Information Commissioner's report to Parliament on the state of surveillance

Contents

Part A

Part B

The Surveillance Society

An update report on developments since the 2006 *Report on the Surveillance Society* by members of the Surveillance Studies Network

Charles Raab, Kirstie Ball, Steve Graham, David Lyon, David Murakami Wood, Clive Norris

November 2010

Part A

1. Summary and recommendations

Since 2006 there has been welcome strengthening of the data protection regime, a higher and better informed level of debate and scrutiny of surveillance related developments as well as a renewed political commitment to address the unwanted consequences of existing measures that raise concerns about unwarranted surveillance of the citizen.

Despite these welcome changes, technological and societal developments have proceeded and the risks to individual privacy remain real. Further safeguards are still required and require further protection. The Commissioner recommends:

a. Increased adoption of a 'privacy by design' approach through greater use of privacy impact assessments and adoption of privacy enhancing technologies across public and private sectors aimed at ensuring reductions in information risks

b. Inclusion of robust privacy safeguards as the default setting when new on line services are offered to individuals

c. A requirement for a privacy impact assessment to be presented during the parliamentary process where legislative measures have a particular impact on privacy

d. An opportunity for the Information Commissioner to provide a reasoned opinion to Parliament on measures that engage concerns within his areas of competence

e. Increased post legislative scrutiny of legislation, based on a formal report on the deployment of the legislation in practice, the value of the information collected, the impact on privacy and the continued need for such measures

f. In certain appropriate circumstances inclusion of a sunset clause in legislation that is particularly privacy intrusive

2. Introduction

The Home Affairs Committee in its report on its inquiry entitled "A Surveillance Society?" (HC 58-1) recommended that the Information Commissioner produce a report to Parliament on the state of surveillance (recommendation 2, paragraph 36). This report is in response to that request. The Commissioner had given evidence to that inquiry submitting in evidence commissioned research entitled "A Report on the Surveillance Society" produced by the Surveillance Studies Network, a group of respected academics and experts in this field. That report was published by the Commissioner in 2006 and this led to increased parliamentary, media and public interest in the developing capability to monitor and record information about citizens as they go about their daily lives. That report observed that much of what is taken as surveillance is undertaken for benign reasons with the aim of providing beneficial results for individuals and society. However the capacity to record information and to do so in many different contexts was increasing and this posed risks to individuals and society as a whole that needed to be addressed.

In the intervening period the Commissioner has developed his approach from one of helping ensure proper debate about developments to one of developing tools to assist with the effective proactive consideration and addressing of privacy risks in new developments. The production of a Privacy Impact Assessment Handbook and encouraging a 'Privacy by Design' approach to building privacy safeguards from first principles are examples of the practical focus of this work.

Since 2006 the value and vulnerability of personal information has become increasingly apparent with high profile information security breaches. This has further engaged the concerns of the public, parliamentarians and the media. It was apparent that information risk had outpaced the safeguards and governance in organisations as well as the regulatory sanctions necessary to encourage responsible use of personal information and to deter and punish those who do not live up to their legal responsibilities. The Commissioner has been given powers to impose monetary penalties for significant breaches of the law, to draft a statutory information sharing code of practice to encourage best practice and to carry out non consensual audit and inspection activities.

More recently concern over increased surveillance has become an election issue. The new Government has declared its wish to increase citizen control of their information and roll back what has been described as "the database state". These ambitions are in their early phase and how these will be met not yet fully articulated.

It is against this backcloth of substantial developments since 2006 that the current state of surveillance and the adequacy of any safeguards must be judged.

3. Developments in surveillance since 2006

The centrepiece of this report is the attached update report by the SSN entitled "The Surveillance Society-An update report on developments since the 2006 Report on the Surveillance Society". The Commissioner is indebted to the team that produced the report for again producing an expert and perceptive analysis. Their report gauges the changes between the original report and the present day. The report provides an authoritative account of the main trends and developments in surveillance in the United Kingdom and draws conclusions on whether safeguards and regulation have kept pace with these developments.

The report examines the information collected on individuals. It describes the proliferation of government databases, the increased use of CCTV and allied technology like automatic number plate recognition (ANPR) and how these can creep beyond their original function. It goes on to look at how there is increasing sophistication in the combination, analysis and sharing of information with the effect of sorting individuals into different categories. It notes how privacy risk can increase as personal information is shared more widely and how trends in social networking create new significant challenges.

The report analyses the impact of these developments noting that these engage a host of privacy and human rights issues. These arise from increased analysis of information and profiling of individuals, wider sharing sometimes for undeclared purposes and the flow of information beyond national boundaries. Function creep continues to be apparent and this undermines transparency and accountability. This is further underscored by the blurring of boundaries between the public and private sectors.

The report notes that since 2006 visual, covert, database and other forms of surveillance have proceeded apace and that it has been a challenge for regulators who often have limited powers at their disposal, to keep up. The report looks at how the regulatory landscape has changed and how this may do so in the future. The report observes that the quality of debate surrounding developments is hampering proper consideration. Anticipating and controlling new developments is a constant challenge. This has become more difficult as issues become enveloped in what is described as a 'hyperbolic fog' of claims and counterclaims about benefits and dangers concluding that Parliamentary and regulatory scrutiny would be improved with less exaggeration of the benefits and the dangers of surveillance.

The report concludes that there has been a better level of public, media and political debate since the previous report with surveillance becoming an election issue and being one of the first matters to be addressed by the incoming government. However, there are still many areas where surveillance continues to intensify and expand. Technologies that used to be the subject of speculation have moved into mainstream use. The linking and sharing of data from different databases, development of facial recognition, the

increased rollout of ANPR, private sector data gathering and analysis and increased information sharing are of particular note. In the longer term the continued development of 'ubiquitous computing', the deployment of sensing devices and the use of analytical tools to predict human behaviours will continue to challenge the existing regulatory repertoire and traditional assumptions.

The report poses the question whether regulation and crucially the awareness of the public has kept pace with the development of surveillance since 2006. It recognises that the increased powers within the regulatory system and the encouraging efforts in both public and private sectors to change the culture in personal information practices have been positive developments. It also recognises the role played by privacy impact and other proactive assessment methodologies and the increased interest in embedding privacy friendly mechanisms. However it observes that these must become the norm not the exception as at present. It concludes that important questions are whether current legal instruments on data protection and human rights at both domestic and European level are robust enough to limit surveillance and excessive collection of data and whether legal reform and better integration of the legal and other regulatory instruments will be the linchpin on which much else depends.

4. Information Commissioner's perspective

The Commissioner believes that the analysis of the developments in surveillance described in the report is soundly based. He recognises developments that have caused him to intervene to ensure that a data protection compliant approach is adopted. The creation of a national ANPR data centre by the police, the blanket requirement by some licensing authorities to install CCTV in all licensed premises irrespective of need, the fingerprinting of passengers using common departure lounges at airports and the creation of 'blacklist' databases are all instances. The continued stream of self reported security breaches continues to underline the risks to individuals' personal details.

He remains concerned to ensure that effective safeguards are in place to minimise information risk which can increase if developments in surveillance and greater exploitation of personal information go unchecked. He believes that whilst there have been welcome developments such as strengthening the data protection regime, greater scrutiny of surveillance developments and greater questioning as to whether existing developments go too far, there are still opportunities available to strengthen the safeguards that will help ensure that we do not end up with a society where citizen surveillance and inadequate protections become the norm.

The Commissioner believes that there is still greater scope for the adoption of a 'privacy by design' approach. Using privacy impact assessments and then adopting privacy enhancing technologies can do much to ensure that information risk is identified and then minimised. There is a worrying trend particularly with those who provide on-line services not to have thought through the privacy implications of their activities and given users robust privacy settings as a default.

On a more positive note it is clear that there is an increasing appetite for privacy friendly techniques in areas such as identity management, that help minimise personal data and put individuals increasingly in control of their information. Similarly there are privacy enhancing technologies which minimise access to identifying particulars and other personal information whilst still delivering the benefits sought in the first place. Whilst the Commissioner has worked hard to promote these, including developing a business case for adopting proactive privacy protection entitled 'The Privacy Dividend' much more still needs to be done. Adoption of proactive privacy safeguards could be much improved and innovation in the protection of personal information continues to lag behind the motivation and capability to exploit it. The Commissioner will be continuing to work to ensure that more is done to improve the current situation.

The report points towards particular gaps in the way developments are scrutinised not only during the process of debate and analysis but also in post implementation scrutiny. A number of examples in the report point to the use of powers granted to the Government and public bodies by Parliament to deal with pressing public policy concerns being used over time to address les pressing matters in a disproportionate way.

The Commissioner recognises that the parliamentary process is designed to provide thorough scrutiny of new measures but that this can be hampered when the assertions of those either for or against surveillance related developments are presented with little concrete evidence established on which to base decisions. The Commissioner suggests that imposing a requirement on Government to conduct a privacy impact assessment when bringing forward any law which engages concerns about increased collection and exploitation of personal details of citizens may aid parliamentary scrutiny. Those who make claims and counterclaims would have to back up their assertions with facts and evidence enabling conclusions to be drawn on whether the proposed measures are effective and proportionate when set against the impact on personal privacy. This assessment would be submitted as part of the scrutiny of such legislation. Providing the Commissioner with a formal opportunity to provide Parliamentarians with a reasoned opinion during the passage of legislation that impacts on information rights is a further possible option.

The Commissioner understands that on some occasions there may be emerging and pressing matters where the full scale of a problem and the impact of the proposed solution is difficult to judge or scrutinise. Where potentially far reaching measures are proposed which involve the collection, use or exploitation of personal information for new or different purposes then a form of enhanced post legislative scrutiny is required.

Parliamentary Committees already play an invaluable role in holding the Government and others to account for the use of powers granted to them. However this process is inevitably inconsistent as Parliamentary committees struggle under the weight of business and the range of matters which they must address. The Commissioner proposes a more formal and consistent approach to ensuring post legislative scrutiny. Legislation engaging significant privacy concerns should include on the face of it a requirement on the Government to report back to Parliament on how the measures have been deployed including evidence of the extent to which the expected benefits and possible risks have been realised in practice and the continued need for the measures in question. In certain cases consideration should be given to the inclusion of 'sunset clauses' which would cause legislation to lapse unless renewed on the basis of evidence of continuing value.

It is clear that where difficult issues affecting the balance between matters such as security, crime prevention and detection, transparency and privacy are concerned Parliament has a central role to play in ensuring proper debate and scrutiny particularly in the face of strongly argued assertions by proponents and opponents. The proposals suggested by the Commissioner for compulsory privacy impact assessments during the passage of legislation backed up by effective post legislative scrutiny once the legislation is being used in practice are aimed at assisting parliamentarians in their essential tasks.

Part B

The Surveillance Society

An update report on developments since the 2006 *Report on the Surveillance Society* by members of the Surveillance Studies Network

Charles Raab, Kirstie Ball, Steve Graham, David Lyon, David Murakami Wood, Clive Norris

1 - Executive Summary

This report selectively describes developments in surveillance since the publication of the *Report on the Surveillance Society* written by members of the Surveillance Studies Network (SSN) for the ICO in 2006. It comments on trends, new practices, and the regulatory landscape of responses and prospects.

The warning that the United Kingdom may be 'sleepwalking into a surveillance society' – or that one already exists, requiring limitation and regulation – is no less cogent in 2010 than it was several years ago. It is not being suggested that the UK is a 'police state' or that there are surveillance conspiracies afoot against the public. Neither the 2006 report nor this one supports such an assumption, and evidence for it is lacking. Much of what is taken to be surveillance is done for benign reasons and has beneficial effects on individuals and society. But much surveillance also goes beyond the limits of what is tolerable in a society based on the rule of law and human rights, one of which is the right to privacy.

Surveillance involves the use of techniques to gather and use information about individuals – their personal details, their movements and social contacts, their habits and behaviour, their communication – in order to make administrative or business decisions that affect their life chances and those of the groups or categories into which they are construed to fall. Surveillance has ancient roots in society and the state, but in today's world it engages the latest technologies to gather more data, to analyse it in minute detail, and to disclose and share it rapidly with a wide number of others, both within the UK and across national boundaries.

Since 2006, visual, covert, database and other forms of surveillance have proceeded apace, with regulators working hard to apply their often-limited

powers or to anticipate and control the next developments. Surveillance practices are often surreptitious, non-transparent, and unaccountable. The aims, motives and procedures of those who collect and use personal information are often unclear, and therefore difficult to regulate, even when they fall within the scope of the law.

