

**INFORMATION
COMMISSIONER'S OFFICE**

**PUBLIC ATTITUDES
TO THE DEPLOYMENT
OF SURVEILLANCE TECHNIQUES
IN PUBLIC PLACES**

Qualitative Research Report

Prepared for:

**Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF**

Prepared by:

**Sharpe Research Ltd
7 Broadhinton Road
London
SW4 0LU
020 7627 3143
*sharpe.research@btinternet.com***

March 2004

CONTENTS

| | Page No. |
|---|-----------------|
| INTRODUCTION | 1 |
| Background | 1 |
| Research objectives | 3 |
| Method and sample | 4 |
| SUMMARY AND CONCLUSIONS | 7 |
| MAIN FINDINGS | 13 |
| 1 CCTV experiences and attitudes | 13 |
| 1.1 Awareness and knowledge | 13 |
| 1.2 Personal involvement with CCTV | 15 |
| 1.3 Perceived purpose of CCTV | 16 |
| 1.4 Perceived effectiveness of CCTV in combating crime | 19 |
| 1.5 Attitudes towards CCTV surveillance | 22 |
| 1.6 CCTV regulation | 24 |
| 2 Personal privacy | 27 |
| 3 Other surveillance technologies | 28 |
| 3.1 Infra-red | 28 |
| 3.2 Microphones | 28 |
| 3.3 Facial Recognition Software (FRS) | 29 |
| 3.4 Speed cameras | 30 |
| 3.5 Road pricing – satellite vehicle tracking | 32 |
| 3.6 Radio Frequency Identification (RFID) | 33 |
| 3.7 Millimetre wave imaging (T-rays) | 34 |
| 3.8 Camera phones | 36 |
| 3.9 Iris biometrics recognition | 36 |
| 4 Data protection | 37 |
| 4.1 Experience and knowledge | 37 |
| 4.2 Data protection Principles | 39 |

CONTENTS contd.

| | Page No. |
|--|-----------------|
| 5 Response to Scenarios | 43 |
| 5.1 Scenario 1 | 43 |
| 5.2 Scenario 2 | 44 |
| 5.3 Scenario 3 | 45 |
| 5.4 Scenario 4 | 47 |
| 5.5 Scenario 5 | 48 |
| 5.6 Scenario 6 | 50 |
| 5.7 Scenario 8 | 52 |
| 5.8 Scenario 9 | 53 |
| 5.9 Scenario 10 | 54 |
| 5.10 Scenario 11 | 55 |
| 6 Post-deliberative views on surveillance | 56 |
| 6.1 Misuse of CCTV | 56 |
| 6.2 Surveillance acceptability | 58 |
| 6.3 Desired rules for surveillance | 60 |
| 6.4 Data linkages | 65 |
| 7 Young people | 66 |
| APPENDICES | |
| I Discussion Guides | |
| II Scenarios | |

INTRODUCTION

BACKGROUND

Britain has the densest CCTV coverage of public places anywhere in the world. A recent estimate puts the number of CCTV cameras in Britain at 2.5 million – 10% of the world's total. In part, this is because the Home Office has made funding for CCTV systems available on a considerable scale, as a crime prevention measure for public spaces such as town centres, shopping malls and housing estates.

Previous research indicated a high level of public support for CCTV, but had not attempted to investigate the limits of public tolerance, nor the specific factors that might in the future undermine public confidence as video surveillance technologies and potential usages change.

In 2000 the Office of the Information Commissioner published a Code of Practice on CCTV. Technological developments in public surveillance argued that the time might now be ripe to update the Code.

New technologies already in place include:

- speed cameras with automatic number plate recognition (ANPR)
- London Congestion Charge enforcement cameras, also with ANPR
- other roadside traffic safety enforcement cameras with ANPR, including at traffic lights and to keep bus lanes clear
- Facial Recognition software, whereby the images of individuals captured by CCTV can be identified by matching them against an existing database

Technologies in existence but not yet in common use include:

- Microphones fitted to CCTV cameras
- Radio Frequency ID microchips, developed as the eventual successor to barcode inventory tracking systems
- Millimetre Wave Imaging (T-rays) which produces images derived from passive radiation from the human body, and shows whether items like weapons are hidden under clothing. The effect is that the image looks as though the person has no clothes on.

The Information Commissioner wished to gain a better understanding of public attitudes towards the increasing range of surveillance activities being carried out in public spaces, in order to:

- guide the revision of the CCTV Code of Practice, so that it would reflect real issues of public concern
- contribute to the public debate on balancing individuals' rights of privacy with public safety and protection
- comment on government road pricing initiatives for satellite technology to track the movement of vehicles

In order to fill gaps in knowledge and understanding, research among well-informed members of the general public, was required to seek opinions on these issues.

Sharpe Research Ltd was invited by the Information Commissioner's Office to conduct a programme of qualitative research that would fulfil these aims.

