

# LIBERTY

PROTECTING CIVIL LIBERTIES  
PROMOTING HUMAN RIGHTS

## **Liberty's response to the Home Affairs Committee Inquiry into 'A Surveillance Society'**

**April 2007**

## **About Liberty**

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

## **Liberty Policy**

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at

[www.liberty-human-rights.org.uk/resources/policy-papers/index.shtml](http://www.liberty-human-rights.org.uk/resources/policy-papers/index.shtml)

## **Contact**

Gareth Crossman

Director of Policy

Direct Line: 020 7378 3654

Email: [GarethC@liberty-human-rights.org.uk](mailto:GarethC@liberty-human-rights.org.uk)

Jago Russell

Policy Officer

Direct Line 020 7378 3659

Email: [JagoR@liberty-human-rights.org.uk](mailto:JagoR@liberty-human-rights.org.uk)

## Introduction

1. In November 2006 the Information Commissioner Richard Thomas said “*Two years ago I warned that we were in danger of sleepwalking into a surveillance society. Today I fear that we are in fact waking up to a surveillance society that is already all around us.*” His words came at the time ‘*A Report on the Surveillance Society*’<sup>1</sup> was published. Liberty agrees with the assessment made by the Information Commissioner. We also accept that surveillance is an unavoidable, and often justified, aspect of life in the early 21<sup>st</sup> century. However, the extent to which every person in the UK is subjected to surveillance, has increased disproportionately to any justifying social need or benefit. We are pleased that the Home Affairs Committee is calling for evidence at this time. However, a word limit of 2, 500 precludes any detailed examination of an extremely complex subject. Liberty will be publishing a substantive work on surveillance and privacy over the summer which will cover in far greater detail some of the issues touched on here.

2. It is useful to clarify what types of activity might be considered ‘surveillance’. ‘Mass informational surveillance’ relates to the retention and dissemination of database information. This would cover databases such as the National Identity Register (NIR), created by the Identity Card Act 2006 (IDCA) and the children’s index set up by the Children Act 2004. ‘Mass Visual Surveillance’ relates to the use of CCTV cameras. ‘Targeted Surveillance’ refers to the use of intrusive powers such as communication interception by means of the framework created under the Regulation of Investigatory Powers Act 2000 (RIPA). The central distinction between these types of surveillance is that targeted surveillance is commonly used as part of an intelligence led investigation into illegal or unlawful activity. Mass visual and informational surveillance does not take place in anticipation of a specific investigation into impropriety but will often be claimed to have some crime detection or (in the case of CCTV) crime prevention purpose. Information is retained and disseminated in anticipation of being of use for investigation. Mass informational surveillance will also take place for purpose unrelated to investigation such as assisting access to public services. Mass and targeted surveillance techniques have

---

<sup>1</sup>[http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/surveillance\\_society\\_full\\_report\\_2006.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf)

usually been distinct. However, in the last few years this distinction has been blurred by increasing use of ‘data matching’ and ‘data mining’ processes. These techniques are based on the use of automated processes which analyse or match seemingly innocuous data in order to throw up anomalies or inconsistencies. When used in relation to information about people this is more commonly known as ‘profiling’. The blurring of distinction arises from the fact that there is no human or intelligence led initiation of suspicion. Human investigation will follow *after* initial matching or mining. Finally, the retention of DNA retained on the National DNA Database (NDNAD) is arguably surveillance. It is, however, distinct from mass informational surveillance in that it is ‘data’ that (at present) serves a specific single purpose which cannot be applied elsewhere. We will make brief observations on all these forms of surveillance along with appropriate conclusions and recommendations.

### **Mass informational surveillance**

3. Proliferation of CCTV might attract more observation and comment. However, the increase in informational database use has arguably been the more profound societal shift in the last decade. Access to and use of mass informational databases is part and parcel of everyday life, whether it is almost instant information provision via an internet search engine or identifying a postal address by way of a postcode and house number. Mass informational database use is increasingly being used as a tool of government through programmes such as the compulsory NIR or the children’s index. The children’s index is intended to assist child protection by allowing different services the ability to enter and access details of children onto the index, including anything that might constitute a ‘cause for concern’.
  