Some commentators have noted the 'hyperbolic fog' that surrounds debate around one of the databases that have been in the spotlight in recent years – a ratcheting-up of claims and counter-claims by critics and champions of surveillance that does a disservice to public understanding and political or regulatory effectiveness. Parliamentary oversight as well as the work of statutory regulators requires less exaggeration of the benefits and dangers of surveillance, and a better grounding in knowledge of what the state of play is regarding surveillance and what is likely to occur in future.

For convenience, this report marshals evidence of trends and developments in UK surveillance under three main but overlapping headings:

- Information collection
- Information processing
- Information dissemination

It looks briefly but indicatively at information collection in terms of overt and covert surveillance, the proliferation of government databases, the burgeoning use of closed-circuit television (CCTV) and the increasing employment of Automatic Number Plate Recognition (ANPR) in ways that 'creep' beyond their original intended function. Although they might become issues largely for the future, it considers the use of unmanned drones and body scanning to detect. The report also looks into the collection of data in relation to border controls and the monitoring of employees in the workplace.

Information processing is not clearly separate from collection, and is highlighted by techniques of data combination and analysis, and by data sharing. The use of personal data gathered by ANPR in controlling protest activities is given as an example of the public-order application of data processing, and the increasing use of geodemographic tools (the combination of digital mapping technologies with individual or aggregated personal data) shows how people's spatial movements and locations are tracked, monitored, and represented by data. The processing of information for public-service administration is described, involving the sorting of populations into categories. Ethnic targeting features in some of the ways in which data are collected and processed, and – in the private sector,

but not confined to it – call centres illustrate the issues involved in the processing of data for certain activities.

The report considers information dissemination in terms of the broader communication or disclosure of personal information to a wide audience. The sharing of data between organisations has become a main means for this, and data breaches have also resulted in potentially widespread dissemination through unintended lapses in care and security. The huge growth in social networking is the most dramatic example of recent years, and has generated new and difficult privacy and data-protection issues on a global scale that pose a challenge to national regulators and law.

Turning to the implications of these aspects and examples of surveillance, and reflected in the trends of recent years, the report comments upon problems and issues regarding:

- Privacy, ethics and human rights
- 'Function creep'
- Transparency and accountability
- Blurring of the public and the private
- Unintended consequences

There are a host of privacy and human-rights issues involved in, for instance, techniques for analysing data about individuals, the sharing of data among organisations – often for undeclared and unconsented purposes – and the flow of data across national boundaries. 'Function creep' has been much commented upon, involving new uses for technologies or for data beyond what was originally envisaged or legitimated: for example, certain uses of ANPR and of databases collected ostensibly – and possibly under legislation – for a defined purpose. Such practices, as well as the sharing of data, make transparency and accountability very difficult, not only for regulators but for the public who are asking increasingly about what happens to their information. The public and private sectors are no longer discretely bounded, as data flows across them between the state and private companies in complex pathways. The distinction between private and public activities are also blurred, with one result being unintended consequences of practices that people engage in, for example exposing their 'private' and intimate social networking activities to wider audiences. There are serious privacy and ethical dilemmas in these trends.

Finally, the report reviews regulatory developments and problems, focusing on challenges and responses in recent years, in which the UK has seen a plethora of

parliamentary and other reports about surveillance and its implications for privacy and other social values, and has witnessed massive data breaches as well as other violations of data protection principles and information rights. Responses have featured innovations such as Privacy Impact Assessment, the encouragement of better data handling and more regulated systems for sharing data, stronger ICO powers and penalties, and more effective codes of practice. But the regulatory future is hard to discern in detail, including the likely revision of the European Data Protection Directive and consequent changes to UK law, and the efforts of the new Government to limit the perceived excesses of the 'surveillance society'.

The report finishes by canvassing some proposals that have been made elsewhere for strengthening, and integrating better, the regulatory forces of official agencies and civil-society as well, and for increasing the international efforts to limit surveillance and to protect privacy and related values. Whether these will be necessary or sufficient is a matter for discussion.

2 - Background

In 2006, the *Report on the Surveillance Society*,[1] produced by members of the Surveillance Studies Network (SSN) for the ICO, argued that we are already living in a surveillance society. The report defined the surveillance society as one that is organised and structured using surveillance-based techniques. There was no suggestion, then or now, that the United Kingdom was or is becoming a 'police state', or a society under total and malevolent control, as some commentators may assert. The report stated that to be under surveillance meant having information about one's movements and activities recorded by technologies, on behalf of the organisations and governments that structure the society. The report showed how this information is then sorted, sifted and categorised, and used as a basis for decisions that affect our life chances. Such decisions concern our entitlement and access to benefits, work, products, services, and criminal justice. They concern our health and well-being, and our movement through public and private spaces: in other words, most of what is regarded as our 'everyday' life.

Amongst the indicators, the report noted:

- The increasing ubiquity of video surveillance cameras, and automatic systems for number plate (and face) recognition
- Electronic tagging of those on probation
- DNA and many other databases, and 'precautionary' intervention
- The need to prove identity, for benefits, healthcare and so on, including the proposed new system of biometric ID cards linked to a central database of personal information
- Proposals for biometric passports and surveillance at borders
- The use of multiple surveillance systems in schools
- Consumer surveillance, the collection and sale of data, and the use of these data to provide differential levels of service
- The monitoring of telephone and Internet communications by intelligence agencies
- The monitoring of performance in the workplace.

[1] David Murakami Wood (ed.), Kirstie Ball, David Lyon, Clive Norris and Charles Raab, *A Report on the Surveillance Society for the Information Commissioners Office by the Surveillance Studies Network: Full Report*, 2006, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf, accessed 15/06/10.

The SSN argued that this society is the sum total of many different technological changes, policy decisions, and social developments. Some of it was shown to be essential for providing the services we need, for example, health, social security, and education, but some were considered to be unjustified, intrusive and oppressive. The report noted that until that point, there had been very little public debate about surveillance. At the same time, it was estimated that the global surveillance industry was worth almost 1 trillion US dollars, covering a massive range of goods and services from military equipment through high street CCTV to smart cards.

It was stated very specifically that this was not a conspiracy or always a matter of deliberate policy, but the result of a confluence of many different trends, and the report noted that the intention behind many surveillance systems was benign. Nevertheless it was argued that this did not justify apathy or a lack of scrutiny and regulation, and that understanding the often unintentional controlling effects of surveillance and the impacts they have on our personal lives and on society was crucial.

This analysis was placed in a social context that had become increasingly concerned with risks and dangers (both to security and to profit), rather than positive social goals. Thinking of more and more everyday situations in terms of 'risk' leads to what was previously exceptional security becoming normal, and to many unintended consequences that generate inequalities of access and opportunity, and distinctions of class, race, gender, geography and citizenship. These discriminations are not only made worse but also fixed into the way all everyday decisions are made.

One of the biggest effects of surveillance processes and practices is to create a world where we are not really trusted. Surveillance, it was argued, fosters suspicion, whether this is in the private sector – with the employer who installs keystroke monitors at workstations, or tracking devices in service vehicles – or in state services, where the welfare benefits administrator seeking evidence of double-dipping or soliciting tip-offs on a possible 'spouse-in-the-house' is saying she does not trust her clients. Even at the personal level, there were an increasing number of technologies designed for parental use in checking on children's activities. Trust, therefore, as much as privacy, was the major casualty of the surveillance society.

But at the same time, it was shown that the decline of trust creates a further demand for more certainty about those others we no longer trust: about backgrounds, identities, interests, motives, and even likely future behaviour. This

demand places a high priority on the collection and analysis of personal information, storing it in large databases with increasing interaction and sharing of data. The report asked whether we had become so hypnotised by the 'need' to find high technology solutions to crime, terrorism, fraud and many other problems that we forget to ask whether these solutions even work in the ways they were intended, let alone whether they were appropriate in a wider social context, or might have consequential side-effects, and whether there might be other, non-technological or less invasive answers. The report did not discount that possibility that people may want to live in a surveillance society, but if that was the case, it was argued that it had to be something decided in full understanding, with our eyes open and not in our sleep.

All these themes and analyses that were explored are at least as relevant in 2010 as they were in 2006. This much briefer Update Report focuses on the key thematic developments since the 2006 report. These include:

- the increasing blurring of private/public sector boundaries in collecting and processing surveillance data
- the increasing nodes in the system, both public and private, where information is collected, processed and shared
- the application of more sophisticated analytics for data-mining and profiling, leading to enhanced mechanisms to privilege, prioritise and exclude
- the decreasing visibility of surveillance processes, which is paralleled by an increase in their social consequences.

Research for this report was guided by some key questions that remain pertinent today:

- are there new applications of technology?
- are there new instances of 'function creep'?
- have new unintended consequences been produced?
- have there been new instances of information-sharing across public/private boundaries?
- have new forms of analysis been applied to personal data?
- whose lives have been enabled and constrained, and how has this changed?
- has public accountability for surveillance practices changed?
- are there new challenges to the regulation and limitation of surveillance?
- have the recommendations of parliamentary reports been satisfactorily implemented?

- how have the possibilities and practices of public and parliamentary scrutiny changed?
- are the surveillance and regulatory trends of recent years likely to continue?

Documenting and analysing the impact of these developments forms the core of the report, with particular attention to their implications and the challenges they pose for regulatory regimes.

3 - Main Areas of Surveillance, 2006-10

The current report concentrates on a small number of areas and recent trends in surveillance, but seen in terms of the processes they illustrate, and the issues to which these processes give rise, before the penultimate section considers the implications of these processes and issues for policy and regulation.

Three types of activity that can present privacy problems and lead to regulatory challenges and responses are identified. These are the *collection*, *processing* and *dissemination* of information.[2]

The surveillance processes highlighted are described under these headings, although in many cases the examples involve more than one of these kinds of activity. It should be borne in mind that there are also beneficial purposes served by activities in these groups, but in focusing on the potential regulatory problems, attention must be concentrated on the more disturbing effects on individuals and society. It can also be argued that the balance between the more positive and caring aspects of surveillance and those that are more harmful has shifted even more towards the latter in recent years. The examples described in each of the three subsections give rise to a number of implications and issues to be dealt with by public policy and regulation. Comments upon these issues are given later in the report.

[2] This reflects, in part, the taxonomy in Daniel J. Solove, 'A Taxonomy of Privacy', *University of Pennsylvania Law Review*, 154, 3, 2006, pp. 477-560. His fourth category, 'invasion', involves intrusion and interference with decisions. It need not involve personal information, but often does, and sometimes represents the effects of social sorting and covert surveillance that are discussed at a later point.

4 - Trends in Surveillance

Information Collection

The collection of personal information has become increasingly central to the activities of organisations in both the public and private sectors. Many large databases of personal information have been created on segments of the population, and online collections of data in social networking, commercial and governmental contexts are now common features of contemporary life in the UK. The covert or overt surveillance of the population, especially in public places, along with tracking physical movement and behaviour, overlap with database collections. The 2006 report illustrated the prevalence of these activities; since then, we have not until very recently seen any significant decline in the practices, nor any major increase in regulation. This report touches on, but does not discuss at length or systematically the increase in surveillance operations conducted by police and other public authorities under the Regulation of Investigatory Powers Act (RIPA) 2000. This has attracted criticism, perhaps most notably in the case of its use in fairly trivial circumstances by local authorities, whose use of RIPA powers – not envisaged in the original legislation – has proliferated, attracting public and parliamentary criticism.[3] Other matters of serious concern include the procedures for authorisation of surveillance operations, and the fragmented system of oversight through Commissioners, both of which have cast doubt upon the effectiveness of surveillance regulation under one of its main legitimising statutes.

However, as we shall note, the recent change of Government has now led to some significant rolling back in some areas of state data collection, and further changes are promised, although in a number of cases are far from certain to be put in place. This should not, however, distract attention from those areas that remain unaffected, nor from the growing importance of private sector data collection.

Government databases

Public services rely heavily on the collection and further processing of large amounts of personal data, increasingly so because of the trend towards anticipatory, proactive and predictive policy-making and implementation. In 2006, the SSN reported that the use of personal information for public services is a form of surveillance that poses threats to privacy and other social values, even though it serves beneficial purposes: saving lives, protecting the vulnerable, and

[3] e.g. House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the State*, HL Paper 18-I, paras. 153-77.

making public services more efficient and effective.[4] On the other hand, because data collection is so ubiquitous, the protection of personal information and the restriction of database surveillance is made at once more difficult and more necessary. There is little in the experience of the past four years that would cause a serious questioning of that overview.

