NINE PRINCIPLES FOR ASSESSING WHETHER PRIVACY IS PROTECTED IN A SURVEILLANCE SOCIETY.

An analysis from AMBERHAWK TRAINING LIMITED
April 2012

NINE PRINCIPLES FOR ASSESSING WHETHER PRIVACY IS PROTECTED IN A SURVEILLANCE SOCIETY.

Dr. C. N. M. Pounder

chris.pounder@amberhawk.com

The original publication was published in "Identity in the Information Society" and is available at

www.springerlink.com

Synopsis

This paper uses the term "surveillance" in its widest sense to include data sharing and the revealing of identity information in the absence of consent of the individual concerned. It argues that the current debate about the nature of a "surveillance society" needs a new structural framework that allows the benefits of surveillance and the risks to individual privacy to be properly balanced.

To this end, the first part of this article sets out the reasons why reliance on the current framework of data protection or human rights legislation, or on the current regulatory regime does not necessarily protect privacy. The second part sets out nine principles that can be used to assess whether individual privacy is comprehensively considered when surveillance policy is developed. These principles are applied to surveillance in the UK to identify the structural improvements that could create an effective balance.

These principles are not legislative proposals but provide a means of exploring possible deficiencies in information law governance and, in particular, Parliament's role in scrutinising the executive and the powers needed by a regulator when engaging with the Parliamentary process. As most European countries adopt a democratic, human rights framework, it is suggested that these principles are not limited in an application in the UK environment.

The views expressed in this article are the author's own.

Key words: "Privacy policy": "Surveillance": "Supervisory Principles": "Article 8": "Human rights": "Data Protection"

PART I: WHY THE CURRENT FRAMEWORK OF PRIVACY PROTECTION IN THE UK IS DEFICIENT

Links between the three laws that apply to a surveillance activity

In a European democracy, most surveillance has to be authorised by law – whether that surveillance relates to contagious diseases or countering the threat of terrorism. If surveillance relates to identifiable individuals, Article 8 of the Human Rights Act becomes engaged and this requires specific legislation to be enacted in order to ensure the lawfulness of any surveillance that interferes with private and family life.

Usually, the surveillance legislation contains its own mechanism for individual protection (e.g. the conditions needed for authorisation of a surveillance activity), and often this legislation identifies a regulator whose role is to ensure that the rules that relate to a surveillance activity are followed. In addition, if personal data are captured as a result of a surveillance activity, data protection legislation becomes engaged, subject to any exemption.

It can be seen that the protective mechanisms that apply to surveillance can be spread over a minimum of three separate pieces of legislation – data protection, human rights and the surveillance legislation – each mechanism having its own characteristics. Thus in cases where surveillance has been unnecessarily invasive, individuals could face a confused picture of three possibly divergent routes of redress.

It is important to note that when surveillance legislation is enacted, the Minister accountable to Parliament for the public authority that undertakes the surveillance will usually be the Minister who guides the legislation through Parliament. So, for example, the Home Secretary will deal with surveillance associated with policing and the Security Service, whilst the Secretary of State for Health will deal with health surveillance. Thus it is the Minister who is politically accountable for the surveillance policy (and for the bodies that undertake the surveillance) who effectively establishes the privacy constraints that apply to that surveillance. Often this surveillance legislation will define the powers or role of an independent regulator and dictate how and to whom the regulator reports (often to the Minister concerned with surveillance policy[1]).

[1] *For example the Commissioner established by the ID Card Act 2006 and the Commissioners involved with scruitinising national security report to the Home Secretary.*

It is argued that this approach to accountability results in a weak regulatory framework where the regulator reports to the Minister who has a political interest in the outcome of the surveillance. There is a therefore a heightened risk that privacy can easily become subservient to policy objectives that depend on an extension of surveillance.

When a public authority considers interference with the "right to respect for his private and family life, his home and his correspondence"[2], Article 8(2) states that this interference has to be "in accordance with the law" and "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

This means that any interference by a public authority must pass three legal tests:

- Is the processing of personal data in accordance with a law that has been enacted within a democratic framework?
- Is the law pursuant to one or more of the interests of the legitimate objectives identified in Article 8(2) (e.g. "national security", "public safety")?
- Is that law "necessary in a democratic society" in relation to meeting a pressing and identifiable social need?

Note that the these legal tests mainly apply to question "**whether** the processing can lawfully occur?" and this question is one that should normally be considered when legislation is scrutinised by Parliament. By contrast, the main focus of the data protection principles[3] relate to **how** personal data are to be processed in the context of procedures that concern retention, fairness, relevance, security or accuracy[4] etc.. It is argued that the focus on the **how** (rather than the **whether)** which suggests that data protection principles can provide a means for assessing human rights concepts such as "proportionality" or "necessary in a democratic society".

[2] *Article 8(1) of the European Convention of Human Rights.*

[3] *As found in national legislation based on Council of Europe Convention No 108, Directive 95/46/EC or OECD guidelines (e.g. the UK's Data Protection Act 1998).*

[4] *Schedule 1 of the Data Protection Act 1998 and Articles 7, 10,11,16, 17,25 and 26 of Directive 95/46/EC list all the data protection principles.*

For example, the House of Lords has concluded that concept of "proportionality" means that any interference with private and family life does not have to be greater than that required to meet the legitimate objective which the state seeks to achieve (*R v Shayler)* (i.e. the state should not undertake excessive surveillance. However, if personal data were to be captured by such surveillance in the UK, the Third Data Protection Principle would be engaged ("Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed"). It follows that the Third (and other Principles, if relevant) can be used in a determination of whether any processing of personal data or surveillance activity is "proportionate" in terms of Article 8.

Similarly the European Court of Human Rights has considered the meaning of the term "necessary in a democratic society" and has determined that "the adjective 'necessary' is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'"(*Silver v UK*). However, the First Principle of the UK's Data Protection Act requires a public authority to process personal data on specific grounds that are qualified by the word "necessary" (e.g. "the processing is necessary ….. for the exercise of any functions conferred on any person by or under any enactment"). This linkage also suggests that surveillance that is "unnecessary" can breach the First Data Protection Principle, if personal data are processed.

One purpose of the Independent Supervision Principle (as described in Part II of this paper) is to make explicit, the links between data protection law and concepts such as "necessary" and "proportionality".

The inevitability of function creep

Once expensive surveillance technology is installed, it has to be expected that the purpose of a system will broaden. The joint CCTV/ANPR system, for instance, was first introduced in London to create a "Ring of Steel" in order to counter the threat of IRA terrorism. Now such systems are commonly used for other aspects of policing[5] (e.g. non payment of licence fee; identifying uninsured cars) as well as intelligence purposes (e.g. by alerting a control room if cameras detect a vehicle that has been placed on a watch list). Transport for London's Congestion Charge system

[5] *The use of ANPR is explained on http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR_10,000_Arrests.pdf?view=Binary.*

uses this technology to charge, bill or fine owners of vehicles who drive into central London, whilst data from these cameras are to be captured by the national security agencies[6].