The findings of this research were presented verbally to ICO officials at their offices on 24th March 2004. This report documents the findings in more detail.

RESEARCH OBJECTIVES

The main aim of the research was to investigate informed public attitudes towards current and planned public surveillance activities, and establish the limits of public acceptability and confidence, to provide understanding of where the boundary might lie between personal privacy and society's ability to intrude into an individual's affairs. This involved investigation of the following:

- levels of spontaneous knowledge and awareness about:
 - the extent and prevalence of CCTV and other surveillance technologies
 - the purposes for which video surveillance is deployed
 - which authorities and other organisations use video surveillance
 - how the recordings are used or processed
 - how long recordings are kept
 - who can see them, and in what circumstances
 - the effectiveness of video surveillance in preventing and/or detecting crime
- sources of knowledge and awareness, including personal experience;
- reactions to prompted information on
 - licensing/authorisation
 - covert vs. overt installations
 - new surveillance technologies
 - new 'purposes', such as road pricing
 - 'sensitive' personal data, in the data protection context
- factors underlying public confidence in video surveillance;
- the perceived applicability of the 8 data protection principles to the deployment and use of surveillance technology;
- perceived risks of unlawful or criminal violations of privacy arising from video surveillance, looking both at likelihood and potential severity of consequences to the individual;
- what rules ought to control the deployment and use of video surveillance in public places, and who should set and enforce those rules;
- information needs – what members of the public want to know about video surveillance and its regulation.

METHOD AND SAMPLE

Technique

Qualitative techniques of data collection, using unstructured interviewing, were adopted to fulfil the exploratory and deliberative objectives of the research.

A series of ten group discussions was carried out altogether, over the period 22nd January to 11th March 2004.

Most of these (8) were conducted as reconvened focus groups; respondents were invited to take part in a normal group discussion one evening, and then return a week later for a second discussion, having read, considered and deliberated on information introduced at the first session.

A series of 10 Scenarios were developed for the research, designed to illustrate different ways in which video surveillance might be misused. These were fictional stories, but based on actual cases in Britain or elsewhere – copies will be found in the Appendix to this report. Four of the Scenarios were selected for each group, randomly across the sample.

For the reconvened groups, respondents were given copies of the four Scenarios to take away to read and think about between the two research sessions, plus a copy of the 8 data protection principles of good information handling. Respondents' reactions to the Scenarios were then obtained during the second, reconvened research session.

The additional two groups, with young men from ethnic minority communities, were convened as extended 3-hour workshops. With these, copies of the relevant Scenarios were given to respondents to read during a break in the middle of the research session, and reactions obtained during the second half.

Discussions in both cases followed the sequence of topics set down in the Discussion Guides prepared for the study. Copies for Stage I and the reconvened Stage II are appended.

Proceedings of all the research sessions were tape-recorded for subsequent analysis and reference, with respondents' knowledge and agreement. Only first names were used for recording purposes, to protect anonymity. This report makes extensive use of verbatim quotes from the tapes, to illustrate how respondents spoke and felt.

Sample

The main sample of eight reconvened groups was structured fairly conventionally by demographics, to cover the whole adult population.

The additional two extended workshops, with young men from ethnic minority communities, were recommended to shed light on the views and experiences of a section of the population which is often the focus of crime prevention and detection activities, as perpetrators or as victims – regardless of ethnicity. Previous research indicated, however, that the reconvened group technique works least well with young people, because of reluctance to engage with the research topics during the intervening week between the two discussion sessions – hence the decision to opt for single, but extended sessions.

The final sample design was as follows:

| | | | | |
|-----------------|---------------------------|-------------|-------|------------|
| Group 1 | Male, singles | 18-24 years | C2DE | Suburban |
| Group 2 | Female, singles | 18-24 years | ABC1 | Large town |
| Group 3 | Male, young families | 21-40 years | ABC1 | Small town |
| Group 4 | Female, young families | 21-40 years | C2DE | Inner city |
| Group 5 | Male, older families | 35-54 years | C2DE | Inner city |
| Group 6 | Female, older families | 35-54 years | ABC1 | Suburban |
| Group 7 | Male, empty nesters | 50-75 years | ABC1 | Large town |
| Group 8 | Female, empty nesters | 50-75 years | C2DE | Small town |
| Group 9 | Young men, Asian | 18-28 years | C1C2D | Inner city |
| Group 10 | Young men, Afro-Caribbean | 18-28 years | C1C2D | Inner city |

Locations referred to in the Table were selected to represent a range of different types of neighbourhood, and geographical areas. These were as follows:

Inner city – Lewisham, South-east London
Asian young men – central Birmingham

Suburban – Sale, Greater Manchester

Large town – Leamington, Warwickshire

Small town – St Austell, Cornwall

Respondent recruitment was carried out with the aid of a structured questionnaire, designed to check eligibility. As well as establishing the correct demographics, the questionnaire sought to:

- exclude people with occupations that might give them special knowledge of surveillance – including police, Customs and Excise and retail, and members of Liberty (NCCL) – in addition to the usual marketing, market research, journalism and PR exclusions
- ensure some level of newspaper readership, national or local, to fulfil the sampling criterion of ‘well-informed’

Recruitment was subcontracted to Jill Lonsdale Research Services, fieldwork specialists with a network of trained and experienced recruiters nationwide, working to the direction of Sharpe Research.