In 2008, the Government's written evidence to the House of Lords Constitution Committee's surveillance inquiry described a large number of policies, practices and systems for personal data collection, data sharing and surveillance in central government departments and agencies.[5] This report can only deal with a few of these; for example, it leaves on one side law-enforcement databases and the NHS IT development. In terms of databases, the blurring of the boundaries of the public, private and voluntary sectors continues; the aim of 'joined-up' government – transformed and enabled by technology[6] – has not abated, although the pace is often halting and in certain sectors, such as health, enormous IT implementation difficulties persist. Government still pursues policies based on 'better safe than sorry' premises that require large amounts of personal data to identify and profile those at risk of harm to themselves or to others. Parliamentary scrutiny and privacy safeguards lag behind, and there is insufficient independent assessment of necessity and proportionality.

It is impossible to say how many databases there are in the public sector, in part because the term 'database' is not a precise one. It cannot be affirmed that the judgments and legality ratings concerning 46 UK state databases made in a prominent recent review[7] are anchored in reliable methodology yielding sound evidence, and those opinions are therefore not endorsed in the present report; in addition, the previous Government's rebuttal is to be noted.[8] Nevertheless, that study of the 'database state' reflects wider concerns about the resort to database 'solutions' to social or policy problems, and served to bring this trend into wider public awareness and debate.

For several years following the 2006 report, government's propensity to process

---

[4] Charles D. Raab, 'Expert Report: Public Services', in Murakami Wood *et al.*, *op cit*, *A Report on the Surveillance Society – Appendices.*

[5] House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the State*, HL Paper 18-II, pp. 315-41.

[6] Cabinet Office, *Transformational Government – Enabled by Technology* (Cm 6683), London: The Stationery Office, 2005.

[7] Ross Anderson, Ian Brown, Terri Dowty, Philip Inglesant, William Heath and Angela Sasse, *Database State*, York: Joseph Rowntree Reform Trust, 2009, p. 4.

[8] Ministry of Justice, *Government response to the Joseph Rowntree Reform Trust report: 'Database state'*, 08/12/2009, available at: http://www.justice.gov.uk/government-response-rowntree-illegal-databases-report.pdf, accessed 19/04/10.

ever more data continued with, for example, the National Identity Register (NIR), the controversial database that formed the heart of the identity cards scheme (2006). The Government elected in 2010 has, however, announced the demise of identity cards for UK citizens and the destruction of the NIR, although questions remain about how its data, which is not unique to the NIR as such and which forms part of the life-blood of state administration, will be used. There are concerns on grounds of discrimination about the continuation of identity cards for non-citizens and the use of data collected for supplying these. Moreover, surveillance practices with respect to the identification and verification of individuals and their claims persists across government, even in the absence of a discrete 'identity card'. The policy aim to transform government and its services through the use of information technology, especially online, is likely to generate continuing problems concerning data protection, including data security, and possible discriminatory effects, despite the professed reforms in data handling that followed the rash of data breaches in 2007 and after.

Another example, still in formation, is the Vetting and Barring Scheme (VBS) managed by the Independent Safeguarding Authority (ISA), established in England and Wales and coming on stream from 2010 to 2015.[9] The Scheme covers those who come into regular contact with children and vulnerable adults and requires such paid or voluntary workers, with some categorical exceptions, to register with the ISA, with the application and monitoring processes being performed by the Criminal Records Bureau, which already operates criminal records checks. There will be lists of those who are barred from contact with children and vulnerable adults. ISA decisions will be based on information from the police as well as referrals from employers and regulatory or other agencies. In addition to information on offences, convictions and cautions, evidence of 'inappropriate behaviour' or of behaviour likely to result in harm will be considered. The ISA said that '[r]eferral information, such as allegations, will never lead to automatic inclusion on the ISA Barred Lists. Before a barring decision is made, the individual is given the information on which the decision is based and the opportunity to explain their case.'

This new system was established following the recommendation in the 2004 Bichard Report on the Soham murders. However, by saying that the vetting scheme 'is about making sure we can stop that very rare risk, because if it led to

[9] Factsheets and material formerly on the ISA website at http://www.isa-gov.org.uk/, accessed 24/04/10, are now unavailable; FAQs on the website of the Department of Children, Schools and Families at http://www.dcsf.gov.uk/news/index.cfm?event=news.item&id=vetting_and_barring_myth_buster, accessed 24/04/10, are now unavailable.

harm, the harm could be devastating', the previous Government revealed an approach to risk that established an elaborate system to guard against events that, they admitted, were highly improbable. This raises concerns about the disproportionality of a Scheme that, according to some, reverses the assumption of innocence regarding the individual and may lead to decisions being influenced by 'soft' information. The previous Government scaled back its scope following criticism, and the current Government has announced that it will 'review the criminal records and vetting and barring regime and scale it back to common sense levels'.[10] At the time of writing, further details had not been made available, although it is to be hoped that a revised Scheme will accord better with the spirit of data protection and human rights. A great deal will depend on how the Scheme is implemented, including the transparency of decision-making and ensuring rigorous safeguards for the data involved in the vetting process. The ICO has in the past not been convinced that all the data protection implications of VBS had been resolved, but 'received assurances that the scheme will engage with the ICO in constructive dialogue'.[11]

A further example is the database on all children in England and Wales up to age 18, on which the *Report on the Surveillance Society* commented in 2006, and which was renamed 'ContactPoint'. This is intended to improve and speed up contact between professionals in children's services across England and Wales. Implementation began in local authorities late in 2009, following a period of limited early adoption.[12] It may be too soon to evaluate its success[13] or its avoidance of the potential privacy and human rights dangers highlighted by its many critics in NGOs and parliament. These include accessibility by too many persons (reportedly, over 330,000), undue interference with family privacy, ignoring children's rights, and violation of European Convention rights under Article 8.[14]

ContactPoint raises privacy concerns over the storage of sensitive data with no effective opt-out, lack of security, and potential relationship to the NIR.[15] On the

---

[10] HM Government: *The Coalition: Our Programme for Government*, 05/2010, p. 20, available at: http://programmeforgovernment.hmg.gov.uk/, Accessed 15/06/10.
[11] ICO Policy Committee Minutes, 14/09/09, available at: http://www.ico.gov.uk/upload/documents/library/corporate/notices/20090914_pc_september_mins.pdf, accessed 15/06/10.
[12] Department for Children, Schools and Families, 'Contactpoint to start national rollout', 06/11/09, available at: http://www.dcsf.gov.uk/pns/DisplayPN.cgi?pn_id=2009_0210, accessed 19/04/10.
[13] But there are research-based apprehensions about its usefulness in the daily work of practitioners; see Sue Peckover, Sue White and Christopher Hall, 'Making and Managing Electronic Children: e-Assessment in Child Welfare', *Information, Communication and Society*, 11, 3, 2008, pp. 375-94.
[14] See Joint Committee on Human Rights, *Children Bill*, Nineteenth Report of Session 2003-04, HL paper 161.
[15] Anderson *et al.*, *op cit* pp. 17-18.

other hand, the previous Government robustly defended ContactPoint and rejected such criticism in detail as vague and unfounded.[16] In this 'hyperbolic fog'[17] of criticism and defence, which stifles genuine debate about these issues and contributes little to public understanding and sensible policy-making, it can still be argued that this and other large databases are likely to pose threats that require vigilant regulatory oversight. The new Government has pledged seriously to reassess ContactPoint but, again, details about this have not been announced. There remain considerable pressures from the child-protection and care community for some form of collected data on children, whether gathered centrally or not, and even if it is confined to only certain categories of children – itself a form of social sorting and discrimination, albeit benevolently intentioned. Therefore, it would be premature to consider that the demise of ContactPoint itself will reduce concerns about the collection and processing of often sensitive and 'soft' data on children.

A final example is the National DNA Database (NDNAD), which has caused concern because of its collection and retention of millions of samples taken from persons over ten years of age and from crime scenes, including the DNA of those who were never charged or convicted of a recordable offence. Scotland and Northern Ireland have separate databases operating under different retention rules. In proportionate terms, the NDNAD is the largest of its kind in the world, containing DNA profiles of more then 7 per cent of the UK population. England and Wales are unique amongst Member States of the European Union in systematically retaining the profiles or samples of individuals who have not been convicted of a crime.

Government and the police, as well as critical groups, have seen the NDNAD as an essential tool in law enforcement, but many – including parliamentary committees – have raised serious concerns, especially with the retention of DNA profiles of large numbers of innocent people who should arguably be treated as though they had never been arrested. In December 2008, the European Court of Human Rights (ECtHR) delivered its judgement in the case of *S. and Marper v. the United Kingdom*, a case that was brought by two individuals, one of whom had been charged with a recordable offence but was subsequently acquitted, and the other charged but saw his case discontinued. Both had requested that their DNA be removed from the NDNAD. The ECtHR ruled that the Government's policy breached Article 8 of the European Convention on Human Rights. The Government then resisted complying with the Court's ruling. The new

[16] Ministry of Justice, *op cit* pp. 27-9.
[17] Peckover *et al.*, *op cit.*

Government has now committed itself to implementing the ruling along the lines of the Scottish model of deletions and much more limited retention periods.

Two other NDNAD issues remain important. The first concerns possible discrimination, in that some groups are over-represented on the database in relation to the general population, in part related to stop-and-search policies in policing that disproportionately target black and other ethnic minority persons. The second is the implications in the development of familial searching techniques, whereby offenders who do not have a profile on the database can be traced through a close relative who does. This of course represents a significant expansion of the reach of the database, which started as one of offenders, then of suspects, and now covers the relatives of those on the database.[18]

Visual surveillance through CCTV and ANPR

Visual surveillance through CCTV is perhaps the image most people have in mind as denoting what 'surveillance' means. The use of public-space CCTV has become even more widespread for various purposes associated with the prevention and detection of crime and the maintenance of public order. Yet its relative ineffectiveness in achieving its objectives, despite its public and political support, has remained a remarkable anomaly.[19] Recognition of the need for improvement in CCTV's ability to fulfil functional expectations came with the promulgation of a 'new strategy' in 2007 by the Home Office and the Association of Chief Police Officers (ACPO).[20] This strategy was aimed at overcoming many of the technical and operational flaws of CCTV schemes, and at improving standards, quality and training.

CCTV has also continued to find new applications. In September, 2006, Middlesbrough police announced that they had fitted 7 of their 158 CCTV cameras with loud speakers enabling control-room staff to 'talk' to those they were monitoring. The aim of the system was to 'shame' low-level offenders into conformity.[21] In April, 2007 talking CCTV was extended to 12 other areas though

---

[18] For a discussion about the implications of familial searching see Chris Pounder 'Issues Arising for the Retention of DNA Personal Data', p. 9, available at: http://www.amberhawk.com/uploads/website%20DNA%20article%202010(2).pdf, accessed 15/06/10

[19] The latest meta-evaluation is the Campbell Collaboration report, based partly on research funded by the Home Office, which found that there was very little evidence of the success of CCTV except in controlled spaces like car parks. Brandon C. Welsh and David P. Farrington, *Effects of Closed Circuit Television Surveillance on Crime*, Oslo: The Campbell Collaboration, 2008.

[20] Home Office and ACPO, *National CCTV Strategy,* 2007.

