

A Surveillance Society:

Executive Summary of Qualitative Research

Prepared for:



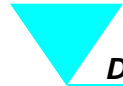
On behalf of:



Prepared by:

Oliver Murphy

**Project No: A4428
15th November 2007**



EXECUTIVE SUMMARY

BACKGROUND & OBJECTIVES

The Information Commissioner's Office (ICO) wanted to explore and understand public awareness and perceptions of the various forms of surveillance in society, which can be defined as involving 'gathering, recording, processing, monitoring, analysing, sorting and flow of personal information, movements, lifestyle habits and behaviours', including in particular the less obvious 'electronic footprints'. Qualitative research was commissioned to explore, with a cross-section of the general public, what they feel are the effects of surveillance on their privacy, society, levels of choice, power and empowerment. The study also set out to understand what safeguards the public feel might be necessary to control any perceived risks.

The research is intended to contribute further to the public debate on the surveillance society and it is envisaged that other end users such as parliamentary committees, undertaking current enquiries into the surveillance society, may also utilise the results of this research.

METHODOLOGY & SAMPLE

The study was conducted via a series of 12 discussion groups. These lasted for two hours each and comprised six respondents. The groups were held across the UK in London, Birmingham, Doncaster, Cardiff, Glasgow and Belfast, and were segmented by age/lifestage and socio-economic grade. There was a mix of men and women in each group, and all respondents were recruited to be exposed to a range of types of surveillance to a greater or lesser extent, such as internet purchasing, using Bluetooth mobile phones, using a loyalty card etc.

In addition to the group discussions, all respondents completed a two-stage pre-task. At the point of recruitment, they were asked for their spontaneous feelings, including any concerns, about their personal details and activities being recorded and collected. This was to help the research team understand respondents' views on this area before they began to be 'educated' by the research process. Respondents were then required to complete a week's diary, recording any occasions when they thought they or their details were being recorded. This was to ensure respondents had given some thought to the subject matter before attending the group discussions, ensuring a more fruitful debate.

SUMMARY OF FINDINGS

1. It is worth noting that respondents did not view all the types of data collection under discussion as ‘surveillance’. Indeed ‘surveillance’ was largely thought of as referring to active ‘watching’ of our activities (mainly CCTV, but also including person-based observation/checks such as bag searches or door security staff, and some monitoring of our electronic activity by both the state and employers). The types of ‘data collection’ about whose use most concerns were expressed (mostly commercial activities) were not really thought of as ‘surveillance’.
2. Broadly speaking, the majority of our sample was not unduly worried about ‘pure’ surveillance or data gathering. Indeed, data collecting and trawling by the security services/police was thought to be appropriate, seen as necessary in an evermore dangerous and crime-ridden world, and could even go further (e.g. compulsory fingerprint/DNA databases for all) to bring about a safer society.
3. For most, spontaneous concern was largely confined to the activities of commercial organisations and to a fear of ID fraud.
 - a. The collection and use of data by commercial organisations was a source of irritation and concern to many respondents, in large part, because people believed that the sharing/selling on of data within and between companies, leads to cold-calling, direct mail and sales emails/spam. These uninvited intrusions, often by unknown companies, into their private life were highly resented, and created a sense of unease about the amount of information held about them *in toto* by commercial and other organisations. Some were able to imagine an extreme scenario where these bodies ‘join up’ the information they hold, thus, to our respondents’ eyes, reducing them to pieces of (impartial) data and robbing them of their individuality.
 - b. ID fraud was seen as a lurking menace, with concerns fuelled by commercial and state warnings, but also often backed up by personal experiences or tales of friends/family. The potential consequences of such fraud were very frightening and yet many people felt there was very little they could do to guard against it. Aspects of the collection and use of data were thought to increase the risk of ID fraud; in particular, there was a perception that the more companies that have access to your personal data, the greater is the risk of fraud, either due to the actions of criminal individuals or carelessness over the communication/storage/disposal of such data.