The main sample of reconvened groups in Lewisham, Sale and Leamington (but not St Austell) included members of ethnic minority communities as well as white respondents, to check for any major differences in response among demographic groups other than young men.

SUMMARY AND CONCLUSIONS

The ubiquitous presence of CCTV cameras in the streets and town centres across much of Britain is widely accepted as a fact of modern life, and welcomed by many.

Everyone seems aware of CCTV, though few have had any close involvement in terms of aftermath to having been filmed.

CCTV is universally perceived as an anti-crime measure, helping both to deter criminal and anti-social behaviour, and to catch the perpetrators. People generally claim they feel safer where CCTV is installed, and express unquestioning faith in its crime prevention effectiveness.

CCTV seems mostly to be judged in the context of violent attacks against innocent passers-by – mugging and robbery. While its use in combating property crime is readily acknowledged – shoplifting, vandalism, theft from commercial premises – crime against the person is what counts in people's estimation of the legitimacy of CCTV in public places. They feel it gives them protection.

CCTV is therefore reckoned to offer great personal benefit to the individual, with few if any disadvantages that people are conscious of, and this largely accounts for popular support and confidence.

Another relevant factor in public support for CCTV is trust in authority. People frequently quote the maxim 'innocent until proved guilty', and genuinely believe that this prevails in the British system of law enforcement and criminal justice. They expect citizens to be fairly and benignly treated.

The main problem with CCTV arising from personal experience is with poor quality images, which frustrate the purpose of identifying individuals shown on camera to have committed crimes. This can also lead to 'false positives', whereby innocent individuals are apprehended. Despite occasional personal awareness of such cases, however, support for CCTV remains strong.

Even when the potential for misuse of surveillance images is drawn to people's attention, they still tend to fall back on their own experience, which tells them that in real life the risks arising from CCTV are small, whereas the potential benefits are seen as very great.

This research focused mainly on CCTV, as the form of surveillance people are most likely to be familiar with and thus have views about. However, discussion about some other surveillance technologies introduced in the research reveals that when the perceived balance of personal advantage tips the other way, support weakens. With satellite vehicle tracking, for example, and Radio Frequency ID and T-rays, the potential disadvantages to the individual are seen as considerable, whereas the personal benefits may be negligible. This even applies to speed cameras, in some minds.

These perceived disadvantages consist mainly of invasions of personal privacy – widely agreed to be a universal human right. At a spontaneous level, privacy is mainly associated with people's homes, but further discussion shows that conversations, financial information and people's whereabouts are covered too by the notion of privacy. There is also a sense of the protection of personal dignity and personal integrity in many people's understanding of personal privacy.

CCTV is not generally considered to intrude on personal privacy. This may be because individuals expect to be seen when out and about in public places, and they behave and dress accordingly. They are already 'on show', as it were. Being watched by a camera does not appear very different from being looked at by passers-by.

Many also claim to have a choice over whether to submit themselves to CCTV scrutiny, and that CCTV objectors have a similar choice. This offers a degree of personal control, which also gives confidence. Providing that there are clear warning signs about the presence of cameras, most people become consciously complicit in surveillance in public places.

The limits to public acceptability of surveillance thus exclude measures which:

- fail to offer protection to individuals and their personal safety
- invade personal space
- intrude into private homes
- incriminate innocent people
- lead to innocent people being treated as criminals
- lay people open to the possibility of fraud, through access to their financial details

While people's own experience of CCTV does not generally demonstrate any breaches of these limits, this seems less certain with some of the other, newer surveillance technologies discussed in this research.

The idea of data linkage – being able to connect personal data about individuals, including images, from different sources – has not occurred to most people. In the context of the projected introduction of ID cards for all citizens, data linkage does not appear very threatening. Linking between different types of personal record is believed to be possible already, with no obvious adverse effects. In fact many welcome the thought of ID cards, as incontrovertible proof of identity. Again, this may reflect most people's evident trust in authority.

The state is one thing, however, and commercial organisations are quite another. Surveillance for purely commercial purposes – specifically marketing and promotion – is rejected, and this applies to data linkages too. The main reason is that the crucial condition for acceptance of surveillance, ie. the protection of personal safety, is unmet.

Resistance to CCTV is found mostly among young people. This may be because they have an imperfect grasp of the narrow crime-prevention purpose of CCTV, and/or exaggerate its technical capability and power. Surveillance therefore seems to be capable of abuse, in terms of unjustified harassment – especially to those from minority communities. Even among young people, however, objectors appear relatively infrequent.