[21] 'Big brother is shouting at you', *Mail Online*, 16/09/06, available at: http://www.dailymail.co.uk/news/article-405477/Big-Brother-shouting-you.html, accessed 15/07/10.

the use of a £500,000 grant from the Government's Respect programme.[22] In 2007, the Home Office initiated a £3 million national roll-out of body-worn CCTV to police forces[23] after a trial in Plymouth.[24] CCTV has also found increasing use in less obvious law-enforcement roles. In 2006, the Department for Environment, Food and Rural Affairs commissioned research to produce good-practice guidelines for the local authority management of fly-tipping,[25] the report stressing CCTV's utility in prosecutions. In particular, it recommended that serious consideration be given to the use of covert CCTV, although the good-practice guidance was silent on how to ensure compliance with RIPA.[26] Moreover, the use of covert CCTV by local authorities to tackle a range of low-level offences from parking to littering to defying the smoking ban have led to calls for local authorities to be stripped of their powers under RIPA. The new Government intends to ban their use of RIPA powers 'unless they are signed off by a magistrate and required for stopping serious crime'.[27]

That CCTV has become a routine feature of most urban public space landscapes now seems to be taken for granted. However, police and Government attempts to impose mandatory CCTV requirements on the private sector have run in to some resistance since 2006. In March, 2009 it was reported that the Metropolitan Police had insisted to a public-house landlord in Islington that they would oppose his licence application unless he installed CCTV. The landlord claimed it was an infringement of his customers' civil liberties, and after the ICO intervened the police backed down. A number of other police forces have tried to emulate Islington, arguing that landlords believe cameras improve security in pubs, although it is the licensing authority, not the police, who make the final decision. The previous Government proposed that CCTV systems should be installed in licensed premises in positions dictated by the police, with CCTV footage being kept for 28 days and made available on request to an authorised person or a constable. The ICO argued that, while surveillance in a specific pub can combat

---

[22] Philip Johnston, 'Oi! Talking CCTV cameras will shame offenders', *The Daily Telegraph*, 05/04/07, available at: http://www.telegraph.co.uk/news/uknews/1547663/Oi-Talking-CCTV-cameras-will-shame-offenders.html, accessed 15/07/10.

[23] "Smile, you're on camera!" Police to get "head-cams"', *Mail Online*, 13/07/10, available at: http://www.dailymail.co.uk/sciencetech/article-467877/Smile-youre-camera-Police-head-cams.html, accessed 15/07/10.

[24] 'A watching brief with body-worn video devices', *BAPCO Journal*, 25/07/07, available at: http://www.bapcojournal.com/news/fullstory.php/aid/752/A_watching_brief_with_body-worn_video_devices.html, accessed 15/07/10.

[25] http://www.defra.gov.uk/environment/quality/local/flytipping/research.htm, accessed 15/07/10.

[26] Jill Dando Institute of Crime Science, *Fly-tipping: Causes, Incentives and Solutions – A good practice guide for Local Authorities*, 6 July 2006, available at: http://www.defra.gov.uk/environment/quality/local/flytipping/documents/flytipping-goodpractice.pdf, accessed 15/07/10.

[27] HM Government, *The Coalition: our programme for government*, May, 2010, available at: http://programmeforgovernment.hmg.gov.uk/files/2010/05/coalition-programme.pdf, accessed 15/07/10.

specific problems of bad behaviour, to hard-wire such blanket coverage where there has been no history of criminal activity is likely to breach data protection requirements.[28] In the end, it appears to have been economic rather than data protection considerations which laid rest to these plans: the Government's consultation revealed strong opposition from the industry on financial grounds,[29] and the proposal was withdrawn.

Video surveillance has also expanded in state institutions. In particular, the use of CCTV in schools has migrated from perimeter security and access control to monitoring pupil behaviour in public areas such as in corridors and playgrounds, and to more private realms such as changing rooms and toilets.[30] Furthermore, a recent survey by the Association of Teachers and Lecturers found that 7 per cent of teachers reported CCTV being used to monitor classrooms, raising fears that CCTV would be used to monitor teacher performance as well as pupil behaviour[31]. As the function of school CCTV has changed, it is apparent that some schools have not understood their new regulatory responsibilities.[32] These issues are only likely to intensify with new uses for cameras in education, such as the remote-operated web-cams on laptops provided for pupils' home use in the USA.[33] Similar practices are more likely in the UK if private sector management of state schools spreads, as the Government intends.[34]

The growth in one form of visual surveillance aimed at data collection has attracted increasing attention: Automatic Number Plate Recognition (ANPR). ANPR illustrates the progress of data-enhanced policing, using new technological tools to move from being an 'add-on' project 'to becoming a mainstream policing tool, integrated into police force strategies and policy, tactics, systems,

---

[28] 'Warning over use of CCTV in pubs', *BBC News*, 16/03/09, available at: http://news.bbc.co.uk/1/hi/uk/7946752.stm, accessed 15/07/10.
[29] Association of Convenience Stores (ACS), 'Response to Safe, Sensible and Social: Selling Alcohol Responsibly', available at: http://www.acs.org.uk/en/lobbying/issues/alcohol/, accessed 15/07/10.
[30] Emmeline Taylor, *I Spy with My little Eye: Exploring the Use of Surveillance and CCTV in Schools*, Unpublished PhD Thesis, University of Salford, 2009, Chapter 5.
[31] Olinka Koster, 'Revealed: The CCTV cameras spying on hundreds of classrooms, *Daily Mail*, 18/08/08, available at: http://www.dailymail.co.uk/news/article-1046236/Revealed-The-CCTV-cameras-spying-hundreds-classrooms.html, accessed 15/06/10.
[32] See Taylor, *op cit.*
[33] Ron Todt, 'School Caught In Spying Scandal Admits Activating Webcams On Students' Laptops', *Huffington Post*, 02/20/10, available at: http://www.huffingtonpost.com/2010/02/22/harriton-high-school-admi_n_471321.html, accessed 15/06/10.
[34] Patrick Wintour and Nicholas Watt, 'Coalition's schools plan to create 2000 more academies', *The Guardian*, 25/05/2010, available at: http://www.guardian.co.uk/education/2010/may/25/david-cameron-coalition-academies-plan, accessed 15/06/10.

processes, training and baseline funding'.[35] However, within the private sector, other uses are flourishing, illustrating the collection of information but information processing and sharing as well. The Driver and Vehicle Licensing Agency (DVLA) does not just supply information to the police, but also to a variety of accredited trade associations.[36] In 2007, it was reported that the DVLA was selling driver details to 157 firms at a charge of £2.50 per enquiry, making the details of millions of drivers available to bailiffs, credit-control companies, debt collectors, property managers, leisure centres, solicitors and a large financial services firm.[37] Since 2005, the DVLA is said to have raised an estimated £44 million by selling details on 18 million registrations.[38]

ANPR systems in privately owned car parks are increasingly linked to the DVLA database and used to enforce parking rules and restrictions through the use of a Parking Charge Notice (PCN), akin to a fine, for breaches to the regulations, such as overstaying or parking in a restricted area. The DVLA database is used to provide the name and address of the registered keeper so the PCN can be sent to their home address;[39] if not complied with, civil action is undertaken with bailiffs potentially being engaged to enforce payment. The possibility that DVLA data could be commercially exploited through more novel uses of ANPR technology was recently reported. A prominent motor-oil company's advertising campaign included billboards on five major London routes. Roadside cameras recorded number plates before flashing their registration onto screens and indicating the grade of oil recommended for the vehicle. To enable this precision, another firm had apparently been used to obtain vehicle data, believed to have contained most of the 34 million-strong driver details held by the DVLA. While the DVLA had neither sold its data to the oil company nor given permission for its use in this way – which would contravene the prohibition of the use of registration numbers for marketing purposes – it appears that data had been supplied to the third-party company by a firm to which DVLA does sell data. When the DVLA

[35] ACPO, *ANPR Strategy for the Police Service – 2007/2010*, September 2007, p. 2.
[36] DVLA, 'DVLA Accredited Trade Associations (ATAs)', available at: http://www.dft.gov.uk/dvla/data/trade.aspx, accessed 16/07/10.
[37] Martin Delgado, Rob Ludgate and Mark Nichol, 'DVLA sells your details to criminals', *Mail Online*, 12/02/07, available at: http://www.dailymail.co.uk/news/article-369838/DVLA-sells-details-criminals.html, accessed 16/07/10.
[38] John Oates, 'DVLA makes £44m flogging drivers' details', available at: http://www.theregister.co.uk/2010/01/20/dvla_data_flog/, accessed 16/07/10.
[39] National Parking Control, 'A.N.P.R. Services', available at: http://www.nationalparkingcontrol.co.uk/anpr_services.asp, accessed 16/07/10.

complained, the advertising campaign was abandoned.[40] These examples provide evidence of the process of 'function creep', as is pointed out later.

In 2005 ACPO published their National ANPR Strategy, 'Denying Criminals the Use of the Roads 2005/2008'. The strategy is underpinned by the creation of new data flows between cameras and the ANPR database, and between the latter and existing databases. The strategy consisted of four key components, the setting up of a national network of ANPR-capable cameras; the creation of dedicated force intercept teams; real time linkages with the DVLA database of registered keepers of motor vehicles and to the databases contained on the Police National Computer (PNC) (the system is also linked to local force databases, the Motor Insurance Database and counter terrorism databases); and the creation of a National ANPR Data Centre to house a database capable of storing 50 million ANPR 'reads' per day.[41]

The main aims of ANPR systems extend from the apprehension of owners of untaxed and uninsured vehicles, and car thieves, to the wider one of 'targeting criminals through their use of the roads'. In so doing, the movements of all vehicles, not only those involve in criminal activity, are tracked. There is now a national network of some 10,000 ANPR-enabled cameras installed in the UK, as well as intercept units in all police forces, a Data Centre lodging some 10-14 million ANPR 'reads' per day,[42] and real-time police access to all ANPR reads from Transport for London's (TfL) Congestion Charge scheme, allowing them to track all vehicles entering central London. With the advent of vehicle-borne terrorist activity, the Home Secretary in 2007 ordered an exemption of TfL from parts of the Data Protection Act. While the TfL data can only be used currently for issues relating to national security,[43] the Home Secretary did not rule out the possibility

---

[40] Christopher Leake, 'Drivers' details sold by DVLA are used in bizarre roadside adverts for Castrol', available at: http://www.dailymail.co.uk/news/article-1216414/Now-drivers-details-sold-DVLA-used-bizarre-roadside-adverts-Castrol.html, accessed 16/07/10.

[41] See 'Fears over privacy as police expand surveillance project', *The Guardian*,15/9/2008, available at: http://www.guardian.co.uk/uk/2008/sep/15/civil_liberties, accessed 15/06/10

[42] See 'Police secretly snapping up to 14m drivers a day', *Times Online*, 4/4/10, available at: http://www.timesonline.co.uk/tol/news/uk/crime/article7086783.ece, accessed 15/07/10. ACPO Freedom of Information requests have revealed an exponential rise in data flow to the National Data Centre from individual police forces. For instance, between 2007 and 2008 Devon and Cornwall police recorded a near 10-fold increase in ANPR reads from 6.7 million to 63.9 million and Dyfed-Powys Constabulary recorded a 12-fold increase from 2.6 million to 33.2 million. See http://www.dyfedpowys.police.uk/documents/FoIDisclosure/RoadsPolicing/2009/361.pdf, and http://www.devoncornwall.police.uk/YourRightInformation/FreedomInformation/Lists/Disclosure%20Logs/Attachments/282/Record%201.pdf, accessed 15/06/10.

[43] *BBC News*, 'Met given real time c-charge data', 17/07/2007, available at: http://news.bbc.co.uk/1/hi/uk_politics/6902543.stm, accessed 15/06/10.

of police using the data for other purposes in future.[44] Further uses of ANPR data are highlighted later on.

Unmanned drones
Recent developments in national security technologies – unmanned drones and body scanners – provide further examples of novel forms of information collection. These are not yet significantly deployed in the UK, but if they were more fully implemented in future, they would mount important challenges for regulation and surveillance control.

The deployment of unmanned helicopter drones (Micro-Unmanned Aerial Vehicles, Micro-UAVs, or MAVs) in UK civilian airspace for policing purposes has begun with the recent trial conducted by Merseyside Police. Derived from military models now widely used in counterinsurgency operations, drones are equipped with wirelessly-connected digital CCTV systems that can record extremely high-resolution images, in the visible and infra-red spectrums, from heights of 500m. At 100m hovering height, the drone's small size and battery power means that it is rarely noticed from the ground. It is quite probable that the use of drones will become more commonplace in covert surveillance, and will feature in the policing of the 2012 Olympic Games. The South Coast Partnership (SCP), a project led by Kent Police involving five other police forces in conjunction with BAe Systems, plan to pilot the use of drones with a wide range of potential uses. *The Guardian's* Freedom of Information requests have revealed that the list of potential applications includes addressing 'fly-posting, fly-tipping, abandoned vehicles, abnormal loads, waste management' and '[detecting] theft from cash machines, preventing theft of tractors and monitoring antisocial driving'.[45]

Body scanning
Body scanning has begun to be used in civilian airports in the UK. Full body scanners fall into two main types: backscatter machines that use a low-intensity X-ray beam to construct a two-dimensional image of the body, and millimetre-wave machines, that use non-ionising radio frequency energy to detect energy radiated from the body as a means to construct a 3-dimensional image. Heralded as a means to complement or replace walk-through X-ray and physical pat-down

[44] 'Webchat with Jacqui Smith, Home Secretary', 03/08/2007, The National Archives, available at: http://webarchive.nationalarchives.gov.uk/+/http://www.number10.gov.uk/Page12804, accessed 15/06/10.
[45] The SCP working groups include representatives from the Serious Organised Crime Agency, HM Revenue and Customs, the Maritime and Fisheries Agency, and the UK Border Agency. See Paul Lewis, 'CCTV in the sky: police plan to use military-style spy drones', *The Guardian*, 23/01/10, available at: http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones, accessed 15/06/10.

searches, their advocates argue that such scanners have a far superior ability to detect threatening objects held in or about the person.

