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

Response to House of Lords Select Committee on the Constitution

1. Detail of Respondents

Name: Becky Hogge
Responding on behalf of: The Open Rights Group
Address: Open Rights Group, 7th Floor, 101 Grays Inn Road, London WC1X 8TY
Telephone: +44 (0)20 7096 1079
email: becky@openrightsgroup.org

2. Introduction

2.1 New technologies for data collection, data storage and data manipulation appear to offer governments the tantalising opportunity to find out more and more about those they govern. This opportunity has been seized many times over the last few years, in the name of efficiency, economy or security. The resulting armoury of legislation[1] and practice[2] is eye-watering; in effect it legitimises the mass surveillance of UK citizens. This consultation is therefore a timely one and we welcome the opportunity to respond.

---

1 Some recent surveillance state Acts and bills:

- Immigration, Asylum and Nationality Act 2006
  http://www.statutelaw.gov.uk/legResults.aspx?activeTextDocId=2321295
- Terrorism Act 2006
  http://www.statutelaw.gov.uk/legResults.aspx?activeTextDocId=2321013
- Identity Cards Act 2006
  http://www.statutelaw.gov.uk/legResults.aspx?activeTextDocId=2321581
- UK Borders Bill 2007
  http://www.publications.parliament.uk/pa/pabills/200607/uk_borders.htm
- Serious Crime Bill 2007
  http://www.publications.parliament.uk/pa/pabills/200607/serious_crime.htm
- Digital Switchover (Disclosure of Information) Bill 2007
  http://www.publications.parliament.uk/pa/pabills/200607/digital_switchover.htm
- Statistics and Registration Service Bill 2007
  http://www.publications.parliament.uk/pa/pabills/200607/statistics_and_registration_service.htm

2 Public and private practices include:

- RFID-based tracking systems in Passports and Oyster cards
- The monitoring of internet use through search engine and ISP logs
- Police National DNA database
- Fingerprinting practices in crime preventaion and school identification systems
- CCTV
- Number-plate recognition systems (National Vehicle Tracking System, London Congestion Charge)
- Facial recognition cameras
- NHS Care Records Service
- The Children's Index
- NpfIT (NHS data spine)

3. The Impact of Surveillance

3.1 Pervasive surveillance degrades human dignity. The erosion of privacy - a fundamental human right - that such surveillance represents is neither proportionate to its stated aims nor wholly legitimate according to the purpose it serves.

3.2 When data gathering becomes routine and automatic, but when the protections afforded those data are uncertain and the purposes to which they might be put unclear, the relationship between citizen and state changes fundamentally. Citizens are no longer aware when their privacy is being breached, for what reason or purpose, and must therefore assume they are under a constant "watch"[3]. This is highly likely to alter their behaviour over time.

3.3 For example, faced with this threat, those who engage in unpopular practices (activities often considered most protected: religious, sexual, political) effectively lose the right to hold their viewpoint or to act in a manner theoretically protected by law, because they cannot be sure their personal information will not be leaked by contractors or corrupt civil servants, or indeed simply published through incompetence.

3.4 Further, surveillance has the potential to undermine the work of communities, transferring the responsibility to "look out for each other" to a centralised, faceless, database state. This loss of local control in favour of central control leads to alienation and, in turn the demand for a more "disciplinary" society, led from the centre.

4. Constitutional Protections

4.1 In theory, the Data Protection Act, grounded in the right to privacy, should go some way towards protecting UK society from these outcomes. But in practice, its enforcement record is weak and there are currently no effective criminal sanctions for its breach.

4.2 When banks dump personal data in outdoor rubbish bins, in direct contravention of the Act, their punishment is to sign a form saying they won't do it again[4]. When the identities of staff at Network Rail and the Department of Work and Pensions are stolen from a compromised HMRC portal to defraud the tax credit scheme, HMRC escapes unpunished[5][6].

4.3 Indeed, it may be true that constitutionally, the UK is protected from the threats of a surveillance state. But unless these protections are enforced, they are meaningless.

---

3 See McCullagh, Karen (April 2005) "Identity information: the tension between privacy and the societal benefits associated with biometric database surveillance", *20th BILETA Conference: Over-Commoditised; Over-Centralised; Over-Observed: the New Digital Legal World?*

4 Press Association, 13 March 2007 "Banks 'dumped personal information in bins'", http://money.guardian.co.uk/saving/banks/story/0,,2032962,00.html

5 The Register, 18 January 2006, "HMRC tax debacle spreads", http://www.theregister.co.uk/2006/01/18/hmrc_tax_debacle/

6 An register of "UK Privacy Debacles" is maintained by the Open Rights Group community at http://www.openrightsgroup.org/orgwiki/index.php/UK_Privacy_Debacles

5. About the Open Rights Group

5.1 The Open Rights Group is a grassroots digital rights advocacy group based in the UK. It aims to increase awareness of digital rights issues, help foster grassroots activity and preserve civil liberties in the digital age. It is funded by individual donations and small grants.