Public policy in the UK has developed mechanisms to make more certain the means of identifying individuals, and this increases the potential for surveillance and for the creation of linkages between diverse databases. The Identity Card project, for example, has incorporated the Citizen Information Project (CIP) so that the National Identity Register (NIR) can be used to co-ordinate the sharing of commonly held personal data (e.g. name, address) between most public authorities (*CIP:2005*). The intention also is that the NIR's audit trail will record transactional data that will build a picture of every event where and when the ID Card is checked against the NIR (e.g. the opening of a bank-account, hiring a car, or first visit to an outpatient's department).

It should be added that the Information Commissioner has questioned the need to retain this transaction data as part of the NIR (*Constitution Committee: 2007*). The Principles identified in Part II empower the Commissioner beyond the posing of questions.

Identity management will encourage linkages between databases and mass data retention will also facilitate the emergence of new data mining techniques, mainly because it is known that the personal data are retained. For example:

- familial techniques can use the DNA data of known criminals on the UK's National DNA database to identify other family members that do not have a criminal record; in this way, a DNA database of criminals could eventually span most of the UK population (*Pounder: 2006*);

- the Serious Crime Act 2007 authorised the Audit Commission to extend its data matching techniques from benefit fraud to debt recovery[7], possibly to include private sector databases;

- Ministers have been given powers to disclose patient registration information from the NHS Summary Care Record to the newly formed Statistics Board[8] for its purposes; and

[6] *Certificate of the Home Secretary signed under Section 28 of the DPA, by Jacqui Smith MP, in July 2007.*

[7] *Schedule 7 of the Serious Crime Act 2007 permits data matching "to assist in the recovery of debt owing to public bodies".*

- communications data are retained by law on the grounds that retention is needed for anti-terrorism purposes; however a separate law allows many organisations access to communications data for diverse purposes[9].

In summary, the point being made is not whether a particular activity or technique or system is acceptable or not, but rather to stress that if personal data are retained in connection with one purpose, then such retention will always encourage the emergence of other ideas for the use of these data. **As function creep can always be authorised by a future law, function creep should be anticipated as an inevitability**. So the question then arises as to whether the current legal framework or system of scrutiny affords sufficient protection when such function creep occurs, or provides the correct structure to balance the opposing objectives (the public interest served by performing a new purpose against the public interest served by maintaining individual privacy)..

Why data protection legislation will not afford sufficient privacy protection

All legislation that legitimises retention, surveillance or sharing of personal data, to some extent, will negate the protective effect of most of the eight Data Protection Principles of the Data Protection Act (DPA) 1998.

The central problem arises if surveillance legislation such as the ID Card Act 2006 states that X items of personal data are to be processed for purpose P1 for Y years, and can be disclosed to organisation Z for purpose P2[10]. In such circumstances, it is going to be very difficult to claim that the First, Second, Third and Fifth Data Protection Principles have been breached because the enactment of surveillance legislation establishes that:

- the processing purposes are lawful and compatible (meeting the relevant First and Second Principle obligations in the Data Protection Act);

[8] *See section 43 of the Statistics and Registration Service Act 2007.*

[9] *For example, section 104 of the Anti-Terrorism, Crime and Security Act gave powers to order the retention of communications data for anti-terrorism purposes but it is section 22(2) of the earlier Regulation of Investigatory Powers Act 2000 that allowed access to the communications data retained for wider purposes (e.g. preventing disorder; economic well-being of the United Kingdom; public safety; public health; assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; emergencies) as well as "for any purpose….specified for the purposes of this subsection by an order made by the Secretary of State".*

[10] *The ID Card Act establishes that 50 items of personal data (Schedule 1) are collected for 5 purposes (Section 1(4)) and can be retained indefinitely. Such data could be disclosed to any public authority (see section 20) for its purposes.*

- specifies the duration of the processing of personal data (satisfying the Fifth Principle obligations over data retention) and

- specifies the items of personal data to be processed (satisfying the Third Principle obligations in connection with the relevance of the personal data to the purpose).

As the disclosure to Z for purpose P2 is likely to be also subject to the exemption from the non-disclosure provisions[11], the Fourth Principle and parts of the Sixth Principle can **additionally** be negated with respect to any disclosure of personal data[12]. As the Eighth Principle is negated if any transfer of personal data outside the European Economic Area is in the "substantial public interest"[13] (e.g. transfers of personal data to the USA for national security, child protection or crime related purposes are likely to pass this substantial public interest test), then the Eighth Principle falls away. This leaves only Principle Seven dealing with security as being unscathed. So when Ministers state something like that "the Data Protection Act safeguards the processing", the claim can be disingenuous[14], if Ministers can subsequently use their powers to modify the impact of the Principles[15].

The use of powers to remove privacy protection can be illustrated by the Community Charge legislation of the nineteen-eighties. In Scotland, regulations required Scottish Community Charge Registration Officers (CCROs) to use a specific Community Charge form produced by the Secretary of State for Scotland; this form collected the date of birth of everybody eligible for the Community Charge. In England there was no such statutory provision, so when English CCROs collected dates of birth using Scottish Community Charge forms, the Data Protection Registrar enforced the data protection principle dealing with the processing of excessive personal data on the grounds that a CCRO only needed the date of birth in limited circumstances (e.g. when someone

[11] *For example, sections 28, 29 or 35 of the Data Protection Act.*

[12] *The exemption from the non-disclosure provisions (in section 27 of the DPA) exempts most of the first data protection principle, and the second, third, fourth and fifth data protection principles, and rights of objection to the disclosure*

[13] *Schedule 4, paragraph 4 allows the Secretary of State to identify what transfers are in the "substantial public interest".*

[14] *A general statement on the lines that "the database will comply with the Data Protection Act" was given, for example on 20 Apr 2006 : Column 807W; and 20 Jul 2005 : Column 1784W and 16 Nov 2004 : Column 1430W in relation to ID Cards Act. Or 1 Sept 2004 : Column 774W and 2 Nov 2004:Column 228 for the Children Act 2004.*

[15] *Section 12 of the Children Act 2004, for example, provides powers to Ministers that could modify the impact of six Data Protection Principles.*

became eligible for the Charge on their 18th birthday; or where two people living at the same address had the same name)[16] (*Rhondda*: *1990*).

Another problem arises because many the Data Protection Principles involve consideration of the "purpose" of the processing. Thus, if the purpose is widely defined (for example, "the efficient and effective delivery of public services" as defined in the ID Card Act 2006), this can degrade the protection of those Principles which are usually interpreted assuming a narrowly drawn "purpose" of the processing[17]. Additionally, data sharing statutory gateways allow personal data collected for one purpose by one Government Department to be used for other purposes under the control of different Departments. In data protection terms, this especially degrades the protection afforded by the Second Principle (purpose limitation).