Responses amongst civil liberties advocates and information commissioners centre on the technology's alleged threats to personal and medical privacy and individual dignity, as well as possibilities of misuse. For example, in March 2010, a 'first instance harassment warning' was issued to a 25-year old male security worker at Heathrow, who made lewd comments about a co-worker who had mistakenly passed the scanner area.[46]

Border controls

More conventional data collection, as well as analysis and dissemination, is in use in the e-Borders programme, currently being implemented by the UK Border Agency (UKBA) in the Home Office. The programme's aim is to collect and analyse all passenger, service and crew data from air, sea and rail operators that provide services into or out of the UK. The programme relies on the transfer of passenger name record (PNR) and passport data collected by private sector carriers – charter carriers just have to provide passport information – to the UKBA's data warehouse between 24 hours and 30 minutes in advance of travel. There, all data are checked against watch lists, and on certain routes, travel patterns are subject to profiles or 'rules based targeting' to identify persons suspected of being involved in dangerous activities (e.g. drug smuggling). Following analysis, 'risk flags' are attached to particular names, and the border agent then decides whether to alert law enforcement agencies or immigration officers to their presence so they can take further action, which could include the individual being questioned or detained. The information is then held for 5 years in an active database and a further 5 years in an archive with stricter access controls and access on a case-by-case basis. Since 2005, according to a Home Office Minister in 2009, 137 million journeys have reportedly been logged, and 4,700 arrests made.[47]

The success of e-Borders is premised on the collection of all information relating to all journeys made into and out of the UK. It has been difficult to implement for two reasons. The first concerns infrastructural systems difficulties and costs surrounding the transfer of data from private sector carriers to UKBA, and the second concerns the ethical implications of total data collection. Whilst significant

---

[46] 'Heathrow worker warned over body scanner misuse', *BBC News*, 24/03/10, available at: http://news.bbc.co.uk/2/hi/8584484.stm, accessed 15/06/10.

[47] Charles Kelly, 'eBorders scheme is legal Border and Immigration Minister confirms', *Immigration Matters*, 19/12/09, available at: http://www.immigrationmatters.co.uk/e-borders-are-legal-eu-confirms.html, accessed 23/03/10.

industry investment has overcome the practical problem of ensuring that traveller data flow from the private sector to government, including investment upstream data capture and transfer to UKBA for advance clearance, the outcome of privacy challenges from the EU is less certain. Pending resolution of the legal issues, Eurostar and the ferry companies are still consulting with UKBA over their involvement in the programme.[48]

Workplace Monitoring

Surveillance practices are part of everyday organisational life. Computer-based employee performance monitoring, the tracking of mobile employees through GPS applications in their phones, the use of mystery shoppers and the monitoring of internet use in the workplace are common examples. Recent developments have indicated some new trends that are noteworthy. The first is an increase in the use of CCTV in the workplace. CCTV and other surveillance measures have been recently identified as the solution to fraud and dishonesty at work that costs UK businesses upwards of £2 billion per year[49]. Despite the proliferation of CCTV policies, complaints to the ICO about CCTV abuses have risen in the last year. School teachers, in particular, have found that CCTV installed to control pupil behaviour has been used to monitor their teaching performance.[50]

The mobile phone now sports a range of different applications and many support GPS mapping functions, which provide extremely useful navigational aids for their users. Others support accelerometers, which analyse the speed and direction of the movement of the mobile phone and can enable it to be used as a spirit level or in a whole new range of gaming applications. However, both these developments raise serious issues of function creep. The networked capability of mobile phones coupled with GPS, illustrating a form of geodemographics – the combination of digital mapping technologies with individual or aggregated personal data, which is discussed more extensively below – can now enable employers to track the whereabouts of their employees to within a few metres of accuracy, and the accelerometers can be used to monitor worker performance. For instance, one Japanese company has developed a management application to monitor worker performance though exploiting the accelerometer's properties as a 'mobile phone strapped to a cleaning worker's waist [that] can tell the

[48] See Kirstie Ball, Elizabeth Daniel, Sally Dibb, Maureen Meadows and Keith Spiller, 'Exploring private sector responses to government surveillance agendas', paper to be presented at 'The Political Economy of Surveillance: an international research workshop', 9 - 11 September 2010, Open University, Milton Keynes.
[49] Nicola Harrison, 'Undercover Work', *Human Resources*, October 2007, pp. 29-32.
[50] Taylor, *op cit.*

difference between actions performed such as scrubbing, sweeping, walking and even emptying a rubbish bin'.[51]

While both these new developments may be seen as providing useful management information, they represent both an intensification of surveillance and a diminution of our normal expectations of privacy. We discuss social networking under another heading below. But there is also an interesting application of networking information in the workplace setting. In 2009, the software firm SAP unveiled its 'Social Network Analyzer'. According to SAP blogger Timo Elliott, the system uses Web 2.0 and cloud computing to integrate information from LinkedIn, Facebook and other social networking sites to enable businesses to manage their internal relationships.[52] The aim of the system is to enable users to 'get to know' colleagues in different parts of the organisational hierarchy, and to understand their extended networks of contacts, based on new data flows. Although this application can have benefits in terms of managing the day-to-day detail of business meetings, its use for restructuring may imply a role for it in dismissing staff. It also creates a new layer of visibility for employees, by generating a tag cloud based on their employees' interests and networks, drawn from social networking data.

Information Processing

Information processing describes the operations that organisations perform on personal information beyond collection, practices often known as 'dataveillance', data mining, or Knowledge Discovery in Databases (KDD). In practice – as has been shown above in several examples of information collection – there is no sharp break between these phases, but the problems are somewhat distinct. We are aware that 'data processing', in the terms of data protection legislation, describes a 'cradle-to-grave' arc as far as personal information is concerned, from gathering to destruction. However, the term 'processing' is used in this report in a more limited and perhaps conventional sense to focus upon certain prominent activities in the public and private sectors, where personal information is analysed, combined, and shared. Since 2006 the stakes have been raised around data flows as the commercial and governmental sectors have sought to harness the potential of personal data, with attempts to apply a data 'silver bullet' to strategic ends in both commercial and governmental settings.

---

[51] Michael Fitzpatrick, 'Mobile that allows bosses to snoop on staff developed', *BBC News*, 10/03/2010, available at: http://news.bbc.co.uk/1/hi/8559683.stm, accessed 15/06/10.

[52] The application effectively harnesses and commodifies the personal information volunteered by employees as part of their social networking activities and brings it to bear on the relationships and opportunities they have at work.

Data combination and analysis

One of the most significant current trajectories is towards the integration of diverse forms of data. For example, whereas previously visual surveillance and dataveillance were largely separate, the increase in visual data now exceeds the capabilities of either human or conventional software analysis. The development of recognition software for visual surveillance has been advancing, but this is generally used in quite simple ways: for example, in movement recognition, which is the basis of behavioural recognition systems in CCTV. Large amounts of extant visual surveillance data are being subjected to specific kinds of recognition and context analysis to build up patterns that can then be used for predictive or anticipatory actions. Crucial here is the shift to analytics: 'intelligent' algorithms tasked with identifying 'targets' worthy of further scrutiny amidst what data analysts often term a 'tsunami' of data.

Data mining is also moving to new environments including – as predicted in 2006 – social networking and online gaming. The 2008 US Director of National Intelligence's *Data Mining Report*, for example, includes reference to 'Project Reynard', which is a seedling project to explore the emerging norms of such environments and identify deviations that might indicate suspicious activity[53], and such suggestions surfaced in publications leading up to a possible revised Telecommunications Data Bill in the UK. There have also been significant state investments in pioneering 'Web 2.0' analysis companies.[54]

ANPR and protest activities

The extension of ANPR systems has provided a major spur to dataveillance. In July, 2009 the National Policing Improvement Agency (NPIA) and ACPO issued advice to police forces entitled 'Practice Advice on the Management and Use of Automatic Number Plate Recognition', which detailed the extensive data mining potential of the new database. One example given in this Practice Advice concerned the collection, under RIPA, of images of potentially violent protesters, and loading them onto the central database.[55]

---

[53] See: http://www.fas.org/irp/dni/datamining.pdf, accessed 15/06/10.

[54] Such as the CIA's purchase of a stake in Visible Technologies Inc., a firm which specialises in monitoring new social media such as blogs, micro-blogs, forums, customer feedback sites and open social networking sites; see: Noah Shachtman, 'U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets', *Wired*, 19/10/09, available at: http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/, accessed 15/06/10.

[55] National Police Improvement Agency, *Practice Advice on the Managements and Use of Automatic Number Plate Recognition*, 2009, p. 54.

While the use of ANPR cameras to identify those who are driving without insurance or road tax, or to monitor those suspected of being involved in serious crime and disorder, may not be seen as contentious, the extent to which it is used to track, monitor, and profile 'legitimate' protesters is. For instance, the National Public Order Intelligence Unit (NPOIU) is responsible for providing intelligence on 'domestic extremists'[56] and maintains a database of individuals identified as a potential threat. How many people are registered on the database is secret, but it is estimated to run into thousands.[57] It is clear, however, that ANPR data are being used routinely to track and monitor political protestors logged on the 'domestic extremists' database, and that inclusion in the database is not confined to those who propagate violence and disorder. Merely being 'associated' with protests that have given rise to 'crime, disorder and the deployment of significant resources' appears to give the police sufficient justification to include such persons in the database and subject them to extensive tracking and repeated stops.[58] But even those attending peaceful protests have also been logged: it was reported that an IT manager with no criminal record was stopped 25 times in fewer than 3 years after a 'protest' marker was placed against his car following his attendance at a small and peaceful protest against duck and pheasant shooting.[59] This episode suggests that attendance at any political protest gathering can now leave individuals open to extensive surveillance.

Geodemographics

Since 2006, a number of new geodemographic products and systems have come onto the market. Google StreetView, one of the best known, now has almost total coverage of the United Kingdom. However, while there have been privacy concerns expressed with regard to the ability to identify individuals or vehicles in embarrassing contexts through their chance exposure at the time that the Google StreetView photographic collection vans were passing, the system is a static photographic view, not a live video feed, and most privacy concerns can been easily addressed with simple technological solutions. In May, 2010 – as with Facebook – Google responded apologetically to a wave of criticism about the

---

[56] Her Majesty's Chief Inspectorate of Constabulary, *Adapting to Protest*, London: HMIC, 2009.

[57] Ian Johnston, 'Peaceful protesters included on police database of "domestic extremists"', *The Daily Telegraph*, 26/10/09, available at: http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/6433980/Peaceful-protesters-included-on-police-database-of-domestic-extremists.html, accessed 15/06/10.

[58] Paul Lewis and Rob Evans, 'Activists repeatedly stopped and searched as police officers "mark" cars', *The Guardian*, 25/10/09, available at: http://www.guardian.co.uk/uk/2009/oct/25/surveillance-police-number-plate-recognition, accessed 15/06/10.

[59] Paul Lewis, Rob Evans and Matthew Taylor, 'Police in £9m scheme to log "domestic extremists"', *The Guardian*, 25/10/09, available at: http://www.guardian.co.uk/uk/2009/oct/25/police-domestic-extremists-database, accessed 16/07/10.

(apparently incidental) collection of personal information from wireless networks by StreetView's photographic vehicles in the UK.

Of much more concern is the new breed of social geodemographic systems, exemplified by Google Latitude. These combine GPS-enabled mobile telephones with Google Maps and social networking data. Individuals can choose to have their mobile location tracked by selected friends and to track their friends' mobiles. While this system is voluntary (opt-in) and consensual, there is the potential here for rather less consensual activities though hacking or simply by companies integrating databases of mobile telephone location data with other publicly available or purchasable data.