On the whole, the eight Data Protection Principles of good information handling are felt to deal adequately with the instances of surveillance misuse featured in the Scenarios prepared for deliberation in this research. If the Principles had been adhered to, it is generally concluded that the misuse would not have happened.

The fact that surveillance images count as ‘personal information’, and are therefore covered by Data Protection law, comes as a new thought to many, and this discovery is reassuring. The basic concept of data protection – keeping personal details confidential – seems familiar to all, and is broadly deemed to be a good thing. Awareness of the right of subject access seems quite widespread. Detailed knowledge of other aspects is slight, however.

Similarly, levels of knowledge are low about the regulation of CCTV and indeed other surveillance technologies. While the public generally takes it on trust that there must be some form of regulation, many would be interested and reassured to know more.

Following deliberation on the Scenarios, a number of desired rules emerge by which people believe the use of surveillance, including CCTV, should be regulated:

- | | |
|-------------------------------|--|
| Clear signs | Unless there are signs, potential wrong-doers or criminals are unlikely to be deterred, or indeed caught afterwards – thus frustrating the main purpose of surveillance. |
| Quality of images | Poor quality images similarly counteract the crime-prevention purpose of surveillance, if they are unable correctly to identify the perpetrators. |
| Corroboration evidence | The possibility of surveillance images leading to mis-identification or incrimination of innocent individuals means that additional evidence of wrongdoing should be required before suspects are apprehended. |
| Security of images | Surveillance images should be proof against theft, tampering and unauthorised disclosure. (However, the term ‘secure’ does not convey the concept with sufficient clarity or force, in many cases.) |
| Operators | Operators of CCTV and other surveillance equipment should be carefully selected, trained and supervised, so that personal privacy is protected. CRB or equivalent reference is sometimes recommended. |
| Disclosure | Consent should always be obtained from the people concerned for showing personal images, especially for a purpose other than why they were recorded. |
| Redress | Individuals harmed by misuse of surveillance information should be able to complain and/or obtain compensation – signs should explain how to go about the process. |

In all of these cases except the requirement for corroboration, the ICO's current CCTV Code of Practice seems to cover these rules, though not necessarily in so many words. However, the evidence of this research indicates that stronger enforcement may be required to ensure fuller compliance.

Looking to the future, it seems likely that popular support for CCTV and other surveillance technologies would only be undermined if the perceived balance of personal advantage were to swing away from the ordinary individual citizen and the protection of personal safety.

If, for example, stories were to gain currency about the ineffectiveness of surveillance in preventing or solving crime, specifically violent crime, then confidence might start to waver. Breaches of personal privacy or other instances of unfairness or misuse of personal images would have a similar damaging effect. Young people might be especially susceptible, given their generally weaker faith in the benefits of surveillance and in the wider authority of the state.

The Information Commissioner's role is primarily to ensure that the Data Protection Principles apply in detail to the operation of surveillance in public places, and are seen to be properly and wholeheartedly enforced.

MAIN FINDINGS

1 CCTV experiences and attitudes

While this research was concerned with surveillance technologies of all kinds, CCTV formed the main centrepiece of discussion, since it is the most prevalent, well-established and well-known.

1.1 Awareness and knowledge

Everyone in the sample was aware of and familiar with CCTV from their own experience, locally and elsewhere, and was largely taken for granted. CCTV was said to be “*everywhere*”.

*“They are all over the place, aren’t they”... “In the shops and in the streets”...
“They put them on the housing estates now too, don’t they, on great big massive poles.
Like the lamp posts but really tall.”*

[Women with young children, 21-40 yrs, C2DE, Inner city]

“High street, inside shops, outside shops, everywhere – spy cameras.”

[Men with young children, 21-40 yrs, ABC1, Small town]

All appeared to know that the initials stood for Closed Circuit Television, and referred to CCTV freely during the discussions.

Town centre streets and shopping centres were mentioned most frequently, but a wide range of other places where CCTV could be found also included:

- inside shops
- banks, ATMs
- commercial premises
- hospitals
- schools
- garage forecourts
- car parks
- airports
- bus stations, railway stations
- parks
- clubs, bars, pubs – outside and inside

A few mentions were made of CCTV at work, but this was usually in the anti-theft context of shops and bars, rather than monitoring of employee productivity – which was in any case outside the main focus of this research on surveillance in public places.

There were references to CCTV installations in people's homes, though these seemed to be based mainly on supposition rather than first-hand knowledge and experience of specific instances. Nevertheless some respondents were adamant that domestic CCTV systems could be bought quite cheaply on the high street.

“You can buy them yourself from Argos and Homebase”... “You can fix them and watch them on your telly”... “Say you are watching EastEnders and someone steps onto your property, it will turn the channel onto the security channel and you can see who is outside.”

[Women with young children, 21-40 yrs, C2DE, Inner city]

CCTV images on television programmes were widely familiar.