Finally, it should be noted that, at the time of writing, the Information Commissioner is not a powerful regulator[18],. Currently, the Commissioner does not have powers to audit compliance with the Data Protection Act without permission and the Commissioner can only "name and shame" transgressors in exceptional circumstances. The Commissioner cannot prosecute data controllers that recklessly or deliberately breach a data protection principle and it is only recently, that the Commissioner has been given the ability to fine data controllers when there are serious transgressions[19]. Additionally when the Information Commissioner does raise an issue in connection with a surveillance policy, these views are dismissed by Government as being part of the general opposition to that policy[20].

---

[16] *As the Fourth Principle of the Data Protection Act 1984 is identical the Third Principle of the Data Protection Act 1998, the decision of the Tribunal can be reliably applied to the 1998 Act.*

[17] *For example, if someone says "data item X is relevant to a housing benefit purpose", the claim can objectively be tested- is the data item relevant or not relevant to the housing benefit purpose? However, this kind of test is substantially diminished if the purpose is broadly defined. In the ID Card Act, for example, one purpose relates to "the efficient delivery of public services" which means that to show a breach, the Commissioner has to establish "inefficiency". Most of the data protection principles are defined in terms of a purpose which is assumed to be narrow; the broader the purpose, the narrower the protection afforded by the Principle.*

[18] *The Government have promised the Commissioner more powers of intervention in the wake of the lost CD disks at HMRC*

[19] *In May 2008, the Secretary of State obtained powers under the Criminal Justice and Immigration Act to allow the Commissioner to issue a Monetary Penalty Notice. The use powers by the Commissioner has yet to be determined but Ministers indicated that they are likely to be exercised in those circumstances where the Commissioner also serves an enforcement notice. The serving of an enforcement notice is a rare event.*

[20] *The Information Commissioner's concerns over the ID Card scheme provides an example. The Home Secretary said that the Information Commissioner was "a long-standing opponent of the identity card system" (28 Jun 2005: Column 1157).*

Why scrutiny is deficient in terms of Human Rights legislation

Given the limitations of the data protection regime, Parliamentary scrutiny of legislation that authorises surveillance assumes great importance, and such scrutiny, in privacy terms, is often undertaken in the context of Human Rights legislation.

The Joint Committee of Human Rights (JCHR) has recommended that effective scrutiny of Government legislation requires that a Human Rights Assessment is published (*JCHR: 19th Report*); a recommendation that has not been accepted by Government. Given that one can assume that the JCHR is calling for this Assessment because the requested information is not made available to the Committee, the text of its recommendation reveals several shortcomings in Parliamentary scrutiny.

The Committee stated that it wanted an Assessment "at the very minimum" to include details that:

- "identify the Convention rights and any other human rights engaged by the bill, and the specific provisions of the bill which engage those rights;
- explain the reasons why it is thought that there is no incompatibility with the right engaged;
- where the rights engaged are qualified rights, identify clearly the pressing social need which is relied on to justify any interference with those rights;
- assess the likely impact of the measures on the rights engaged;
- explain the reasons why it is considered that any interference with those rights is justified; and
- cite the evidence that has been taken into account by the Department in the course of its assessment".

The call for an Assessment arose because the JCHR's queries were deflected by the claim that the Human Rights Act provides the necessary safeguards. For example, the Home Secretary on the regulations and orders which could be made under the Identity Cards Bill of Session 2004-05 told the JCHR: "We will be under a duty, under section 6 of the Human Rights Act, to act compatibly in making subordinate legislation and if we did not do so the courts will have the power to strike it

down" (*JCHR: 8th Report*). In other words, scrutiny by Parliament was unnecessary because the Courts could pick up the question of compliance with Human Rights legislation.

The lack of an Assessment also explains the occasional outburst from the Committee in its reports: "This is the fifth Government Bill within a very short period of time containing information sharing provisions the Convention compatibility of which has been asserted but not explained. In respect of each [Bill] we have commented that this is not satisfactory, but there has been no change in the Government's practice. This presents a very real obstacle to our scrutiny work" (*JCHR: 12th Report*). Three years later, the Committee maintains that "a dedicated human rights memorandum should accompany every Government bill" (*JCHR: 6th Report*).

These sentiments are repeated in the Committee's report on Data Protection and Human Rights (*JCHR: 14th Report*) published following an inquiry into to a spate of well publicised data losses by the public sector (e.g. the HMRC's lost CD disks containing 25 million bank account details). The Committee stated that in relation to eighteen Bills that had data sharing provisions that "the Government's response has generally been to resist our recommendations" on the grounds that "public authorities must comply with the provisions of the Data Protection and Human Rights Acts". It stressed that it "fundamentally disagreed" with an approach to setting data sharing policy that depended on "very broad enabling provisions" that grant Ministers far reaching powers. The Committee recommended that data sharing purposes should be specified in primary legislation as this would "increase the opportunity to hold the executive to account".

It is also worth adding that there is also a lack of information for scrutiny purposes in the field of national security (*Pounder, WE 156*) and DNA profiling (*Science and Technology: 2004*), and that the European Parliament has impact on the decisions made at the Council of Ministers; this has raised concerns in the field of law enforcement (*EDPS: 2007*). It is also worth noting that the current Parliamentary arrangements are not responsive to the increasing number of international commitments and treaties[21] and often decisions have to be accepted by the UK Parliament on the grounds that the UK has signed up to an international commitment[22].

[21] *International Treaties or Decisions of the Council of Ministers are often presented to Parliament as fait accompli – for example the ICAO agreement to capture two fingerprints was used in Parliament to justify the capture of all ten fingerprints for the purpose of the ID Card.*

Scrutiny of Secondary Legislation is also generally deficient

The reason why the JCHR is concerned to ensure that any data sharing purpose is specified in primary legislation arises because secondary legislation, enacted via the use of Statutory Instruments (SI), are subject to limited scrutiny in Parliament (if any scrutiny actually occurs)[23]. Ministers can therefore expect the use of their powers to be approved by Parliament and it is a very rare occurrence that an SI is defeated or withdrawn[24]. Even so, the scrutiny of that part of primary legislation which grants the powers to Ministers can also be limited, because of the timetabling procedures are regularly used by Government to ensure that legislation, such as the ID Card Act, passes through Parliament quickly.

