The Royal Academy of Engineering

# The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State

House of Lords Select Committee on the Constitution

June 2007

1. *How has the range and quantity of surveillance and data collection by public and private organisations changed the balance between citizen and state in recent years, whether due to policy developments or technological developments? Which specific forms of surveillance and data collection have the greatest potential impact on this balance?*

1.1 As the capacity to store and search data held electronically continues to grow, so more and more personal data is collected and retained. The balance between citizen and State is affected when that data is collected without citizens' consent or knowledge, when they have no choice to 'opt out' of surveillance, and when data collected for a specific purpose is used in ways the citizen did not foresee.

1.2 The rise of camera surveillance probably has the greatest impact as individuals in public spaces cannot refuse consent for the recording of their image. Often people do not know that a particular area will be under the view of surveillance cameras and they may not be aware of when they are being filmed. The increase in such surveillance means that the 'big brother' State becomes more than just a cliché. Authorities are watching citizens for increasing proportions of their daily lives and citizens have no power to reject such surveillance.

1.3 This imbalance of power between the citizen and the state can be addressed by introducing an element of 'reciprocity' into the surveillance relationship. Reciprocity could be achieved by allowing the public access to detailed information about the siting of cameras. For example, a website could be launched containing maps which indicate the locations of cameras, and sample images from cameras demonstrating their range. This would allow individuals and communities to raise complaints should they feel that particular cameras are unnecessary or excessively intrusive.

1.4 In the private sector, schemes like the Oyster travel card introduced by Transport for London and store loyalty cards involve collection of data about individuals. Although these are voluntary, people would miss out significantly on benefits and convenience if they refuse them or use them anonymously. These technologies and services effectively collect data about peoples' journeys and purchases by stealth, as the user may be unaware that such information is generated when they are used. It is not obvious that a loyalty card designed to attract customers into a store will be used to harvest personal information used in marketing, and it is not clear that the card should have to function in that way.

1.5 People should be able to choose not to give away personal information in the process of 'registering' a loyalty or travel card. This is similar to the choice not to receive further marketing information when signing up for a service. Although there may be some disadvantages in holding a travel or loyalty card anonymously (eg, losing the possibility of retrieving credit on a lost card), the individuals who hold them should be able to choose to take that risk.

1.6 Risks arise when data collect by the private sector is used by the public sector – eg, the police accessing footage from a store's CCTV or examining Oyster card or store card records. The potential merging of private and public data sets – where the former are collected with consent for a specific purpose – should be carefully monitored.

2. *What forms of surveillance and data collection might be considered constitutionally proper or improper? Can the claimed administrative, security or service benefits of such activities outweigh concerns about constitutional propriety? If so, under what circumstances? Is there a line that should not be crossed? If so, how might that line be identified?*

2.1 Surveillance and data collection is constitutionally proper when it is done in the interests of the citizen. For example, the collection, retention and sharing (between appropriate parties) of data about individuals' health is essential for providing proper health care. Notwithstanding the notable difficulties encountered in the NHS's move to electronic patient records, it is right and proper that the health service update the means by which it collects, stores and shares patient information in order to improve the service that the patient receives.

2.2 Similarly, the use of camera surveillance in areas of high crime can be justified if it aids in the conviction of criminals. Thus it can support the police service in fulfilling their duty to protect the public.

2.3 In such cases there is a clear benefit from surveillance and data collection or processing. However, as these benefits diminish they are outweighed by factors of constitutional propriety. Camera surveillance is less beneficial in areas where there is less crime. Although it might seem obvious that increased surveillance prevents crime, evidence for this is low (see Home Office Research Study 292, 'Assessing the Impact of CCTV', by Martin Gill and Angela Spriggs). When blanket surveillance is employed, its benefits are outweighed by the fact that innocent citizens are being watched and are thus experiencing diminished privacy. In such circumstances concerns about constitutional propriety outweigh any claimed benefits.

2.4 In short, surveillance and data collection are acceptable if they bring a clear benefit to members of the public. Collecting data or filming on streets on the basis of the mere 'chance' it will be useful is neither constitutionally proper nor an efficient use of resources. (This point is especially relevant to the National DNA Database, discussed under point 6 below.)