4. Liberty’s views on the undesirability and likely ineffectiveness of the NIR are well documented and we do not intend to repeat these here. There are, however, several points that can be made about the IDCA that are relevant to consideration of the surveillance society. The reserved powers scattered throughout the bill allow scope for the range of uses and purposes of the NIR, and those who can have access to it to be increased. If the NIR comes into existence then it is likely to make logistical, financial and political sense to increase the purposes it serves. If, for example, the NIR had been in operation at the time of Ian Huntley’s conviction for the Soham murders, the mood of public outrage was such that there would have been political

pressure to place details of convictions or ‘soft’ non conviction police intelligence onto NIR entries<sup>2</sup>. The experience of the previous World War II identity cards suggests that extra purposes would be found as that scheme saw an increase in uses from three to 39 in 11 years. A further point worth making is that as the identity cards scheme is rolled out, the NIR will also allow a detailed audit trail of individual activities to be drawn on each entry by virtue of the entries permitted by paragraph 9 of Schedule 1 IDCA. If private sector agencies such as banks gain access to NIR as a means of verifying identification, the detail on this audit trail will increase.

5. While Liberty does not believe that there is any justification for the NIR, we do not take a similar position in relation to others mass informational databases. For example, we accept that the children’s index was created to protect children. We did take issue with the bill when it was passing through parliament. The policy driver for information sharing powers was the tragic death of Victoria Climbié. The implication was that social workers in her case were somehow prevented from sharing information. Information sharing powers were available and Victoria’s death was more a result of a catalogue of mistakes and that those responsible for her care lacked training, resources and guidance. Liberty also felt that the proposals were so broad and poorly framed as to raise significant concerns over the privacy of children and families. We believed the index might also undermine child protection. So much information would be gathered that children genuinely at risk might be overlooked as a consequence of ‘not seeing the woods for the trees’. However, we do believe that the children’s index, if limited in scope and effectively regulated, could prove to have genuine child protection benefits. The application of Human Rights principles of necessity, proportionality and legitimate purpose could ensure that only appropriate information is entered into the index and only those who have proper justification would have access. Effective oversight of the ICO would also be essential for proper operation. As previously stated, there is not the space to provide more detail in this document; Liberty’s forthcoming work on privacy gives more detail on this subject. However, the example of the children’s index encapsulates Liberty’s approach to mass informational surveillance. Used effectively, it can be of public benefit. Used excessively, it infringes privacy and can be counterproductive. Human rights

---

<sup>2</sup> As it was the Bichard Inquiry into the killings made the commendable suggestion that a positive vetting process be introduced.

principles and effective regulation can provide a framework for striking a balance. Unfortunately, comments made by the Prime Minister earlier this year indicate that the prevailing attitude in government is that mass public sector information sharing is, by its nature, desirable.

## **Mass Visual Surveillance**

6. The proliferation of CCTV in the UK is well documented. Hardly a week passes without new newspaper reports of CCTV technology advances. Whether these new generation systems will prove to be of greater use in combating crime remains unproven. Many improvements seem little more than gimmicks. Liberty believes that CCTV has some limited crime detection use, but negligible crime prevention use. At most, it can play a part in a holistic approach to combating crime.

7. Liberty has two principal areas of concern over the use of CCTV. Firstly, it remains effectively unregulated. The legislation that can<sup>3</sup> apply to CCTV is the Data Protection Act 1998 (DPA). However the DPA is not intended to provide a comprehensive framework for CCTV regulation. The data protection principles in the DPA cater for the processing, retention and dissemination of data. They do not provide any detail on, for example, the need to justify location for cameras, details on notification of location, good practice on handling footage and so on. Good guidance does exist for the use of both private and public sector systems<sup>4</sup> but these are effectively voluntary and unenforceable.

7. Our second principal concern is that even the limited applicability of the DPA only relates to a small number of CCTV cameras. The case of *Durant*<sup>5</sup> in 2004 has resulted in many systems not being subject to the DPA. The basic position is that CCTV is only covered by the DPA if it can be shown that a system is targeted on an identifiable subject. Clearly many systems, especially those set up by public

---

<sup>3</sup> But which often does not. See paragraph 7

<sup>4</sup> See for example the guidance issued by the Information Commissioners Office in 2000 for operators of CCTV systems

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/cctv\\_code\\_of\\_practice.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cctv_code_of_practice.pdf) and “*A Watching Brief – A Code of Practice for CCTV*” aimed at public sector users of systems published by the Local Government Information Unit in 1996

<sup>5</sup> *Durant v Financial Services Authority* [2004] F.S.R 28, CA

authorities, do not target individuals and would not be governed by the DPA. As a consequence, CCTV in the UK remains largely unregulated.

