdf; 2000.
Seale C. 'Quality in Qualitative Research'. Qual Inq 1999;4:465–78.
Surveillance Studies Network. A Report on the Surveillance Society: for the Information Commissioner. UK: Newcastle; 2006.
Surveillance Studies Network. A submission to the UK Parliament House of Lords Constitution Committee Inquiry into the Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State; 2008.
Taylor JA, Lips AMB, Organ J. 'Freedom with Information: Electronic Government, Information Intensity and Challenges to Citizenship'. In: Chapman RA, Hunt M, editors. Freedom of Information: perspectives on open government in a theoretical and practical context. Ashgate: Aldershot; 2006.
Taylor JA, Lips AMB, Organ J. 'Information-intensive Government and the Layering and Sorting of Citizenship' in Public Money and Management. 2007;27(2).
Varney SD. Service Transformation: a better service for citizens and businesses, a better deal for the tax payer. Norwich: The Stationary Office; 2006.
Vickers G. The Art of Judgment. London: Chapman & Hall; 1965.
Walsham G. Interpretive case studies in IS Research: Nature and Method. In: Myers MD, Avison D, editors. Qualitative research in Information Systems. London: Sage; 2002.
6 P, Bellamy C, Raab C. 'Joined-up Government & Privacy in the United Kingdom: managing tensions between data protection and social policy'. Part 1. Public Administration. 2005a; 83:1.
6 P, Bellamy C, Raab C. 'Joined-up Government & Privacy in the United Kingdom: managing tensions between data protection and social policy'. Part 2. Public Administration. 2005b;83:2.