Geodemographics are also 'crowdsourcing',[60] but such crowdsourcing is not always done with the consent of those whose information is being sourced. For example, the locational computing project, CityWare, trialled in Bath, raised concerns for allegedly tracking people's movements without consent via Bluetooth wireless.[61] There is another small but growing trend to crowdsource the analysis of captured data and video images. Early experiments included the Shoreditch Digital Bridge project, mentioned in the 2006 report, which allowed residents of the Haberdasher's Estate in London to see live feed from the video surveillance cameras on their estate.[62] Although the experiment was ended in 2007, others have followed, most notably the Internet Eyes start-up, which operates an 'event notification system'.[63] They plan to broadcast surveillance footage from paying private business customers on the Internet, with the idea that the public will work as monitors. The public participants interact with this system as a game where 'players' gain points for spotting suspected crimes and lose points for false alarms, and monthly prizes are paid out. This particular company may or may not succeed; however, just as early examples of social networking have disappeared or failed, other more robust or different models may well achieve rather greater success. It seems likely that Open-Circuit Television in various forms will gradually replace the old Closed-Circuit model.

Welfare administration and social sorting

---

[60] Crowdsourcing describes the outsourcing of work to a wide group of people, usually via an open call or competition; see Jeff Howe, 'The Rise of Crowdsourcing', *Wired*, 14, 6, 2006, available at: http://www.wired.com/wired/archive/14.06/crowds.html, accessed 15/06/10.

[61] Paul Lewis, 'Bluetooth is watching: secret study gives Bath a flavour of Big Brother', *The Guardian*, 21/07/08, available at: http://www.guardian.co.uk/uk/2008/jul/21/civilliberties.privacy, accessed 15/06/10.

[62] Mark Ballard, 'Home snoop CCTV more popular than *Big Brother'* The Register, 11/11/07, available at: http://www.theregister.co.uk/2007/11/11/home_tv_cctv_link/, accessed 15/06/10.

[63] Internet Eyes website, available at: http://interneteyes.co.uk/, accessed 15/06/10.

The 2006 Report noted that 'social sorting increasingly defines the surveillance society' and 'affords different opportunities to different groups and often amount to subtle and often unintended ways of ordering societies, making policy without democratic debate'. A focus on risk (and 'opportunity') management underlies such social sorting and the widespread use of new technologies and their associated statistical techniques facilitates it. With the decline of shared risks within state-sponsored welfare systems, for example, risk has become increasingly an individual responsibility and the management of those risks has become an industry in itself. In order to streamline and organize such risks, private firms – such as Accenture or Experian – are engaged. They mobilise their considerable information technology and statistical skills to sort risky individuals into categories for differential treatment.

For example, UK government has been concerned with so-called 'high cost, high risk' social groups who are vulnerable to 'social exclusion.'[64] One such group is young people classified as 'NEET' (Not in Education, Employment or Training). According to one study, a NEET 17-year old is likely to cost the British taxpayer 10 times more by the time he or she is 28 than their counterparts in education, training or work, just because they may claim benefits, use health services, become involved with the criminal justice system or not pay taxes. Social intervention, even from the time of pregnancy, is required to avoid social exclusion. Thus locating, targeting, tracking and mapping the distribution of such groups is vital, as is extensive data sharing to classify more carefully and to organise the necessary surveillance. In other words, once socially-sorted, such groups – homeless people, drug users and previous offenders are viewed similarly – can expect greater and continuing scrutiny that may either exacerbate or ameliorate their situation.

Ethnic targeting

Despite some slowing in growth of air transport passenger numbers since 2005 (affecting international holidays and domestic flights), more than 150 million passengers still go through UK airports each year.[65] Scrutinising passengers without examining each individually has led airports to rely on profiling and screening. But this in turn depends on records such as the PNR that is derived

[64] See Nicholas Pleace, 'Workless people and surveillant mashups: Social policy and data-sharing in the UK' *Information, Communication and Society*, 10, 6, 2007, pp. 943-960.

[65] See, UK Parliament, 'Statistical information on air passenger numbers and characteristics Collected for the House of Lords Science and Technology Committee inquiry into the Air Cabin Environment by the Parliamentary Office of Science and Technology (POST)', 10/2000, available at: http://www.parliament.uk/post/e3.pdf, accessed 15/06/10.

from commercial data collected by the airlines from their passengers.[66] Since 9/11 considerable concern has been expressed about the ways that 'Arab' and 'Muslim' passengers are disproportionally singled out for special attention and experience more delay, not to mention affronts to their dignity, than other groups.[67]

Since 9/11, several incidents and deployments have shown how particular groups, especially those deemed 'Muslim' or 'Arab' or 'Middle Eastern,' may experience negative discrimination. In Birmingham, for example, ANPR systems are used disproportionately – 3 times more – in areas where there is a concentrated Muslim population. Introduced as an attempt to combat antisocial behaviour, vehicle crime and drug-dealing in the area, the system is actually paid for by a 'Terrorism and Related Matters Fund.'[68] Following the local and national furore over this scheme in mid-2010, not least in regard to the alleged deception and non-transparency about the aims of the system, the Birmingham scheme was discontinued and the Home Secretary declared that ANPR as a whole should be placed under statutory control.[69]

Call centres

Call centres are well known as the service sector's 'mass production areas'; however they are also custodians of consumer data. The operation of a call centre is based on accurate customer account records so that employees can identify customers before talking to them. Outsourced call centres (sub-contracted to handle calls for other companies) rely on the transfer of customer data from their clients in order to operate their businesses. These domestic and international data flows render them vulnerable to abuse through fraud, theft or employee sabotage. In October 2006, Channel 4's 'Dispatches' documentary series highlighted the customer data black market in India, prompting an investigation by the ICO. The problem is not unique. In 2007, BBC Scotland reported that one in ten Glasgow call centres had been targeted by organised criminals. The negative consequences for customers, ranging from identity theft

---

[66] See Colin J. Bennett, 'What Happens When You Book an Airline Ticket (Revisited): The Computer Assisted Passenger Profiling System and the Globalization of Personal Data', in Elia Zureik and Mark B. Salter (eds.), *Global Surveillance and Policing: Border, Security, Identity*, Cullompton: Willan, 2005, ch.8.

[67] See Nigel Morgan and Annette Pritchard, 'Security and social "sorting': traversing the surveillance-tourism dialectic', *Tourist Studies*, 5, 2, 2005, pp. 115-32.

[68] Paul Lewis 'Surveillance cameras in Birmingham track Muslims' every move' *The Guardian*, 04/06/2010, available at: http://www.guardian.co.uk/uk/2010/jun/04/surveillance-cameras-birmingham-muslims/, accessed 15/06/10.

[69] Alan Travis, '"Big brother" traffic cameras must be regulated, orders Home Secretary', *The Guardian*, 04/07/10, available at: http://www.guardian.co.uk/uk/2010/jul/04/anpr-surveillance-numberplate-recognition, accessed 15/07/10.

to unwanted phone calls, can be very damaging as, for example, in 2009 when T-Mobile employees passed on customer contacts to third parties.[70]

Data Markets
Data markets have also opened up. Organisations that seemed simple a few years ago, for example publishers, have reinvented themselves as databrokers, combining information management from academic books and journals, through media archives, to personal data collation and analysis. SAP (above) is one example; another is Reed Elsevier, which owns companies including Elsevier academic journals, LexisNexis newspaper archives, and Choicepoint data analysis, and calls itself 'a world leading provider of professional information solutions'.[71] Databrokers are a key example of the way in which processing of personal data by private organisations has intensified in recent years, yet they are barely known to the general public as holders of their personal data.

Information Dissemination
As has been shown earlier, much of data processing involves specific data disclosure, but the main emphasis of the concept of dissemination is on the broader communication or disclosure or sharing of personal information to larger numbers of organisations, individuals, or the general public. This takes place in a variety of contexts, and the concerns that arise may be different. The many – and continuing –data breaches and losses that have happened illustrate potential or actual uncontrolled dissemination through lapses in information security and in the duty of care for confidential information on individuals. Dissemination also occurs with regard to the release of information under the Freedom of Information (FOI) regime, when personal details may either be redacted or exposed depending upon the determination of the public interest. Recently, FOI requests and ICO decisions about, for instance, the expenses claimed by Members of Parliament, have highlighted the somewhat paradoxical way in which privacy issues are often engaged, and debate fostered, by the exercise of the countervailing public right to know.

Data sharing
The 2006 report identified flows of data from people to databases, and between databases, as a key process underpinning the surveillance society. Whilst many

[70] Amy Fallon, 'T-Mobile staff sold customers' details to rivals', *The Independent*, 18/11/2009, available at: http://www.independent.co.uk/life-style/gadgets-and-tech/news/tmobile-staff-sold-customers-details-to-rivals-1822232.html, accessed 15/06/10.
[71] Reed Elsevier website, available at: http://www.reed-elsevier.com/aboutus/our-business/Pages/Home.aspx, accessed 15/06/2010. See also: David Murakami Wood, 'Spies in the Information Economy: Academic Publishers and the Trade in Personal Information', *ACME*, 8, 3, 2009, pp. 484-93.

of us willingly consent to the giving of our personal information in one setting, the flow of data from that setting to another (e.g., from commerce to policing, as with Oyster Cards) requires description and comment. Data are frequently traded and transferred, and while surveillance may have adverse effects, data flows can also confer benefits and opportunities. For individuals, the sharing of personal data can cement friendship bonds, enhance leisure and career opportunities, and create greater convenience. For businesses, the gathering of more detailed customer and competitor data can create commercial opportunities. For the public sector, knowing how citizens use resources can result in the better targeting of services, and more efficient use of resources. For government, security, crime control and other policy objectives are facilitated by new data flows from private and public sector partners.

Pressures towards more extensive data sharing in the UK have mounted in the years since 2006, with renewed attempts to provide 'transformational government', including more integrated public services to individuals based on identifying them, verifying their claims to services, and collating personal information from various databases. The sharing of data – or the tragic lack of it – has featured prominently in social care and policing practice, and particularly in child-protection cases since the Bichard Report (2004). It has also been a major element in law enforcement, counter-terrorism, and in combating fraud. This has fuelled greater efforts by government to overcome real and perceived obstacles to access to data, whether legal barriers, operational practices, or organisational frictions. Clause 152 of the Coroners and Justice Bill in 2009 aimed to give Ministers wide powers to authorise data sharing through secondary legislation where they deem it necessary and proportionate, thus sweeping away all barriers. However, the clause was withdrawn by the previous Government following strong and widespread opposition. In the commercial world, the sharing of data across companies and sectors, and between the private and public sectors generally, have become increasingly normal. The state's reliance on exchanges with information-service companies such as Experian when processing individuals' applications for, for example, drivers' licences, has become a routine part of operational procedures.

Social networking

The explosion of social networking has enabled a revolution in how people, particularly younger people, communicate with family and friends. However, since 2006 the proliferation of complex modifications to the way in which the dominant social networking company, Facebook, operates significantly changed how and to whom personal data contained on a person's profile are made available. In particular, Facebook allowed information previously restricted to

those registered as a 'friend' of the user to be shared by all. As the Electronic Frontier Foundation pointed out, Facebook now treats lists of friends, names and many other personal details, as publicly available information.[72] Following public concern, including prominent NGO and regulatory-agency action in Canada, in 2009, and again in 2010, Facebook retreated from its privacy-unfriendly practices and undertook to simplify and improve its privacy settings in order to facilitate individual control and the transparency over the treatment of subscribers' personal information.

The significance of developments in the management of social networking is in the power that they give to create extended profiles of a person. For instance, by analysing the publicly available data revealed by an individual on their Facebook pages and combining it with data from their friends' pages, it is technically possible to predict political affiliations[73] or even sexual orientation.[74] In addition, commercial organisations are already developing software applications to enable businesses to integrate social network data about their employees into their corporate systems, as seen with SAP, above.

5 - Implications, Issues and Problems

This discussion now turns from the description of examples to highlight a number of important issues to which they give rise: issues that represent challenges to society generally, to the individuals whose personal information is involved, to regulatory policy-makers, and to regulatory practice based on legal rules and principles.

Privacy, ethics and human rights

Privacy remains a key concern, whether to do with the collection, use and misuse of databases or with other domains of surveillance. This report cannot discuss the myriad and well-known ways in which surveillance practices impact upon privacy and human rights, but a few relatively novel developments can be highlighted. Recent experiences with body scanning have highlighted the importance of bodily privacy in public places. A number of privacy-enhancing solutions to this problem

[72] Kevin Bankston, 'Commentary: Facebook's New Privacy Changes: The Good, The Bad, and The Ugly', Electronic Frontier Foundation, 09/12/09, available at: http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly, accessed 15/06/10.