8. In March 2007 the Council of Europe Venice Commission published an opinion on video surveillance in public places and the protection of Human Rights<sup>6</sup>. It laid out the Venice Commissions views on the data protection and human rights requirements of legislation and good practice governing the use of CCTV. Its conclusions serve as a useful reminder of the societal impact of CCTV upon a country where it has become ubiquitous. *‘Video surveillance of public areas by public authorities or law enforcement agencies can constitute an undeniable threat to fundamental rights such as the right to privacy...and his/her right to benefit from specific protection regarding personal data collected by such surveillance...it is recommended that specific regulations should be enacted at both international and national level in order to cover the specific issue of video surveillance by public authorities of public areas as a limitation of the right to privacy.’*<sup>7</sup>

### **Intrusive Surveillance**

8. The use of intrusive surveillance is governed by the Regulation of Investigatory Powers Act 2000 (RIPA). This call for evidence does not mention RIPA. However, given that the most invasive surveillance uses RIPA powers, we will make a few observations. There can be no argument against the proportionate use of surveillance powers by the state particularly when involving investigations into serious crime and threats to national security. The use of RIPA has increased considerably since it was passed. To an extent, this might be justified by increased concerns over national security. However the sheer scale of RIPA use is staggering. In February 2007 the Interception of Communication Commissioner, Sir Swinton Thomas, reported that over 439, 000 requests for communications traffic data were made in the period 1 January 2005 to 31 March 2006<sup>8</sup>. A total of 2243 intercept warrants were issued in the same 15 month period<sup>9</sup>. The scale of surveillance can be

---

<sup>6</sup> [http://www.venice.coe.int/docs/2007/CDL-AD\(2007\)014-e.asp](http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.asp)

<sup>7</sup> Ibid paragraphs 79-81

<sup>8</sup> ‘Communications data’ are records (but not the contents) of communication traffic such as mobile phone calls and email records. According to the report for 2005-6 there were 439,054 requests <http://www.ipt-uk.com/docs/HC315.pdf>

<sup>9</sup> ‘Intercept warrants’ allow interception of communications so that the contents of communication s can be recorded

attributed to several factors. The scope of those able to use RIPA powers is wide with a huge range of public bodies having access to them. RIPA orders published as secondary legislation set out those bodies with access to RIPA powers. However, they receive scant parliamentary time and are, in any event, unamendable. RIPA powers are often self authorising with lower level communications data powers being authorised internally and even the highest level interception powers only requiring the authority of a government minister. This can be contrasted with the USA where historically, there has always been independent judicial authorisation at the heart of the US surveillance process. Any surveillance warrant against a US citizen needs to be granted by a court. Meanwhile, interceptions of Communications to the US originating from overseas need authorisation from a special Foreign Intelligence Surveillance Court. After the September 11 bombings, attempts by President Bush to introduce a limited scheme of executive authorisation of warrants (i.e. similar to the UK's) was deemed unconstitutional by the US Federal Court.

### **The National DNA Database (NDNAD)**

9. The UK retains five times as many of its population on the NDNAD as any other country. In recent years the grounds for taking and permanently retaining DNA has expanded from those who are convicted of offences, to the current position of retention on arrest for any recordable offence. There is discretion for the police to remove a sample but this seems only to be exercised in exceptional circumstances. There are indications that the grounds for retention may soon be increased again to cover arrest for non recordable offences<sup>10</sup>. Liberty believes that the continued rolling out of the database will eventually result in a 'tipping point', whereby a large enough proportion of the population are on the register to justify the case for compulsory entry for all on the NDNAD. We believe that if this is the intention then the case for compulsory retention should be made now. Liberty accepts that there is a need for a limited database of those convicted for certain offences (generally involving violence or sexual assault). However DNA is irrelevant in most criminal cases and the vast

---

<sup>10</sup> See the recent Home Office consultation 'Modernising Police Powers: Review of the police and Criminal Evidence Act (PACE) 1984 at paragraph 3.33 "The absence of the ability to take fingerprints etc in relation to all offences may be considered to undermine the value and purpose of having the ability to confirm or disprove identification and, importantly, to make checks on a searchable database aimed at detecting existing and future offending and protecting the public. There have been notable successes particularly through the use of the DNA database in bringing offenders to justice". <http://www.homeoffice.gov.uk/documents/cons-2007-pace-review?view=Binary>

majority of entries on the register will be of no use in solving crimes. It is very difficult to have a debate on the NDNAD as discussion usually takes place following the DNA assisted conviction of a person for a gruesome historical crime. It is difficult to weigh the 'light effect, wide impact'<sup>11</sup> effect of DNA retention on the population as a whole in the context of this type of case. Again there is not space here to discuss these issues in detail but it is worth noting that the impact of roll out has had a hugely disproportionate impact upon certain demographics, particularly Afro Caribbean males. It has also resulted in the permanent retention of thousands of young people under 16 with no criminal conviction or caution. Balanced against this is an admission from the Government that there is no evidence that taking of DNA from those who have not been convicted has helped crime detection<sup>12</sup>. Furthermore, although there has been a massive extension of the NDNAD over the last 3 to 4 years, the rate of crime detection using the Database has stayed at about 0.35% of all recorded crime. If extending the size of the NDNAD had been successful one would expect this proportion to have increased.