The result is that human rights issues are considered by Government when the powers are being made ready for **use** and not when the powers are being **obtained**. **Pre**-legislative scrutiny by Parliament is effectively replaced by **post**-legislative scrutiny by the Courts. Scrutiny in these circumstances becomes the preserve of those rich enough (or poor enough in the case of legal aid) to take human rights cases through the Courts in an attempt to strike out statutory instruments. This legal tussle is also an unequal struggle – the average citizen is pitted against a Government which has access to a bottomless public purse and teams of its own lawyers, if need be.

There are three other problems with the current lack of scrutiny as identified above.

- The Government can use the "powers could be struck-out" argument to ignore criticism in Select Committee Reports which relate to wide ranging powers[25].
- If a Court were to strike out a Ministerial order (as has happened in the field of terrorism) it would bring with it the prospect of further clashes between the Government and the Courts and thereby risk of politicising the judiciary.

[22] *The third pillar Directive on the data retention arrangements in the field of telecommunications, the European Commission agreement on the transfer of PNR data to the USA provide examples where the UK Parliament has to accept the agreement.*

[23] *Parliament considers about 2,500 Statutory Instruments (SI) per year. They cannot be amended but can be rejected. In practice, however, many SIs are not debated. Where debate occurs, it is often within a Committee framework where the majority of members of the Committee are chosen by the Government Whips.*

[24] *One SI on a privacy matter which was withdrawn was the draft SI issued by David Blunkett in relation to wide access to Communications Data (as defined under RIPA). Press reports at the time credited the Home Secretary's son for change of mind (see http://news.bbc.co.uk/1/hi/uk_politics/2051117.stm) and not the rigours of Parliamentary scrutiny.*

- If secondary legislation were to be struck out by the courts, it is possible to envisage circumstances where Ministers would just draft another alternative instrument circumventing any legal problem. The result could be that any legal challenge would need to start again at square one[26].

The lack of Parliamentary scrutiny over policy towards a surveillance activity

The National Identity Register (NIR) of the ID Card Act 2006 provides an extreme example of how a Government can minimise effective Parliamentary and public scrutiny of a proposal – the proposal in question being whether the NIR should be used as a general population register so that commonly held personal data (e.g. name, address) can be shared between most public authorities (*Pounder C: Evidence, 2006*).

In its the two public consultations on its Entitlement/ID Card proposals, the Government specifically **excluded** the use of the NIR[27] to establish a population register for use in general public administration. However, before the General Election of 2005 officials knew (and the evidence suggests that Ministers were informed)[28], that the intention was to use the NIR for this general public administration purpose. This fact could have featured as part of the General Election debate (and the Government could have received an electoral mandate for this element of the ID Card program).

It was also known by Government that the use of the NIR for a general public administration purpose represented around 20% of the business case for the ID Card scheme[29]. However, the Regulatory Impact Assessment associated with ID Card Bill omitted this important fact from the other financial details laid before Parliament as the Bill commenced its Parliamentary stages.

[25] *Recommendations 59 and 60 of the Home Affairs Select Committee's report into ID Cards (session 2004/5). The powers were described as "unacceptable", yet they exist in the ID Card Act 2006 in the same form.*

[26] *This was the practice with respect to National Security Certificates signed under section 28 of the Data Protection Act (e.g. in the case of Norman Baker MP). Mr. Baker won his case, but the Home Secretary issued a modified certificate re-applying the exemption.*

[27] *Paragraph 3.20 of CM 6178, for example, stated that use of the NIR a population register "will also include public consultation to explore the issues around public acceptability of the proposal" and that any new "legislation would also introduce concrete safeguards for the public".*

[28] *A letter dated 10 September 2004 was sent from the CIP project board to the Chief Secretary of the Treasury which stated that the merging of CIP into the NIR would "strengthen the VFM case for ID Cards". It therefore recommended that "the Home Secretary be asked to include improving the efficiency and effectiveness of public services as a purpose of the Identity Card" and that "the NIR should become the national adult population register long term".*

[29] *The CIP minutes of 18 March 2005 identified "substantial CIP related benefits (address sharing benefits) within HO ID Cards outline business case, amounting to around one fifth of the total".*

Several Parliamentary opportunities presented to Ministers to announce this important extension of the NIR's purpose were not taken. A draft Written Ministerial Statement informing Parliament of this extension was prepared, but its publication was delayed for nine months until three weeks after the Bill had received Royal Assent[30].

As is well known, since Royal Assent, the ID Card project has been subject to considerable delay and revision; it is not known whether the use of the NIR as a population register still form part of the plans for the NIR.

PART II: THE NINE PRINCIPLES

Why the Principles are needed

In Part II, the nine Principles are presented in order to provide a framework that corrects the structural defects identified in Part 1. The Principles interact with each other and should be considered as a whole.

As with Part 1, personal data processed as a result of a surveillance activity, any sharing of personal data and any revelation of identity information are all considered to be a surveillance activity. The Principles therefore apply to "dataveillance" (*Clarke R: website*). This extension is important because Government policy involves joined-up public services and widespread data sharing where there is a risk that mistrust of one part of Government also becomes joined-up[31]. It is argued that the application of these Principles to the development of surveillance policy, or to

[30] *A draft "Written Ministerial Statement" to Parliament was included as Annex B of ("Submissions to Ministers") sent to Ministers on 13 July 2005; the actual Written Statement, with minor changes, can be found at Hansard, column 53WS, 18th April 2006.*

[31] *The HMRC security breach involving 25 million records on two CD-disks has undermined confidence in the NHS Spine, the ID Card project and the Children's (contact) index.*

the bodies performing the surveillance, would help maintain public confidence[32] in legitimate surveillance.

The Principles are not primarily presented as proposals for legislation and it is recognised that some of the ideas underpinning a particular Principle are not new[33]. Any novelty lies in the attempt to construct a framework that permits a comprehensive analysis to be undertaken in connection with any surveillance activity. It is for this reason, the commentary on each Principle indicates, where in the UK context, structures can be improved.

Finally, the Principles are expressed using the word "Regulator". Although the Information Commissioner is the most likely Regulator in relation to a surveillance activity, other specialist Regulators in the UK (usually dealing with law enforcement or national security) have to be included as being linked to these Principles. It is worth noting, as an aside, that whereas government services are becoming joined-up, the protection afforded by the current regulatory framework is becoming increasingly disjointed[34].

Principle 1: THE JUSTIFICATION PRINCIPLE

Information relating to any legislation or policy that involves surveillance (or extension to an existing surveillance policy) is provided so an assessment can be made to ensure that the surveillance can be justified in terms of pressing social needs and measurable outcomes; this information is provided prior to the approval of legislation or policy.

Commentary on the Principle

This Principle is about providing full information so that any surveillance policy/legislation can be scrutinised (see Approval Principle).