“I think we became more aware of it when we saw it on television through mostly police reporting”... “That’s what it brings home to you. You don’t realise that it’s there.”

[Older men 50-75yrs, ABC1, Large town]

In addition to *Crimewatch*, which had perhaps the most serious purpose, other programmes in a more overtly entertainment vein included *Police, Camera, Action* – sometimes regarded with a degree of cynicism.

“They make programmes out of CCTV on the telly almost every night... Someone is making money out of the telly programmes, aren’t they.”

[Men with older children, 35-54 yrs, Inner city]

In fact, television news footage of the murdered toddler Jamie Bulger was often mentioned as many people's earliest recollection of CCTV.

1.2 Personal involvement with CCTV

While most people's experiences of CCTV were entirely passive, a few had been personally involved.

For example, one man in south London reported having been picked up by the police while shopping in the high street, on account of his resemblance to the CCTV image of an armed robber. Although the situation took some time to resolve, he expressed himself still much in favour of CCTV.

"I was arrested because I looked like someone on the CCTV camera and it wasn't me... They actually took a photograph of my face and matched it against the person on the CCTV camera... It went on for about 8 weeks... I was taken to the police station and held there for nearly 13 hours. It was quite a serious charge but it wasn't me; I was at work at the time of the incident... They said 'Your description fits an armed robbery'. And that was it; I was taken away – no ifs, buts or maybes. I was thrown in the back of a van because I fitted the description of the person, and because I had a criminal record from 15 years ago... I was angry at the time, but when I sat down and thought about it, it obviously took an armed robber off the street, didn't it."

[Men with older children, 35-54 yrs, C2DE, Inner city]

In Greater Manchester, the teenage son of a friend of one respondent had recently been attacked at a Metrolink station, but no assailants were brought to book. This not only exposed the inadequacy of Metrolink's much vaunted CCTV coverage, but betrayed passengers' trust in Metrolink to protect their safety. The story had been well aired in the local press.

The son of another respondent had recently been robbed of his bicycle, and was waiting for an appointment at the local police station to view CCTV footage of the surrounding streets, to see whether he could identify the thief.

One or two younger respondents knew of acquaintances convicted on CCTV evidence – mostly for fighting.

"To be honest, I really don't know where any cameras are... The only people I'm told by where the cameras are, are people I know who have been in fights I have been told they have caught on camera."

[Young women 18-24 yrs, no children, ABC1, Large town]

Talking about speed cameras brought forth a few admissions of having been caught speeding from some men in the sample, and at least one case of bus lane violation.

1.3 Perceived purpose of CCTV

Respondents were very clear in their minds that CCTV was there because of crime.

“I think they can be as a deterrent to crimes and things like that and quite useful... Nowadays like today on TV you watch these fights on the street and things like that, and people aware of the cameras probably to stop them from having these fights and things. So it could be a positive thing.”

[Men with older children, 35-54 yrs, C2DE, Inner city]

Although they mostly spoke first about preventing crime, they did not seem to distinguish between prevention and detection – perhaps because detection was assumed to be a means to the end: prevention.

Personal safety and security were uppermost in their priorities.

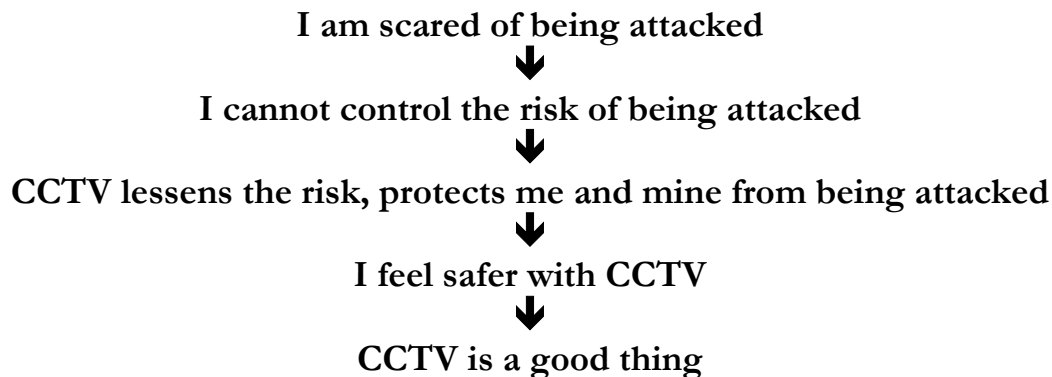
“Ten years back you’d walk along with your bag clutched, holding onto your bag, sort of hearing anyone coming up and taking it. I can walk down there now and not have to bother or worry so much. If something happens I know, hopefully, someone’s watching.”

[Older women 50-75yrs, C2DE, Small town]

“I don’t really care about shoplifters; it doesn’t really affect me whether people steal from shops or not. What I want from CCTV is better security for me.”