### **Data Matching, Data Mining and Profiling**

10. As mentioned in the introduction, data mining and data matching techniques are increasingly being used for crime detection. The Serious Crime Bill before Parliament formalises data matching practices in relation to fraud. A recent Home Office White Paper<sup>13</sup> gave details of plans to increase the use of data mining techniques. These practices are a consequence of increased technological sophistication coupled with vast quantities of data held on mass informational databases, making traditional human lead intelligence policing more difficult. As well as raising significant issues of proportionality and legitimate purpose, there are several specific points that the Committee might consider. Of particular significance and central to Liberty's analysis of the surveillance society is that data matching and data mining practices have outstripped data protection legislation. The DPA is nearly 10 years old. The European directive upon which the DPA is based, dates from

---

<sup>11</sup> 'Light impact, wide effect' measures are ones which have a relatively small impact upon an individual but which have a considerable cumulative effect upon society.

<sup>12</sup> Home Office Minister Joan Ryan 9 October 2006 "As far as we are aware, there is no definitive data available on whether persons arrested but not proceeded against are more likely to offend than the population at large." HC Deb, Col 491W

<sup>13</sup> New Powers Against Organised and Financial Crime

1995<sup>14</sup>. The regime created by the act and its accompanying principles might have provided an adequate framework at a time when processing more usually involved the processing of small amounts of data. However, the DPA is not equipped to cope with mass data processing exercises. For example, the second data protection directive permits data processing only for one or more specified purposes. However, all that is required, is for these purposes to be notified to the Information Commissioners Office (ICO). This would allow mass processing from multiple purposes, just so long as the ICO is notified. Notification is essentially an administrative matter. The ICO has no ability to refuse notification and what limited enforcement powers exist, can apply only once processing has already taken place.

11. As mentioned earlier, data matching and mining processes applied to people can be called profiling. Following the terrorist bombings in July 2005 and the alleged aeroplane hijackings in August 2006, there were calls from a variety of sources to adopt profiling on public transport and for flight passengers. So far, we are pleased to see that there have been no moves in this direction. However, we are concerned that the growth of mass informational databases might make moves towards profiling difficult to resist. The National Identity register is a good example of how this might occur. After the July 2005 attacks, the former Home Secretary, Charles Clarke, publicly accepted that ID cards and the NIR would not have prevented the attacks. This makes sense as it is safe to assume that British intelligence and policing agencies have gathered information on anyone that they believe could constitute a risk to national security. The reality is that anyone who does give reason for concern would become subject to a level of targeted surveillance that would collate information going way beyond what would be contained on the NIR. It is not feasible that the NIR entry would add to that possessed by the Security Services. This leads to a worrying possibility; in order to be of any use whatsoever in combating terrorism, the NIR *must* contain more information. This would need to be of a type that would separate those who present no, or minimal, risk to national security from those who might pose a serious risk. In other words, to be of any use in combating terrorism, data contained on the NIR must be increased in order to allow some degree of profiling and categorisation.

---

<sup>14</sup> Directive 95/46/EC

## **Conclusion**

12. Space considerations preclude anything other than a brief summary of the steps Liberty believes are appropriate to protect privacy against unwarranted surveillance. If the Committee is taking oral evidence we would welcome the opportunity to discuss our observations and conclusions in greater detail. Liberty believes the legislative and regulatory framework has failed to keep pace with surveillance. The HRA offers recourse to individual action which is of limited use in combating mass data processing. As explained above, the DPA is out of date. New data protection legislation is needed to reflect changes in data processing techniques and to properly regulate CCTV. The ICO needs better resourcing and more proactive powers to properly police surveillance. The ICO should also be heavily involved in the drawing up of guidance and good practice in information access and dissemination. The role of Parliament needs to be enhanced by ensuring individual Commissioner's<sup>15</sup> report to parliament rather than to ministers. As details of information access and sharing are typically reserved for secondary legislation, Parliament should be more readily given the power to amend regulation<sup>16</sup>. Privacy impact statements should be introduced to accompany bills. More independent judicial authorisation of interception powers under RIPA are necessary, as is greater oversight and control of communications data access. There should be no further roll out of DNA retention powers. Meanwhile, a presumption in favour of sample destruction should be introduced for those not charged or convicted. These measures will re-introduce proportionality and accountability to surveillance. They require political will but would help counter growing public unease about the extent of the surveillance society.

## **Gareth Crossman, Liberty**

---

<sup>15</sup> The Interception of Communication Commissioner, The Surveillance Commissioner and the National Identity Scheme Commissioner

<sup>16</sup> As has happened in the ID card act in relation to the Information that can be recorded I the NIR