[73] Jack Lindamood, Raymond Heatherly, Murat Kantarcioglu and Bhavani Thuraisingham, 'Inferring private information using social network data', *Proceedings of the 18th International Conference on World Wide Web*, Madrid, 2009, pp.1145-6.

[74] Carolyn Y. Johnson, 'Project Gaydar', *Boston Globe*, 20/09/09, available at: http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/?page=full, accessed 15/06/10.

have been mooted in Canada: developing algorithms which act as 'privacy filters', reducing or eliminating all personal detail from faces and genital areas; strict prohibition of retention and distribution of imagery; a ban on staff bringing photographic devices into the scanning area; a physical removal of scan monitoring to closed rooms and access to personal identification of the passenger throughput; and detailed audits to ensure compliance with these regulations.

Video analytics are also a case in point. The limited protections and rights for those captured by video surveillance become even less relevant once the secondary data generated through analytics allows the reconstruction of patterns of movement, possible place of residence, favourite locations and so on. A major concern is the use of analytics software to scan a scene automatically, identifying patterns and presences which are deemed 'abnormal' within a normative definition of what occurs 'normally' at that time and place within a city. Analytics systems in general facilitate new combinations of data about a subject that, after analysis, create a more fine-grained picture and expose the subject in new ways, raising privacy concerns.

The privacy problems associated with drones are worth mentioning here: specifically, they relate to the extent to which those present 'in public' can claim any kind of right to privacy. Drones also present a more pervasive form of surveillance than CCTV because of their mobility. They raise significant problems in terms of consent and notice, as they are barely visible from the ground, and yet have the potential to track and film people in real time. Issues around proportionality arise when they are following a 'target'.

Flows of data into new domains of application, particularly those that attempt to create total or mandatory visibility of the person, also raise significant concerns. Perhaps the most prominent of these discussed in this report is the question of whether the e-Borders programme challenges freedom of movement within the EU, and is compatible with the national data protection laws of other Member States.[75] Notwithstanding the recent change of Government, commitment to a project that stipulates the mandatory collection and retention of detailed personal information from each traveller was always going to raise privacy and other concerns about the legality, necessity and proportionality of the scheme.

---

[75] House of Commons, Home Affairs Committee, *UK Border Agency: Follow-up on Asylum Cases and E-Borders Programme*, Twelfth Report of Session 2009-10, HC 406.

However, as noted in the 2006 Report, there are social and ethical values other than privacy that are also challenged or damaged by surveillance. Here, the threat to trust must be emphasised, and it is important to continue to underline the way in which 'social sorting' contributes to the drawing of social distinctions. People are sorted into categories (including gender, socio-economic, religious and ethnic/national) in order to distribute opportunities and risks according to some institutional criteria. The effects are often subtle and complex but with everyday consequences for work, travel, consumption and relations with official bodies. As the examples show, the distinctions are often reinforced in the process as well.[76]

It is import to recall, in the words of the 2006 Report, that '[n]o one has voted for such systems. They come about through processes of joined-up government, utility and services outsourcing, pressure from technology corporations and the ascendancy of actuarial practices.' Social sorting is nowhere an official, legislated process. It is one in which statistical categories determine differential treatment for different population groups, directly affecting their life-chances and opportunities. But while it clearly affects social ethics and justice it is not in any sense subject to democratic participation.

The sharing of data sits uneasily alongside concerns about confidentiality, particularly of 'sensitive' data of the kind typically used in personal public services. It also complicates the question of consent to the secondary use of personal data for purposes not clearly related to those envisaged at the time of collection, and cuts across what many people expect or believe happens to their data. Lack of transparency and control are important issues, as people may feel powerless to prevent the processing and sharing of their information by organisations on which they are dependent for important benefits and services.

Finally, the international flow of consumer data to non-EU jurisdictions raises data protection issues. Currently non-EU call centres are required to build data protection principles into service contracts, leaving data protection practices vulnerable to the stresses and strains of call-centre life. Recent call-centre data protection scandals in non-EU countries highlight this as a continuing concern.

'Function creep'

The 2006 Report identified a process of 'function creep' that was noticeable in surveillance. Function creep occurs when a technology introduced for one purpose is then used to fulfil other purposes. Function creep is not an inherently

[76] See Oscar Gandy, *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*, London: Ashgate, 2010.

negative concept, for much beneficial innovation rests on finding new uses for existing applications and technologies. However, in the context of data protection and privacy considerations, if personal data – collected and used for one purpose – migrates to other ones, then surveillance can become intensified and privacy rights breached beyond what was originally understood and considered socially, ethically and legally acceptable. The previous discussion of cameras in pubs and schools, the police use of unmanned drones, mobile phone technology, social networking, and APNR – for example, its use by car-park operators – has illustrated the process in various domains.

Clearly in the case of TfL, the ANPR cameras were installed for the purpose of enabling and enforcing the central London Congestion Charge scheme, but the data are now shared with the police for national intelligence purposes. This is arguably legitimate and beneficial, and has independent oversight because the ICO will receive an annual report from the Commissioner of the Metropolitan Police on the operation of this data-sharing agreement. So, too, would be the use of ANPR in the case of violent protest. However, the logging of political protestors lawfully exercising their right to protest peacefully is arguably less legitimate. A second egregious example is the changes made by Facebook to its privacy settings, as a technology sold to its users as a means to communicate with family, friends and acquaintances now allows that information to be lifted out of context, merged, and reanalysed in contexts that were never imagined or consented to by the owners of the data. Third, the use of UAVs for policing demonstrates another form of function creep: the migration to domestic policing of a technology developed to track the location and movements of the enemy in war. In the context of war, consent, privacy, and data protection may be little considered, but in the context of the mundane policing of citizens, such considerations should not be so easily abandoned.

As systems are designed with interoperability in mind, new products, and new surveillance possibilities, can emerge as older technologies come together to create functions. Once established, systems can easily be 'locked in', while business processes are developed on the assumption that function creep is a benefit without drawbacks. Function creep often happens unobtrusively: for instance, data-mining to profile consumers in an attempt to target marketing more effectively. Its rationale is sustained by considerations of economy, efficiency, effectiveness and convenience in the exploitation of information resources, whether technologies or databases, as assets within the organisation. On the other hand, function creep often stretches fair information principles towards their limits.

Invasions of privacy may be justified in certain cases when compared with the benefits resulting from function creep. This may be particularly so where the nature of the invasion does not violate what people have come to accept as a reasonable expectation of privacy. However, surveillance devices, developed for military, anti-fraud, or revenue purposes may migrate to applications affecting larger numbers or new categories of the civilian population. The use of these tools often connote suspicion of wrongdoing requiring monitoring, and may step over the boundary of what is tolerable in a society that upholds human rights and in which ethical norms shape the approach to privacy protection. The further uses of UAVs, police databases and mobile phone technology particularly raise these concerns, and may be detrimental to the climate of trust that is necessary for social and citizen-state relationships. Function creep facilitates the erosion of these values and rights, even where the intention is benign.

Transparency and accountability
As can be seen in the cases of social networking and CCTV in schools, when there is migration from the original purpose or functionality, it is normally difficult for members of the public, policy-makers and regulators to keep track and to fix responsibility on those who were originally identified as controllers or custodians. This is, in part, because function creep is incremental and does not necessarily create a clearly new system or use that would give rise to such questions, or to a subsequent reconsideration of the grounds on which the original function was deemed to be acceptable, necessary or proportionate. Given the relatively low level of public and political understanding of technologies such as databases, it is too easy for functions to creep surreptitiously without exposure to widespread comment, debate, or procedures for deciding on the acceptability and accountability of the new functions or uses.

The flow of data between databases is a normal aspect of everyday personal, commercial and governmental life. Databases and the data that flow between them are key elements of infrastructure, and hence their effects only become apparent when those infrastructures fail, as recent losses of government data illustrate. Rendering these everyday systems accountable and transparent is particularly difficult in commercial operations where the ownership of personal data – such as customer account details – is the basis of competitive advantage. Law-enforcement bodies would also argue that making ANPR and other data flows transparent would undermine their efforts to fight crime. However, in the case of deliberate commercial and governmental attempts to harness data to strategic ends, it may be possible to identify aspects that represent intensified surveillance, and that should attract regulation. The use of personal social networking data to inform business decisions is a key example. Privacy Impact

Assessment (PIA), expanded to highlight non-privacy impacts, could identify problems with the use of data from an employee's non-work life in the workplace. In the realm of law enforcement, FOI requests have been used to great effect to reveal data flows around ANPR; however their piecemeal nature undermines the introduction of more sustained reporting requirements on data use and analysis by the police.

In the case of new uses for data, especially disclosures or sharing of data, issues of consent and control can be more difficult to address if there is a lack of transparency and weak systems of accountability. These points are revisited later, when the regulatory implications of function creep as well as other processes are considered.

Blurring of the public and the private, and unintended consequences
Controversies surrounding the movement of data across public/private boundaries either at a personal or an organisational level are illustrated by the examples included in this report. For example, worker responses to body scanning highlight the sometimes irresistible urge of voyeuristic opportunism when the private and taboo (i.e., nudity) is made public. The same danger applies when managers are able to peer into the Facebook and LinkedIn pages of their employees. Both examples also represent unintended consequences. Wider experiences of air carriers involved in the e-Borders programme have highlighted the huge investments needed to transfer data from a large number of private organisations, originating in different formats and in different parts of the world, to one central point in the public sector. Once again, the use of ANPR and DVLA data provides other illustrations of the blurring of boundaries between the state and the private sector with regard to personal data flows.

Finally, with data analysis, the ownership of multiple data sources creates enormous economic value, and economic actors may be tempted to overstep the mark in data analysis and their subsequent commercial strategies. Data flows are notoriously opaque and hence difficult to render accountable and transparent. Their start and end points are difficult to define, as are the paths that they take, which often lie deep in the proprietary systems of private actors or public-sector agencies. And finally, the longer and more complex the flow, the more likely that there will be unintended consequences for data subjects, even in the most legal and transparent examples.

6 - Regulatory Developments and Problems

The challenges posed to regulation

As the previous section of this report has shown, there is a formidable array of continuing and new surveillance challenges to protecting information privacy and other individual and social values, including autonomy, dignity, and equality. These challenges have been met with some important recent countervailing action, in which the ICO has played a leading part. However, there are constraints on the activity that any regulator can take within a framework of legal controls. This is because the governance of CCTV, ANPR, the forensic use of DNA, and other surveillance and data collection practices takes place in an under-regulated environment, leaving the individual or social group without a statutory basis for granting consent, discovering what is happening, or obtaining remedy. Only in certain circumstances does much surveillance fall within the purview of general laws such as the Data Protection Act (DPA) 1998 and the Regulation of Investigatory Powers Act (RIPA) 2000, which permit wide exemptions from all or part of their provisions.

Much of the preventative and remedial activity, as well as efforts to warn about threats to privacy and liberties, has taken place through the opportunities provided by the occurrence of scandals, 'security storms' and 'horror stories' of one kind or other. These have included the loss of massive amounts of personal data through carelessness and confusion, poor organisational practice, and weakness in information security across public as well as private-sector organisations.[77] They have also involved the often organised, large-scale and illegal buying and selling of personal information held within public and other bodies.[78] Government's plans to keep details of the internet and telephone communications of the entire population, as well as the continued development of centralised public-sector databases, including the promotion of extensive data sharing and profiling, have continued apace during these years, with some changes and occasional reversals. These are only some of the issues that have fashioned the agenda for regulation.

Regulatory responses

Parliamentary and governmental reports, and those of outside NGOs and think tanks, have contributed strongly to resisting and limiting the adverse effects of

---

[77] See, for example, Kieran Poynter, *Review of Information Security at HM Revenue and Customs: Final Report*, 2008; Cabinet Office, *Data Handling Procedures in Government: Final Report*, 2008; Sir Edmund Burton, *Report into the Loss of MOD Personal Data: Final Report*, Ministry of Defence, 2008.

