House of Commons
Home Affairs Committee

Information Commissioner's Annual Report to the House of Commons pursuant to the Home Affairs Committee's report 'A Surveillance Society', Fifth Report of Session 2007–08

Fourth Special Report of Session 2010–11

Ordered by the House of Commons
to be printed 21 December 2010

HC 702
Published on 1 March 2011
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

The Home Affairs Committee

The Home Affairs Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Home Office and its associated public bodies.

Current membership

Rt Hon Keith Vaz MP (*Labour, Leicester East*) (Chair)
Nicola Blackwood MP (*Conservative, Oxford West and Abingdon*)
Mr Aidan Burley MP (*Conservative, Cannock Chase*)
James Clappison MP (*Conservative, Hertsmere*)
Michael Ellis MP (*Conservative, Northampton North*)
Lorraine Fullbrook MP (*Conservative, South Ribble*)
Dr Julian Huppert MP (*Liberal Democrat, Cambridge*)
Steve McCabe MP (*Labour, Birmingham Selly Oak*)
Rt Hon Alun Michael MP (*Labour & Co-operative, Cardiff South and Penarth*)
Bridget Phillipson MP (*Labour, Houghton and Sunderland South*)
Mark Reckless MP (*Conservative, Rochester and Strood*)
Mr David Winnick MP (*Labour, Walsall North*)

The following member was also a member of the committee during the parliament.

Mr Aidan Burley MP (*Conservative, Cannock Chase*)
Mary Macleod MP (*Conservative, Brentford and Isleworth*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the Internet via www.parliament.uk.

Publication

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the Internet at www.parliament.uk/homeaffairscom.

Committee staff

The current staff of the Committee are Elizabeth Flood (Clerk), Joanna Dodd (Second Clerk), Sarah Petit (Committee Specialist), Eleanor Scarnell (Inquiry Manager), Darren Hackett (Senior Committee Assistant), Sheryl Dinsdale (Committee Assistant), Victoria Butt (Committee Assistant) and Alex Paterson (Select Committee Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Home Affairs Committee, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general enquiries is 020 7219 3276; the Committee's email address is homeaffcom@parliament.uk

Report

In its report on *A Surveillance Society?*, our predecessor committee recommended, amongst other things, that the Information Commissioner publish an annual report to Parliament on surveillance.[1] The first such report from the Information Commissioner is appended to this report.

[1] Fifth Report of Session 2007–08, HC 58-I, paragraph 36

Information Commissioner's Report

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

Introduction

The Home Affairs Committee in its report on its inquiry entitled "A Surveillance Society?" (HC 58-I) 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.

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.

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 less 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.

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

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.

Background

In 2006, the *Report on the Surveillance Society*,[2] 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.

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

2 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.

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.

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.[3]

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.

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.[4] 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.

3 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 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.

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 making public services more efficient and effective.[5] 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.[6] 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[7]—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[8] 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.[9] 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 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

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

6 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.

7 Cabinet Office, Transformational Government – Enabled by Technology (Cm 6683), London: The Stationery Office, 2005.

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

9 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.

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.[10] 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 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'.[11] 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

10 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.

11 HM Government: The Coalition: Our Programme for Government, 05/2010, p. 20, available at: http://programmeforgovernment.hmg.gov.uk/, Accessed 15/06/10.