[Young women 18-24 yrs, no children, ABC1, large town]

The argument for most people seemed to go like this:



Women and older people especially were frightened of the increasingly “terrifying” behaviour of mostly young people on the streets these days, and CCTV served as some kind of reassurance of their personal safety and security.

“The country has got no safer, has it. As I have got older I have felt a lot unsafer on the streets. When I was 14, 15 and 16 I felt a lot safer from now. You never heard of kids being mugged and all that when I was 16 – having their phones nicked on buses, and people being mugged”... “There is more violent crime”... “Criminals are aware of these CCTVs being there, so they will think twice before they commit a crime.”

[Men with older children, 35-54 yrs, Inner city]

CCTV was also aimed at protecting property, it was recognised – including both goods and commercial premises. Shoplifting was mentioned repeatedly, probably because cameras in stores were so ubiquitous – at the insistence of insurance companies, it was sometimes claimed. Theft and vandalism both came under the heading of protecting property too.

There were a few mentions of other kinds of anti-social behaviour being deterred by CCTV – not only fighting and drug-dealing, but also noise and nuisance such as dumping rubbish on the streets.

All of these purposes were seen as legitimate, but being protected against violent assault was the most powerful justification of CCTV for everyone.

“The main objective’s security”... “It makes you feel safer if you know that you’ve got somebody watching, in case you might get mugged, or your bag lifted.”

[Older men 50-75yrs, ABC1, Large town]

Many respondents had concluded that the growing use of CCTV was to substitute for ‘bobbies on the beat’, and regretted the reduction in police presence in public places.

“They should stop spending the money on the high tech and start spending it on the bobby, you know. If they started paying the bobbies £30,000 a year then you would get thousands of bobbies, and they will do their job properly.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

“I think what’s missing now in our society is the policeman on the beat. Years ago I would walk around in the evenings. I had to go to night classes and come home late at night on the last bus. I wouldn’t dare do it now... In the town you would see one or two of them just walking about. To me it’s like a friend walking by.”

[Older women 50-75yrs, C2DE, Small town]

CCTV as a method of social control was barely mentioned – keeping undesirables off the streets and away from public places. This did not seem to have occurred spontaneously even to the young people in the sample, who were most antipathetic to CCTV (see Section 7 below).

1.4 Perceived effectiveness of CCTV in combating crime

There was a general unquestioning assumption that CCTV works. Proof was felt to lie partly in its prevalence – if CCTV did not work, surely there would be less around. Also, while claims in the media of the positive effect of CCTV on crime rates could be recalled, no-one was able to cite stories making the opposite case.

“It was in the (local paper) last week on the front page, that it had reduced crime, to a certain extent”... “I think it’s very good, really. They do pick up a lot with that, don’t they.”

[Older women 50-75yrs, C2DE, Small town]

People without personal involvement were more likely to believe that CCTV works.

Thinking more deeply about effectiveness, the main exception made was with those high on drink or drugs, who would not be deterred by CCTV cameras because they would not even be conscious of their presence, signs or no signs.

“We all go to the cashpoint machines: you might to the cash machine at ten o’clock at night, you know there’s cameras on the parade, you’re less likely to be attacked by somebody because they’ll know they’re on camera. They might still attack you if they’re on drugs or something, but they’re less likely to do it because they’re on camera.”

[Older men 50-75yrs, ABC1, Large town]

“I don’t think it’s really going to deter crime, because most of the people have lost their senses because they’re drunk. They’re not really going to think, ‘Oh, there’s a camera, I’m not going to beat this person up’; they’re just going to do it.”

[Asian young men 18-28 yrs, Inner city]

Habitual criminals, who knew where cameras were sited, might take avoiding action by covering their faces, or by going round the corner out of sight.

But these examples of ineffectiveness tended to be taken as exceptions that proved the rule – especially as far as unplanned, opportunistic attacks against individuals were concerned, which most worried people.

“I think the cameras stop last minute thinking crimes.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

Another problem with CCTV – readily apparent from CCTV images shown on television, and sometimes from personal involvement – was that the images might not be up to the job for identification of criminals.

“You see the ones in the banks and they’re all like, you know, on Crimewatch or something and it’s like, ‘Who’s this guy?’. It’s just a blurred mess... I’ve seen them on the Met station as well – because a friend got attacked on the Met station just recently and there was a group of about seven lads and he couldn’t make out one of them.”

[Young men 18-24 yrs, C2DE, Suburban]

In such cases, people might feel this was “cheating” on the part of the CCTV operator; *“lulling you into a false sense of security.”*

But while this frequent lack of clarity of images was acknowledged, most people’s faith in the effectiveness of CCTV was unshaken.

Displacement of criminal activity was also a problem quite often acknowledged spontaneously, but again, without much evidence of people being turned against CCTV.