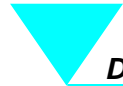
4. Lack of serious concern, among the majority of our sample, about surveillance and data gathering activity was due to a number of beliefs (rational and emotional):
 - i. national security (i.e. preventing terrorism) and personal security (i.e. fighting crime) are of over-riding importance – the common good is paramount;
 - ii. we live in a stable and accountable democracy (not Darfur, Myanmar etc.) so it is ridiculous for us to worry about such issues;
 - iii. the state and security forces are not institutionally malign or corrupt in intent; indeed they are there to protect us, the innocent citizen;
 - iv. the innocent will not be harmed or inconvenienced (or at least, not for long, and this is a price worth paying for the common good);
 - v. only the guilty are actively being watched, so I, as an innocent citizen, will not be ‘picked out of the crowd’ and if I am then I have nothing to hide;
 - vi. sharing personal data is the new norm; we increasingly live in a world where people are used to sharing personal details, and making connections, with complete strangers, particularly through the internet. The value of privacy appears to be decreasing as more and more people enjoy the benefits of social networking and so it becomes increasingly difficult to draw the line between data you choose to share, and data that others might hold about you over which you have little or no control;
 - vii. commercial data collection is the price of modern convenience; for example it helps to speed up our purchasing online;
 - viii. commercial data holding brings benefits to me personally and works on the basis of a reasonable exchange e.g. I save money on my purchases with my loyalty card, and in return they are able to know what I buy etc;
 - ix. someone, somewhere, will be looking after our best interests. There was an assumption that there ‘must be’ laws against extreme abuse of data, although respondents tended to be rather vague about who or what this might be, and no one was able to name the ICO (although there were some spontaneous mentions of the Data Protection Act); and
 - x. I can’t do anything about it anyway. Many, even if they did express some concern, felt powerless to act or to know how they could do anything to tackle/dispel their worries. Many were often unaware of, or at least had given very little thought to, the myriad forms of surveillance/data collection they are subject to and its potential uses. Although they might

have felt uneasy about the data that is gathered about them, most fell back on the assumption that there's 'probably' nothing to worry about (for all the reasons listed above). Ultimately with no organisation, or voice, expressing a strong counter-argument, as individuals they felt there was little point in worrying about these things, and little they could do to change the 'drift' towards shared data and observation.

5. Across the sample, respondents struggled to identify what safeguards they might want or expect, in part because of lack of awareness of how data is being gathered and used. The requests that did emerge were aimed at the two key areas of concern:
 - a. identity fraud: thought to be difficult to legislate against because seen often as the result of individual criminal activity, but there was a desire to see rules tightened about data sharing between companies in order to cut down on opportunities for fraud; and
 - b. commercial data abuse: e.g. tighter rules about data opt-outs on forms, greater transparency about commercial data sharing, rules and penalties on holding data.

There was also some interest in greater public information/education on new technologies, such as Bluetooth and social networking, especially for parents who were often worried about their children's use of such channels, but felt they didn't know enough to understand whether their children were really at risk, or what they could be doing about it.

6. There was a minority who expressed objections to, or greater discomfort with, surveillance, particularly state forms of surveillance and data gathering, although they were unhappy about commercial activities too. This part of the sample were considerably more sceptical about the intentions of the police and security forces and expressed unease about the access they are or might be granted to our personal data. Such respondents also raised some principled objections to the 'drift' towards increasing state-control of our personal information, along the following lines:
 - i. that it runs counter to our tradition and to the principles of a democratic society that citizens should be 'monitored' to such a degree, and that so much information about us should be available to government institutions and police/security forces;
 - ii. that it does not reflect well on us as a society that we feel a need to resort to CCTV and other forms of surveillance in order to feel 'safe';
 - iii. indeed, that this is not the way we should be going about tackling the problem of crime; some individuals raised doubts over whether CCTV is really that effective in preventing crime anyway, while others felt that



it is the (social) causes behind crime that should be the focus of our attention; and

- iv. that many of the forms of state data gathering and surveillance that we discussed work on the principle that you are guilty until you provide the personal data (for example fingerprints) to prove your innocence.
7. There is little doubt that, despite widespread acceptance of the status quo, any future surveillance or data ‘disasters’ will cause most citizens to wonder ‘why nothing was done to prevent it’. Faith in government and industry rules and regulations is not total and the anonymous ‘some-one who is looking after us’ will have been expected to have foreseen the problems and to have taken action to avoid them.