[32] *There are examples of trust being lost. For example, parents who object to the police retaining DNA of their children who have been mistakenly arrested, parents who object to their children's details being retained on a child at risk register when there is no risk and patients who object to the holding of medical records centrally.*

[33] *For example elements of the Adherence , Separation and Independent Supervision Principles*

[34] *Oversight of the Intelligence Services (except interception practices) is carried out by the Intelligence Services Commissioner. Oversight of interception is carried out by the Interception of Communications Commissioner. The Office of Surveillance Commissioners is responsible for oversight of property interference under Part III of the Police Act, as well as surveillance and the use of Covert Human Intelligence Sources by all organisations bound by the Regulation of Investigatory Powers Act (RIPA) (except the Intelligence Services). There is an Information Commissioner, a National Identity Scheme Commissioner, the Commissioners who deal with Northern Ireland policing/terrorism and the Police Complaints mechanisms and the various Parliamentary Ombudsman could also be drawn into the supervision of surveillance. Recently the Financial Services Authority levied a £1 million fine in a case of inadequate security of personal data held by the Nationwide Building Society.*

Effective public scrutiny of legislation assumes that Parliament has access to **all** relevant documents produced in relation to a surveillance proposal (including legal background, a Human Rights Assessment as requested by the JCHR, policy options, cost benefit analysis, details about technical, operational and risk factors). Government should prepare a list of documents and summarise their content in relation to each proposal for surveillance legislation. However, if these documents contain information that relates to actual surveillance operations (e.g. lessons learnt), then the Government can choose to summarise or redact this information (but such redaction to be indicated in the text).

It is recognised that some documents might have to be subject to special procedures and might not be published as a result of the scrutiny process (e.g. because they contain confidential material). Some documents might, in Parliamentary terms, be only accessible in a very restricted fashion (e.g. by Privy Councillors), but the general rule is the provision of information to Parliament for scrutiny purposes– not its withholding. It is noted that Government has chosen to provide information to the Joint Committee on Human Rights (JCHR) on a confidential basis (*JCHR: 16th Report, Appendix*).

If a policy decision was to be devolved to a lower tier of government (e.g. Local Authority), then the Principle would still apply and information would be provided (e.g. to Councillors).

At the surveillance policy level, the Principle could require the release of information about any privacy risk assessment that has been undertaken – this could be the Surveillance Impact Assessment identified in the Surveillance Society report (*Ball. K et al: 2006*) or a Privacy Impact Assessment (*Information Commissioner: 2007*). So, for example, the procurement of a CCTV system to monitor public places should justify its existence in terms of identifiable purposes and measurable outcomes. The identification of likely measurable outcomes permits the comparison that is essential to the Reporting Principle (which deals with actual outcomes).

Any information obtained via the Justification Principle should become subject to the Freedom of Information Act; this engages the exemptions and appeals process in relation to any information provided to the public. To gain public confidence, information about surveillance policy (e.g. justifications, complaints procedures) should be proactively made available by the public authority performing the surveillance (e.g. on an appropriate web-site).

Principle 2: THE APPROVAL PRINCIPLE

Any surveillance is limited to lawful purposes defined in legislation where such legislation has been thoroughly scrutinised by a fully informed Parliament and, where appropriate, informed public debate has taken place.

Commentary on the Principle

The Principle follows the application of the Justification Principle, in that information provided as justification for surveillance (and costs of surveillance) can be independently assessed by those undertaking the scrutiny. The Approval and Justification Principles, by inference, are likely to draw out any alternatives to the surveillance, and thereby strengthen the justification for, and the public acceptability of, any surveillance that is eventually authorised.

Any relevant Regulator should have a role in assisting Parliament or informing public debate by commenting on the information provided by the application of the Justification Principle. Obviously public comment on specific topics might need to be restrained in some areas where a need for secrecy can be claimed.

The Approval Principle assumes detailed Parliamentary scrutiny of legislation that relates to a surveillance proposal, and there are simple ways of strengthening UK Parliamentary procedure. For example, Codes of Practice (or parts of Codes) or Statutory Instruments that concern surveillance matters should be subject to prior consultation with a Regulator. If the consultation produces disagreement, Parliament should have to approve the Secretary of State's Code or Instrument by a positive affirmation procedure as this would allow Parliament to explore the reasons for any disagreement before approving the secondary legislation or Code of Practice. If there is agreement over the content of a Code or Instrument, then it becomes more acceptable for negative affirmation routes to apply[35]. Of course, disagreements (e.g. over a Code) might emerge at a later stage, and this explains why there is a role for the Regulator in referring matters to Parliament (see the Reporting Principle).

It is argued that if all Codes of Practices or Statutory Instruments dealing with surveillance could become subject to a requirement for affirmative action by Parliament, then civil servants would

[35] *Positive affirmation requires Parliament to vote approve the Code or Instrument; a negative route would assume that Code or Instrument is OK unless there was a Parliamentary vote against*

want to minimise possible difficulties during the approval process. A consultation process between Regulator and civil servants would follow, and the drafting of Codes and Instruments drafting would be very mindful of the Regulator's view. In this way, the Approval Principle improves interaction between Government and Regulator.

To strengthen the scrutiny, Parliament could permit a Select Committee to take privacy under its remit (e.g. the Joint Committee on Human Rights seems an appropriate vehicle given the overlap between data protection and human rights). Currently such issues are discussed in the narrow context of a Committee's specialist remit (e.g. child protection and privacy, science and privacy in relation to the DNA database; the ID Card and privacy, etc) with the result that a joined-up picture of how **all** Government initiatives interact has yet to be completed by Parliament[36].

It is suggested that a Regulator could report to a specific Committee which could task (and fund) the Commissioner to investigate matters of concern. Reports from the Commissioner could be tabled before that Committee which decides what is published. It is also recommended that Select Committees of Parliament should allow, if they decide, experts in the field to question Ministers or witnesses. This is because, often, the devil is in the complex detail of **how** surveillance occurs and not on the broad principle of **whether** surveillance should occur[37].

Where surveillance (in particular, data sharing or revealing of identity information) occurs with consent of the individuals concerned, the Approval Principle is satisfied if that consent is properly formulated; the Regulator has powers to modify improper consent procedures.

Principle 3: THE SEPARATION PRINCIPLE:

Procedures which authorise or legitimise a surveillance activity are separate from procedures related to the actual surveillance itself; the more invasive the surveillance, the wider the degree of separation.

[36] *At the time of writing, the Home Affairs and Constitution Select Committees have yet to issue their reports on the Surveillance Society.*

Commentary on the Principle

This Principle mitigates the problems identified in Part 1 of this paper where Ministers are often politically responsible for the policies which require surveillance to succeed and for the mechanisms that protect private and family life from unwarranted intrusion. Some public bodies also have this dual responsibility and produce Codes of Practice specifying their procedures that cover both surveillance and privacy protection[38].