[78] ICO, *What Price Privacy Now?*, ICO, 2006.

surveillance and poor data handling and management. They have urged more effective rules and guidelines for information practices that, if left to themselves, would only aggravate the problems individuals and groups face regarding the collection, processing and disclosure of their information. These reports have highlighted many of the issues that the *Report on the Surveillance Society* brought into public debate in 2006, and that itself inspired some of the parliamentary and group investigations in the years since. The House of Lords Constitution Committee Report, for example, pointed to surveillance's 'powerful influence over the relationship between individuals and the state, and between individuals themselves', thus signifying the importance of surveillance to the very life of our society, going beyond its effect on individual privacy rights and the question of data protection as such.[79]

Following the discovery of massive data breaches by Her Majesty's Revenue and Customs, amongst other departments and agencies, government itself responded by tightening up its approach to data handling. In 2008, it promoted new security, management, and training regimes, and specific techniques including a better understanding of information risk, across the public sector in order to improve the culture and accountability for the public's personal data.[80] How far these have actually taken root, and how uniformly, is not easy to determine, although a recent review describes important progress[81]. The impact of the new Government cannot yet be determined.

However, the lessons learnt from data breaches will more likely be those concerning data *security*, rather than of the wider range of privacy and surveillance issues, such as excessive data collection and disproportionate analysis and sharing of data. If that is so, many facets of surveillance and privacy invasion will not be subject to sufficient regulatory renewal unless attention is deliberately focused on them through parliamentary, governmental, and non-governmental routes. The Thomas-Walport Review[82] went some way towards casting light on the question of data sharing and towards putting it on a more privacy-friendly footing, partly by clarifying the nature of the judgments and decisions required when considering the sharing of data. A number of its recommendations were in line with the new governmental approach to data handling, and emphasised the importance of transparency, accountability, and audit, plus vigorous action by regulatory officials to keep these cultural changes

[79] House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the State*, HL Paper 18-I, para. 3.
[80] Cabinet Office, *Data Handling Procedures in Government: Final Report*, 2008.
[81] Cabinet Office, *Protecting Information in Government*, 2010.
[82] Richard Thomas and Mark Walport (2008) *Data Sharing Review Report*, Ministry of Justice, 2008.

in motion.

It is encouraging that practical recommendations for better instruments and safeguards to be deployed by official regulators have been made in several reports in recent years, increasing the likelihood of stronger regulation that addresses surveillance issues beyond data security. The ICO has championed the development of instruments that, if implemented on a significant scale, might help to keep surveillance in check and mitigate or prevent the misuse of personal data. For example, PIA has been actively encouraged and a framework for its use has been produced and further revised.[83] PIAs could play an important part in mitigating function creep and, if published, help improve transparency. A new Code of Practice for CCTV was adopted in 2008.[84] It, too, will assist in the assessment of impact not only on privacy but on other values that people cherish, in reinforcing purpose-specificity, and in promoting transparency and accountability for CCTV systems. The Government has promised further regulation in this area, but without detail at the time of writing.

A new statutory Code of Practice for Data Sharing – an outcome of the Thomas-Walport Review – is nearing completion, potentially clarifying the validity and limits of data sharing and providing a better basis for making decisions about when to share data, with whom, and why. Reflecting international initiatives, Privacy by Design (PbD)[85] has been recognised, encouraging information technologists to build privacy protection into their systems architecture and specific products from the start.

All these initiatives can be seen as part of a strong regulatory package, but how far they will – or can – be implemented in practice by normally reluctant companies and public agencies will determine their value. Sceptics will say that there are few examples, anywhere, of effective and non-perfunctory PIAs that actually modify the plans or practices of organisations. Codes of Practice can often become symbolic tokens rather than having truly implementable regulatory force. The value of PbD, which so far has more champions than practitioners, is as yet unproven: the business case for its precursor, Privacy-Enhancing Technologies (PETs), has not caught on to the extent that supporters envisaged.

---

[83] ICO, *Privacy Impact Assessment Handbook Version 2.0*, 06/2009, available at: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html, accessed 09/06/10

[84] ICO, *CCTV Code of Practice, Revised Edition 2008*, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf, accessed 09/06/10.

[85] ICO, *Privacy by Design*, 2008, available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf, accessed 09/06/10

However, these regulatory initiatives are advantageously grounded in the law and in the principles and values of privacy and human rights underpinning the law, and do not offer easy options to avoid, displace, or circumvent these. The values and principles that provide the basis for Codes, assessment tools, and technical design are the very ones that are already well-known in data protection and human rights law, usually invoked by those who press for a limitation of the adverse effects of surveillance. Therefore, their proper implementation is likely to represent a significant effort in limiting surveillance.

Regulation in future

Regulatory efforts in the UK have not been best served by existing data protection and privacy law: the former is relatively weak in its domestic transposition of the European Union Data Protection Directive 95/46/EC[86], and – in any comprehensive and focused sense – privacy law is largely absent, although the right to privacy is explicitly and frequently mentioned in the Directive that our Data Protection Act was intended to transpose. These restrictions have set outer limits to what can be expected of a regulatory regime that might safeguard individuals and society from the excesses of surveillance, although it is a promising sign that change in the law and its articulation with human rights legislation, and reform of the Directive, are still on the agenda.

In particular, how the collection of data can be minimised or stopped will remain an important question. It will require sustained debate about what would constitute legitimate and acceptable purposes, and desirable limits. Clarity about this has been to some extent assisted by the raising of public and parliamentary awareness of surveillance in recent years, but continuous efforts by official regulators such as the ICO and other Commissioners will be required to reinforce and extend the platform that has begun to be put in place.

Surveillance cannot be effectively constrained without a more rigorous regime of law, supervision and enforcement. The enactment of positive legislation to create or to reform the regulation of surveillance activities where it is absent or deficient must play an important part in the near future. Regulation would be assisted by reform of the legal framework – perhaps tightening the link with human rights including the right to privacy – and of the powers available to regulators, whether generally or with respect to specific or sectoral surveillance activities.

---

[86] See the European Commission's 'reasoned opinion' of 24 June 2010 on UK compliance with the Directive, in 'Data protection: Commission requests UK to strengthen powers of national data protection authority, as required by EU law', available at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/811, accessed 12/07/10.

The promised repeal of some of the statutory or administrative basis for surveillance will be an important step: for instance the repeal of the Identity Cards Act 2006 and the destruction of the NIR, the reappraisal of ContactPoint, and the cancellation of the next generation of biometric passports. The prospect of further legislative dismantling of parts of the 'database state' and the reform of human rights legislation cannot yet be evaluated in terms of their implications for surveillance itself or for the ability of regulators to enforce other laws, such as the DPA, more effectively. It would be important for any such dismantling to be investigated – by Parliament, but not exclusively – in terms of whether it actually amounts to a net increase in privacy protection and a diminution of surveillance, or instead merely to a reorganisation of current functions – such as systems of identification and authentication – without essential reform of the scope and intensity of surveillance.

Given the powerful commercial, governmental, and popular forces that brought about an intensification of surveillance in the first place, there may be considerable resistance to giving up the right, or the felt need, to hold so much information on citizens and consumers, to share it with other agencies, and to analyse it to yield new and potentially valuable information. There is also likely to be resistance to reining in the proliferation of video surveillance, to curbing the excesses of DNA collection, and to modifying information systems that relate to the safety of vulnerable persons. 'Knee-jerk' reactions to tragic incidents are likely to continue to be favoured. In these contexts, governmental self-restraint and careful scrutiny by Parliament, regulators, NGOs, the media, and the wider public would seem to be essential.

Significant recent changes that are expected to strengthen regulation are the increase in the ICO's budget through a new system of fees for data controllers' notifications, the new power to impose large financial penalties for reckless and wilful breach of the data protection principles, and the enactment of new inspection and assessment powers for the ICO. Unfortunately, the failure to extend the latter to the supervision of the public sector outside central government, or, in particular, to the private sector, is out of keeping with the need to regulate more effectively the privacy implications of the state's increasing involvement of the private sector in the provision of information services for public-sector activities. It also leaves unstrengthened the ability to regulate the private sector's extensive and intensive surveillance and data collection activities as such, some of which have adverse social-sorting and discriminatory effects in the commercial world.

Including some of these changes mentioned above, the House of Lords 2009 Report also made many recommendations for improving not only the legal framework but also the ancillary and supportive mechanisms that might make regulation work more effectively. These would include roles for civil-society organisations and the general public. The ICO welcomed most of the recommendations,[87] some of which were already said to be in train, although relatively few of them have yet to be fully adopted by Government and others have been resisted. This report is not the place to review these possibilities at any length, but a few of them can be commented on as of particular importance in denoting some areas that Parliament and Government may consider unfinished business.

First, the inspection regimes of the Chief Surveillance Commissioner and the Interception of Communications Commissioner, who have RIPA responsibilities, would benefit from greater flexibility so that they can promptly investigate cases of alleged disproportionate or unnecessary use of RIPA. Moreover, a more coherent relationship between the Commissioners who act under RIPA, and with the ICO, would help to increase public confidence in the regulation of surveillance. Second, in view of their apparently excessive and perhaps arbitrary use of surveillance powers under RIPA, consideration should be given whether local authorities, rather than the police, are the appropriate bodies to exercise such powers. If they are found to be the appropriate bodies, such powers should only be available for the investigation of serious criminal offences, and in any case should only be exercised where strictly necessary, and in an appropriate and proportionate way. Third, a system of judicial oversight for surveillance carried out by public authorities would be a major improvement, along with individuals who have been made the subject of surveillance being informed of that surveillance, when completed, where no investigation might be prejudiced as a result. Compensation for persons subject to unlawful surveillance by the police, intelligence services, or other public bodies would help in inducing a further measure of self-restraint.

Finally, regulation and the limitation of surveillance can only go so far within the confines of one country, applying that country's legal and regulatory powers and resources. As with money, information collected by surveillance practices and instruments flows across national boundaries in a variety of contexts: counter-

[87] ICO, 'Information Commissioner's response to The House of Lords Select Committee on the Constitution Inquiry into "Surveillance: Citizens and the State"', 2009, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_response_to_hol_constitution_committee.pdf, accessed 09/06/10.

terrorist activities, law enforcement, international commerce – online and otherwise – and public services. The problems of regulation, as well as the opportunities, are already being realised at European and wider international levels.[88] UK government as well as ICO participate in these processes of deliberation and of forming more effective and collaborative responses to the challenges of surveillance and privacy threats. These transnational efforts must continue to play an important part in protecting the privacy interests and rights of UK citizens and residents.

7 - Conclusion

Since 2006, there has been something like the kind of public, media and policy debate for which the *Report on the Surveillance Society* had called. Surveillance became an electoral issue, and has been one of the first things addressed by the incoming Government. Yet, despite responding to concerns over ID cards, CCTV, the DNA database and ContactPoint, in particular, there are still many areas where surveillance continues to intensify and expand. Some technologies have gone from being a subject of speculation to being in mainstream use in many different areas. The national roll-out of ANPR highlights the expansion of video surveillance and analysis, and the linking or sharing of data from different databases continues. Private-sector data-gathering, analysis and sharing, particularly through online social networking tools, has increased exponentially. In the immediate future, the growth of crowdsourcing and a movement to 'open circuits' will add new dimensions, as will the increasing involvement of the EU in surveillance and security issues. In the longer run, the advent of 'ubiquitous computing' in daily life and work, with the deployment of myriad sensing devices and analytical tools to predict human behaviour and to provide services or controls, will further challenge the regulatory repertory and assumptions that we have known for many years up to the present. A report such as the present one, conducted four years from now, may have to take these developments into account, as the 2016 scenarios projected in the 2006 report had done.

Whether the trajectory of regulation through various instruments, including the law, technical means, and self-regulation – and the critical awareness and vigilance of public opinion – has matched the continued development of surveillance since 2006 is not certain. Some significant steps have been taken to increase the powers available in the regulatory system, and there are encouraging efforts in the public sector and sometimes in the private sector to

[88] Charles D. Raab, 'Information Privacy: Networks of Regulation at the Subglobal Level', *Global Policy*, 1,3, 2010 forthcoming.

change the culture of organisations involved in personal information practices. Testing the plans for surveillance systems against the rigorous criteria that might be available through PIAs and other assessment methodologies that could be adapted to evaluate impacts on other, non-privacy, outcomes of these systems, and increasing the pressure on technology designers and users to embed privacy-friendly mechanisms into their products and systems, can play an important part, but only if these requirements become the norm and not the exception.

It will remain an important question, however, whether the current legal instruments, at UK and European levels, including specific data protection legislation as well as broader human rights law, are robust enough to limit surveillance and curb the excesses of data collection, or whether legal reform and better integration of legal and other regulatory instruments will be the linchpin upon which much else depends.