“They put it in on an estate I used to live in... it was quite a rough estate and it has made quite a big difference. People know it is there, and they know it is on, and they know exactly where the cameras are facing (towards) the shops. There is a stretch which is pretty dodgy and they put it down there, and people just don’t misbehave in the areas because they know the cameras are there”... “Don’t they misbehave everywhere else though, instead?”... “Of course they do, but at least it takes it away from that area, doesn’t it.”

[Women with young children, 21-40 yrs, C2DE, Inner city]

Real-time monitoring of public spaces made people feel safer than recorded footage to be watched later, because incidents could be dealt with at the moment they occurred by sending in police or security personnel. People liked the sense of *“somebody looking after you”*.

“The only cameras that are any good are the ones that are manned, so that if something is going on they can come and be of some assistance.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

Recorded footage, on the other hand, was only useful for identifying suspects after incidents had taken place.

“What I would think is you’re more conscious of the fact that whoever does whatever crime, they’ll have more chance of getting caught for doing it.”... “I think it helps”... “I think it probably makes those that are carrying out those crimes think twice about doing it.”

[Older men 50-75yrs, ABC1, Large town]

Offenders would be deterred from committing criminal acts in full view of the camera in either case, providing they were aware of their presence (and sober) – and this amounted to crime reduction.

“You wouldn’t want to do a crime if you know you are being watched. I know I wouldn’t.... If you know are being recorded you would put yourself on offer, wouldn’t you”... “Look at bank robberies and those sorts of things. They are hardly heard of any more and that must be down to the CCTV in the vans, in the banks and whatever else.”

[Men with older children, 35-54 yrs, Inner city]

But the protective role towards potential victims of violence was greater with real-time monitoring than with recording.

1.5 Attitudes towards CCTV surveillance

Many were very enthusiastic about CCTV. CCTV was regarded as a legitimate – indeed welcome – response to rising crime, especially on the streets, which made them “*feel safer*”. Expressions such as “*brilliant*”, “*marvellous idea*”, “*fantastic*”, “ *hugely beneficial*” were used.

Some were merely accepting of CCTV – just an inevitable part of modern life there was no point in complaining about.

“It’s the world we live in. Like I say, if you want to worry about it then you’ll either end up in a loony bin or living in a tortoiseshell for the rest of your life.”

[Men with young children, 21-40 yrs, ABC1, Small town]

Only a very few resisted the idea of CCTV, on the grounds of unwarranted intrusion into personal privacy, disliking the idea of “*being watched*”.

“It is so blatant though, isn’t it. I mean it is in your face wherever you go. Every street you walk down, they are everywhere... I don’t think you should be watched everywhere you go. If you are getting on with your normal life and you are not offending anyone, why should people be watching what you are doing?”

[Men with older children, 35-54 yrs, C2DE, Inner city]

Rejectors were very often young people – see Section 7 below. There was also some degree of recognition that other people objected to the ‘Big Brother’ nature of CCTV, but not very much sympathy.

“I think they’re a very valuable tool to protect everybody. If you’re innocent and you’re law-abiding I don’t care who takes a picture of me”... “There are a lot of human rights people that really don’t want cameras on them”... “It’s like the Big Brother thing, isn’t it. People worry, don’t they, if somebody’s going to know I travelled to – well, actually, it doesn’t bother me”... “I agree”... “If it saves one life a year, then it’s worth it.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

“It doesn’t bother me, but some people are funny about it”... “I don’t see why anybody thinks it’s intruding on their privacy; I’m damned if I do”... “It is intrusive, but the people that have got most to fear about this intrusion are the people who are doing wrong, and that’s fair enough. It is intrusive.”

[Older men 50-75yrs, ABC1, Large town]

“My husband objects. He says it’s like Big Brother, spying on you, watching you – where you’re going; what you’re doing. He feels it’s an invasion of his privacy. If he wants to be filmed he’ll ask someone to film him. He doesn’t want someone doing it without him knowing.”

[Older women 50-75yrs, C2DE, Small town]

The only people thought really to suffer from CCTV were criminals, for whom no-one had any sympathy. Indeed, CCTV seemed to confirm for many a comforting division of society between good people: ‘us’; and bad people: ‘them’. This thought may have helped respondents reconcile themselves to being part of a society that was readily acknowledged to have become riven by crime.

For most, the balance of advantage was undoubtedly in the innocent individual’s favour. CCTV offered the benefit of protection, with no apparent adverse effects on normal law-abiding citizens. Being watched was entirely passive: no effort was required; no negative impact resulted.

“I think the more CCTV the better, because I do feel more secure”... “I am glad to be watched, because if something happens then I know that they will get caught.”

[Women with young children, 21-40 yrs, C2DE, Inner city]

The mental risk-assessment process with regard to street crime which seemed to go on in most people’s heads focused much more on the gravity of the consequences – being mugged or beaten up – than on the real likelihood of such an event happening to them. As noted above, violent attack was what most people were afraid of, and the presence of CCTV assuaged their fears.