As the Approval Principle (and Reporting Principle in the case of legislation that has been enacted) allows the Regulator to report to Parliament on any legislation or Code, this can include an independent view on the correct level of separation that is appropriate. The Regulator's recommendations on separation can thus be considered by Parliament when it considers the detail of a surveillance proposal contained in a Bill or Code in question. Informed Parliamentary debate about these issues should be a consequence.

Where separation is achieved by an authorisation officer[39] or Single Point of Contact (SPOC)[40], the Regulator could determine how separation procedures should apply, the nature of the records to be maintained by that officer or SPOC (Reporting and Adherence Principles). This would apply to the practice of the Home Secretary authorising warrants or certificates to justify interference in relation to national security or policing. In this way, the Regulator would be in a position to report to Parliament about any deficiency in the system of supervision (e.g. present an informed view as to whether judicial approval of warrants would provide better safeguards).

---

[37] *For example, the vast majority of the public support surveillance for anti-terrorism purposes – the controversy lies not with the **whether** there should be surveillance, but with the **how** surveillance is regulated or **how** the products of surveillance are used or disclosed to others.*

[38] *|For example, the Audit Commissioner Code of Practice on Data Matching.*

[39] *Authorisation officers are used by the DWP in relation to the exercise of its powers in relation to benefit fraud.*

[40] *Usually an authorisation officer or SPOC is a senior officer of a public authority who exercises powers granted to a public body but is not part of the investigating team. The investigating officer has to convince the authorising officer/SPOC that the exercise of powers is needed, and the SPOC determines whether the use of powers would be appropriate. Usually authorising officers/SPOCs are given specialist training on the relevant law.*

Principle 4: THE ADHERENCE PRINCIPLE:

Procedures which authorise a surveillance activity are professionally managed and audited; staff involved in a surveillance activity are fully trained to follow relevant procedures and that such training is assessed if appropriate; any malfeasance in relation to a surveillance activity can be identified and individuals concerned suitably punished.

Commentary on the Principle

This Principle is directed at organisations performing the surveillance. It requires that surveillance procedures are subject to appropriate management and control and any wrongdoing is identified and punished. Often rigorous application of data protection obligations (if backed by a suitably empowered Information Commissioner) should provide a suitable framework for the Adherence Principle (e.g. to security obligations under the Seventh Data Protection Principle).

One would expect the Regulator to give advice in relation to the correct surveillance procedures to be followed whilst the Independent Supervision and Reporting Principles permits the Regulator to intervene on procedural matters if need be.

The Adherence Principle provides an oversight mechanism that could include supervision of the privacy related obligations that are connected to the Government's Data Handling Review (e.g. there is a senior board member responsible for the processing of personal data, that there is suitable training of staff, that procedures are reviewed and maintained, and that risk assessments are taken at regular periods). The same applies to initiatives such as compliance with those privacy-related elements of the National Information Assurance Strategy (*Cabinet Office: 2008*).

From an individual's perspective, the Adherence Principle is important. If an individual experiences failures in surveillance procedure, that individual has to be able to raise issues with the relevant Regulator who then has to possess sufficient clout to resolve and investigate any problem (the subject of the next two Principles).

Principle 5: THE REPORTING PRINCIPLE

A Regulator shall determine what records, including statistical records, are retained and maintained concerning a surveillance activity, in order to ensure transparency and accountability to the Regulator, to the public and to Parliament.

Commentary on the Principle

This Principle deals with the information recorded by those undertaking the surveillance in order to reassure the public that a surveillance activity has followed the rules. These records include details about authorisation, cost of surveillance, outcomes, training, management, procedures, any audit or information requirements as determined by the Regulator. The Regulator should provide relevant advice and guidance on what records to maintain and what needs to be reported (e.g. a loss of unencrypted personal data on a laptop).

Regulations or laws that specify what statistics are collected or published have the potential limit the effectiveness of supervision[41]. Thus it is essential to have an independent Regulator identifying all reporting requirements and the criteria which measure the success of a surveillance activity. In this way, the public can have confidence there is an independent and complete record of the activity that demonstrates it was properly authorised and that the interference was justifiable in terms of actual outcomes. Any Parliamentary Committee, at any time, should be able to commission a report from a Regulator in relation to a surveillance issue.

Reports concerning a surveillance activity are produced by the Regulator and should be laid before Parliament and published. Where sensitive matters are reported, a Parliamentary Committee following consultation with the Government, should determine what is published[42]. All measurable outcomes can be compared with the Justification Principle which deals with predicted outcomes to see whether the surveillance is effective – the inference being, that if the surveillance is ineffective or cost-efficient, then the surveillance ceases.

[41] *Regulation 9 of SI 2007 No 2199 dealing with the retention of communications data illustrates the problem. It limits one statistical item to "the number of occasions when data have been disclosed". This means, for example, that a disclosure of data pertaining to say 3,000 individuals would count as 1 disclosure, when perhaps the 3,000 is the more interesting number the Regulator would want to examine.*

[42] *Currently, the regulators who supervise national security report to the Home Secretary or Prime Minister who then determines what is placed before Parliament.*

From an individual's perspective, accountability is achieved if he or she can refer relevant matters to a Regulator for investigation (e.g. after becoming aware of an unjustifiable surveillance activity that involves them). This involvement could extend from complaints for individuals that they are subjected to unwarranted surveillance or to suggestions from individuals on policy matters.

Principle 6: THE INDEPENDENT SUPERVISION PRINCIPLE

The system of supervision for a surveillance activity is independent of Government, well financed, and has effective powers of investigation and can delve into operational matters.

Commentary on the Principle

The Principle ensures that a Regulator should be able to investigate any aspect of a surveillance activity (including national security) where the Regulator defines the thresholds of what would be considered a valid complaint (in order to exclude vexatious or trivial complaints).

To achieve this objective, a Regulator should possess effective powers of investigation, intervention, audit and prosecution that can extend into operational matters and should be able to employ security cleared experts to investigate relevant matters where this is needed. The Regulator should be able to fine, prosecute or require restitution to individuals who have been significantly damaged or distressed by an inappropriate surveillance activity (see the Compensation Principle).

The Regulator should have a last-resort the power to halt the processing of personal data. This could arise following application to a High Court judge or a power that was subject to appeal via a Tribunal mechanism. The reference to a Court or Tribunal is important as it allows the body undertaking the surveillance to make counter arguments that these powers should not be exercised. In the case of sensitive surveillance operations, the Court/Tribunal can decide whether its hearings are in public or not.

In general, however, any Regulator is unlikely to use his powers immediately or publicise a problem. If made aware of a pressing surveillance problem, the Regulator would first be likely to encourage voluntary changes to any policy, Code of Practice or procedures that, in his view, would

resolve the matter. So, referral to Parliament or public discussion of a surveillance issue (e.g. a report via the Reporting Principle) would only arise if there was a no agreement between Government and a Regulator as to surveillance procedures. For example, a Regulator wanting one level of protection and a Minister wanting another.