2.5 This is not to say that there is a clear line between effective and beneficial surveillance and 'constitutionally improper' surveillance. The Royal Academy of Engineering's report on this subject was entitled *Dilemmas of Privacy and Surveillance* because the choice between privacy and increased security or convenience often poses a dilemma. In most cases there is a delicate balance to be struck. Therefore, any proposed surveillance system, or any service which involves the collection and processing of personal data, should only be introduced with a clear justification of how its benefits outweigh any limitation it may pose on individuals' privacy.

3. *What effect do public or private sector surveillance and data collection have on a citizen's liberty and privacy? Are there any constitutional rights or principles affected?*

3.1 The UK is a signatory to the UN Declaration of Human Rights and has incorporated the European Convention of Human Rights in UK law. Both of these stipulate that an individual has the right to freedom from interference in their private life, home and correspondence.

3.1 Collecting and retaining information about peoples' everyday movements and activities, when those activities are perfectly law-abiding, should be considered an

infringement on a person's right to privacy. Whether this information is collected by cameras, via the ticketing systems on public transport, or in the course of purchasing everyday goods, a person's right to privacy is infringed unless they have explicitly consented to the collection of data or there is a strong justification in terms of peoples' wellbeing or safety.

4. *What impact do surveillance and data collection have on the character of citizenship in the 21st century, in terms of relations with the State?*

4.1 Increased camera surveillance is employed in order to deter and catch criminals; greater sharing and centralisation of personal information is used to identify fraudsters in the public or private sector. Thus the innocent majority are subject to the same measures as the criminal minority and are treated as potential criminals. The State in effect treats citizens as posing an inherent risk which must be controlled. This shows a lack of trust on behalf on the State in its citizens and is likely to cultivate a reciprocal lack of trust.

4.2 People from minority groups, particularly young black males, are more likely to be the subjects of surveillance. For example, they make up a disproportionate number of the entries on the National DNA Database. There is a danger of such social groups becoming increasingly marginalised, resulting in a breakdown of mutual trust between different minority groups and between those groups and the State.

5. *To what extent are the provisions of the Data Protection Act 1998 sufficient in safeguarding constitutional rights in relation to the collection and use of surveillance or personal data?*

5.1 The Data Protection Act 1998 (DPA) can only safeguard constitutional rights if the Information Commissioner has sufficient power to successfully prevent or punish breaches of the act. Recently it has become possible for custodial sentences to be passed for serious breaches of the DPA - this is a welcome development as it increases the strength of the DPA as a deterrent.

5.2 However, the Information Commissioner can only take action against an organisation if there has been a complaint made against it. It is not possible for the Information Commissioner's Office (ICO) to perform 'spot checks' or audits such as are possible with, for example, environmental health regulations. Without such powers to ensure that individuals and organisations are adhering to the principles in the DPA then the DPA cannot effectively safeguard constitutional rights. In addition, greater clarity over the information that an organisation holds about individuals will make it easier for an individual to check that information and raise a complaints with the ICO if necessary.

6. *Is there a need for any additional constitutional protection of citizens in relation to the collection and use of surveillance material and personal data? If so, what form might such protection take?*

6.1 The DPA makes special concessions for the use of data in the investigation of crimes. However, it is important that the collection and use of personal data for criminal investigations is regulated.

6.2 The National DNA Database is an ever-growing repository of DNA profiles and samples collected from suspects, witnesses and volunteers. The existence and use of this database raises significant questions regarding the rights of those individuals on it. Once a profile is added to the database it is retained, even if collected from a

witness, a volunteer, or a suspect who is cleared of involvement in a crime. These are kept on the basis of the mere chance that they will be useful in future investigations – surely something that the DPA would rule out. DNA profiles can be used to identify family relationships or to predict susceptibility to disease. They therefore constitute sensitive personal information that an individual should have the right to withhold if there is no specific need for it in the investigation or prevention of crime.

6.3 Since the use of personal information in criminal investigations is a quite specific issue, there is an argument for new legislation and the establishment of a new body to oversee the collection, retention and use of bioinformation (including DNA profiles, fingerprints, facial images and so on). This body should have powers to check that records are not kept for excessive periods or without clear justification. Alternatively, the role of the Surveillance Commissioner could be extended to cover the collection, retention and use of bioinformation by the police service.

Submitted by:
Mr Philip Greenish CBE
Chief Executive
The Royal Academy of Engineering

Prepared by:
Dr Natasha McCarthy
Policy Advisor
6th June 2007