In the case of the use of Ministerial powers that have been generously interpreted, the Regulator should be provided with an "Article 8 (Incompatibility) Notice" which, as a last resort, can be used to test whether a particular Statutory Instrument or primary legislation is compatible with human rights law[43]. This Notice can be appealed to the Courts so that the issue of compatibility with Human Rights law can be tested.

If such a Notice were to be served, it would signal a severe dispute between Government and Regulator and one would expect Parliament to investigate. So as an intermediary measure, therefore, the Regulator should also be able to require or recommend to Parliament that a particular use of Ministerial powers or procedure should be reviewed. Alternatively the Regulator could be required to negotiate with the Minister before serving such a Notice.

If an organisation were to employ an independent Data Protection Officer, an idea that has resurfaced in the Information Commissioner's written evidence to Parliament[44], the Regulator could specify the procedures, records or reporting framework that Officer maintains in relation to a surveillance activity (the Reporting Principle).

To ensure independent supervision, a Regulator supervising a surveillance activity should be appointed by, removed by, and report to Parliament. Distance from Ministerial influence in the appointment of a Regulator is important. It is suggested that some candidates could be proposed by the relevant Cabinet Minister to be a Regulator but the final appointment (whether on the Ministerial list or not) should be approved by a Parliamentary process or by an independent public appointments commission.

Where surveillance occurs with consent of the individuals concerned, the Principle is satisfied if the Regulator can ensure that any individual consent is properly formulated.

[43] *This ability could apply, for example, if powers relating to the use of Section 22(2)(h) of the Regulation of Investigatory Powers Act 2000 (access to communications data "for any purpose…….specified for the purposes of this subsection by an order made by the Secretary of State") were used in a way that the Regulator found to be excessive.*

[44] *The prospect was explored in paragraph 30 of "Additional Evidence Submitted by the Information Commissioner" to the Home Affairs Select Committee's Inquiry into the Surveillance Society.*

The Regulator should be identified in law as being independent assessor of relevant surveillance activities with particular responsibility to protect the public. Appeals processes against a Regulator's decision can follow established models (e.g. a Tribunal as in the Data Protection Act regime with appeals to the Courts on points of law). Where there is an issue of substantial public interest, individuals should be able to appeal to the Tribunal/Courts on the grounds that the Regulator has not made a particular decision[45]. Finally, Ministers should not possess general powers to overturn the decision of a Regulator (or a Tribunal or Court) via the current arrangements that apply to secondary legislation, as Parliamentary scrutiny is minimal (see Part 1 of this paper).

Principle 7: THE PRIVACY PRINCIPLE

Individuals should be granted a right to privacy of personal data, via data protection legislation, which can be enforced by a Data Protection Commissioner, and should possess a much simpler right to object to the processing of personal data in appropriate circumstances.

Commentary on the Principle

The Principle is aimed at empowering the individual and provides an extension of individual rights in the way that would encourage, in particular, a public authority not to exceed its powers. There are two elements: a new statutory "right to privacy of personal data" and a revised right to object to the processing of personal data (currently found in Section 10 of the DPA).

In the UK, for example, the right to privacy of personal data could be implemented as an amendment to the Sixth Data Protection Principle and expressed in human rights terms. For example:

"*Personal data shall be processed in accordance with the rights of data subjects under this Act and, in particular, personal data shall not be processed in a way that does not respect the private and family life or correspondence of data subjects".*

[45] *The model used here is the Decision Notice under the FOI regime, where the applicant can appeal to the Tribunal on the grounds that the Commissioner failed to issue a Decision Notice in favour of the applicant.*

By implementing a right to the privacy of personal data under the auspices of the Data Protection Act, the processing of personal data for the Special Purpose (i.e. freedom of expression purposes) will be left undisturbed[46]; investigative journalism, for example, is unaffected by the change. Obviously this Principle has to be qualified in a way that engages the exemptions found in Article 8(2) of the Human Rights Convention (i.e. provide suitable exemptions for national security, law enforcement etc).

The effect of this change would explicitly link the Human Rights and Data Protection regimes and give the UK's Information Commissioner an explicit human rights role but only in the context of personal data. It is suggested that this Commissioner should be the Regulator that is empowered to serve an Article 8 (Incompatibility) Notice (as suggested in relation to the Independent Supervision Principle).

However, this Privacy Principle should, be extended to include surveillance undertaken in the domestic circumstance (*Pounder C: 2002*); for example, a householder who installs a CCTV security systems and which also covers neighbours' premises, as currently the householder can be exempt from the application of all the Data Protection Principles and rights[47]. However, it is recognised that this could be a very difficult area to balance correctly – and it could be that a right to object to the processing could work better (see below).

The Section 10 right to object to the processing of personal data under the DPA currently requires the processing to cause substantial damage or substantial distress and for that damage or distress to be unwarranted. Additionally, the right is constrained to that processing undertaken in specific circumstances[48]. These thresholds and limitations, in effect, neutralise a right that cannot be exercised easily by the individual concerned.

The suggestion is that if data sharing occurs following a surveillance activity, then the burden of proof for the right to object should be reversed. Thus, if the right is exercised, the organisation concerned would continue the processing of personal data if it could show that the processing of personal data was warranted in terms of a specific public interest specified in Article 8(2) of the

[46] *Section 32 of the DPA protects the Press until publication of the personal data concerned.*

[47] *Section 36 of the DPA (Domestic purpose exemption).*

[48] *The processing has to be legitimised in terms of paragraph 5 and 6 of Schedule 2 of the DPA*

Human Rights Convention (e.g. that data sharing or surveillance was necessary in terms of crime prevention, public health, national security etc).

In summary, a revised right to object should not interfere with that processing of personal data that has been undertaken by law enforcement etc, but the right would be easier to claim by the individual, in a context where the processing had been undertaken by a public authority on grounds such as administrative convenience[49]. Note that if individuals trusted the data sharing arrangements undertaken by public authorities, then it is unlikely that such individuals would need to exercise the right to object.

It is also noted that there could be a need to protect the public authority if the right to object to the processing of personal data was being exercised vexatiously (e.g. as part of a campaign to disrupt a public authority).

This Principle also extends to the issuing of fair processing notices (if applicable[50]). Such notices are an important protection because it is difficult for individuals to protect their own privacy, or to object to the processing of their personal data, if they don't know whether their personal data are processed in the first place. However, these notice obligations have real value only if individuals can act on the information received (e.g. raise matters of concern with a Regulator).

Principle 8: THE COMPENSATION PRINCIPLE

An individual should obtain compensation if a surveillance activity has caused damage, distress or detriment that proves to be unjustified.

Commentary on the Principle

A Regulator, following detailed investigation under the Independent Supervision Principle, should be able to award limited remedial compensation, to the level assessed in a small claims court, to each individual who has been damaged and distressed as a result of a surveillance activity. Balance

[49] *Section 1(4) of the ID Card Act allows for such data sharing on "efficiency" grounds. The right to object would apply to this purpose but not, for example, to the crime related purpose.*

[50] *An exemption from the notice provisions apply if provision of a notice would prejudice crime prevention or national security etc in order to protect special law enforcement interests.*

could be provided by allowing the body undertaking the surveillance, to appeal against any award to the Courts. Where larger sums of money are involved, the Courts would have to become involved immediately; in such cases, and where appropriate, the Regulator should be able to assist individuals with their claim[51].

Principle 9: THE UNACCEPTABILITY PRINCIPLE

If the other Principles cannot be complied with in relation to a surveillance activity then within a reasonable time:

(a) the activity ceases; or

(b) alternative steps are taken to bring the activity into conformity with the other Principles; or

(c) Parliament or a Parliamentary Committee approves the non-compliance with the relevant Principle.

Commentary on the Principle

This Principle ensures that breaches of other Principles do not arise from actions motivated by executive convenience.

Under the Human Rights Act, the Courts can make a "declaration of incompatibility" in relation to any piece of primary legislation or can strike out secondary legislation[52]. The possibility that a Regulator can issue an Article 8 (Incompatibility) Notice (see the Independent Supervision Principle) makes this protection more accessible in the context of surveillance legislation and allows a Court to consider facts surrounding a surveillance activity. It is for the Court to decide whether any hearing is in public or not.

[51] *This is an extension of S.53 of the DPA which permits the Commissioner to aid an action that involves the Special Purposes (e.g. journalism).*

[52] *See sections 4, 6 and 10 and Schedule 2, paragraph 2(b).*

The suggestion is that this Principle can operate in a similar manner. For example, by a Regulator making a report to Parliament in relation to the steps (a), (b) or (c) above (see the Reporting Principle). It would be for Ministers and Parliament to decide what to do in the light of the report; however, the assumption is that the public interest generated by the Regulator's report would oblige Parliament or a Committee to consider the surveillance issue in detail. It would need a vote in Parliament if the surveillance were to continue.

Concluding comment

Part 1 of this article shows that in the context of privacy protection, the current system of regulation is weak, the current law cannot be relied upon, and that Parliament is not in a position to scrutinise effectively. It is argued that there needs to be a far stronger "feed-back" loop which gives an informed Parliament a leading role in deciding public policy with respect to balancing the need to perform surveillance against the need to respect private and family life. Part of the feedback loop is the empowered Regulator.

Concerns might arise because these Principles envisage conflict between the Regulator and the government of the day. However, if such conflict arises, the matter can be resolved by Parliament or the Courts; the former dealing with policy matters, the latter dealing with legalities. There is nothing in the Principles that is in conflict with the constitutional way of resolving social policy issues in a democratic society.

Finally, and most importantly. these Principles allow the surveillance society debate to take place in a context that rectifies the weaknesses in the current framework of information law governance.

Dr. C.N.M. Pounder
E-mail: chris.pounder@amberhawk.com
July 2008

REFERENCES

1. Ball K, et al, Report for the Information Commissioner on the Surveillance Society. 2006 (http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf).

2. Cabinet Office, Data Handling Procedures in Government (2008) and the National Information Assurance Strategy (2007).

3. CIP (Citizen Information Project) documents on http://www.gro.gov.uk/cip/: all published 2005.

4. Clarke R, Information Technology and Dataveillance; http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html.

5. Constitution Committee of House of Lords, Q7 of the Corrected Oral Evidence of the meeting on the Surveillance Inquiry with the Information Commissioner, Mr Richard Thomas(14 November 2007).

6. European Data Protection Supervisor (EDPS), press release "Data protection framework decision: EDPS concerned about dilution of data protection standards", September 2007.

7. Information Commissioner, Privacy Impact Assessment documents, (http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html).

8. Joint Committee on Human Rights (JCHR), 6th Report, Session 2007-8.

9. Joint Committee on Human Rights (JCHR), 8th Report, Session 2004-5.

10. Joint Committee on Human Rights (JCHR), 12th Report, Session 2004-5.

11. Joint Committee on Human Rights (JCHR), 14th Report, Session 2007-8 and http://www.out-law.com/page-8952.

12. Joint Committee on Human Rights (JCHR), 16th Report, Appendix 20D, Session 2006-7.

13. Joint Committee on Human Rights (JCHR), 19th Report, Session 2004-5.

14. Pounder C, DNA database 'will span most of the UK population": http://www.out-law.com/default.aspx?page=7945, 2006.

15. Pounder C, Published in the Joint Committee On Human Rights, Third Report ("Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters"), Session 2005-2006, Written Evidence (WE) 156.

16. Pounder C, Written evidence given to the Home Affairs Select Committee inquiry into the "Surveillance Society" (full copy on http://identityproject.lse.ac.uk/#Home_Affairs_Committee).

17. Pounder C. Written evidence to the Culture, Media and Sport Committee, "Privacy and Media Intrusion, Fifth Report, session 2002-2003" (Appendix 3).

18. R v Shayler [2002] 2 WLR 754 [House of Lords; paragraph 26].

19. Rhondda Borough Council v the Data Protection Registrar Data Protection Tribunal: 1990 (http://www.informationtribunal.gov.uk/Documents/decisions/community_charge.pdf.

20. Science and Technology Parliamentary Select Committee, "Forensic Science on Trial", Session 2004-2005).

21. Silver and others v United Kingdom ([1983] ECHR 5947/72;paragraph 97).

ADVERT

COURSES FOR INFORMATION LAW OFFICERS, PRIVACY PRACTITIONERS OR DATA PROTECTION OFFICERS

Amberhawk provides a wide range of public training suitable for data protection officers in the UK. These include courses leading to the ISEB qualification in data protection which can be held on-site.

With respect to on-site training, Amberhawk can provide sector specific training (e.g. on rights of access, CCTV, human resources, data sharing, direct marketing) or targeted at specific staff members (e.g. managers) or on specialist aspects (e.g. social work functions, anti-fraud functions).

We have day long public courses in Data Protection Audit, Privacy Impact Assessments and RIPA courses.

We hope to offer the ISEB syllabus into Information Security Management soon; if interested email info@amberhawk.com

COURSES IN FREEDOM OF INFORMATION

Amberhawk provides a wide range of public training suitable for those dealing with Freedom of Information and the Environmental Information Regulations. These include courses leading to the ISEB qualification.

With respect to on-site training, Amberhawk can provide sector specific training aimed at those helping a public authority meet its obligations. Courses can include Re-use Regulations by Public Sector Bodies.

If interested please contact us at ***info@amberhawk.com***