Confidence in CCTV was strongly associated with trust in authority – that individuals would always be fairly and benignly treated. The maxim *“innocent until proved guilty”* was cited repeatedly.

“If you haven’t done anything wrong they’re not going to be interested in you.”

[Older women 50-75yrs, C2DE, Small town]

Similarly, *“if you have done nothing wrong, you have nothing to hide”* was often quoted as a principal justification for people’s faith in CCTV.

1.6 CCTV regulation

Although, when asked, most respondents thought there must be some system of regulating CCTV, it was clear that no-one had previously given the matter much attention.

“There must be a guideline on confidentiality, because you can’t have someone watching it and then going off and meeting a friend in the pub and saying, ‘Oh I saw you on video’. There’s got to be a cut-off somewhere. People must have to sign something to say they won’t disclose any details.”

[Older women 50-75yrs, C2DE, Small town]

It had never really occurred to most respondents to wonder about authorising CCTV installations, the processing of CCTV footage, how long it would be kept for, who was allowed to see it, and so on.

“They’re only allowed to keep it a limited time, because of rules... then they get rid of it”... “Whoever looks at the tape, I don’t even know that”... “If there is an incident, they will then look back at the recordings... only if it’s reported”... “I think two weeks is long enough”... “I think it’s got to be a lot longer; more than a month even, because wheels turn so slowly.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

“Who is watching the people that are watching us, that is what I am wondering.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

When they considered the question of licensing, most were in favour.

“I think you should do. I think there’s got to be some feasible reason for it to be there... There should be some privacy rules.”

[Asian young men 18-28 yrs, Inner city]

Better information in general would be welcomed by many.

“In any situation, if somebody tells you something freely, then you feel slightly more at ease”... “We’re putting it up, for this reason, and what we’re going to do with the tape, and who’s going to be watching it’ “... “and how long it gets kept.”

[Young women 18-24 yrs, no children, ABC1, large town]

Local Councils were assumed to have a role in granting permission for the installation of CCTV cameras, probably from a planning point of view. This would only apply in the case of public places, though; for the interiors of shops or banks or other commercial premises, permission from someone else was not generally believed to be necessary at all.

“I think all the cameras that are in town, the system is basically owned and run by the shopkeepers and they commission a company to monitor them and all that sort of thing.”

[Men with young children, 21-40 yrs, ABC1, Small town]

Interestingly, the involvement of the police in installing CCTV tended to be seen as secondary, indeed if they were mentioned at all.

The idea that local people might be consulted before CCTV equipment was installed sounded good, but no-one was aware that this ever happened – the cameras had simply appeared. Apart from anything, advice from local people about where cameras should be sited for best effect would surely be helpful.

“We should be involved. It shouldn’t just be chucked up where they think... The local community know best, don’t they. They know where all the action is going on. So they should be consulted on where they are put.”

[Men with older children, 35-54 yrs, Inner city]

“I think people should be consulted. I am not saying that they should have the say, but I do think that people should be consulted and asked, and I do think that it should be put to the public and to some sort of vote or something. Then it is for the governing bodies like the police and like the Council to put their case across to you for you to see reason, and then obviously if you are a law-abiding citizen and you have nothing to hide then surely you would be happy for that”... “I don’t think there is a need for it, to be fair, for CCTV. I think it should be done anyway. For other issues yeah, I totally agree with you, but not for CCTV. Criminals would be opposing it.”

[Women with young children, 21-40 yrs, C2DE, Inner city]

Although there were sporadic references to privacy, almost nobody mentioned data protection in connection with CCTV surveillance. Nor, therefore, was the Information Commissioner named. In any event, awareness of the Information Commissioner, or indeed the previous title of Data Protection Registrar, was non-existent.

It must be said that many respondents were very sceptical about the influence of ordinary people's opinions on the deployment of CCTV and other surveillance methods.

"Whatever we say it is not going to change it, is it."

[Men with older children, 35-54 yrs, C2DE, Inner city]

"We haven't been asked or consulted about any of the CCTV cameras going up, which is really a small thing compared to some of the things they might come up with to do, then they're not going to ask us about that either."

[Young women 18-24 yrs, no children, ABC1, large town]

2 Personal privacy

There was a strong and universal belief in the right to personal privacy, for all – including criminals.

“Everyone has the right to privacy, even the pickpocket.”

[Men with young children, 21-40 yrs, ABC1, Small town]

Personal privacy was associated most readily with the home, regarded generally as sacrosanct – *“but not if you’re walking down the road”*.

Several respondents connected considerations of personal privacy with CCTV. While most were unconcerned, some saw dangers, and there was a latent but quite strong sense of unease about the growth of surveillance and its implications for privacy.

Personal privacy was agreed to be a human right.

Knowledge of Human Rights law was extremely sketchy. Explaining that the right to privacy was in law a ‘qualified right’, that could be interfered with by the state in certain defined circumstances, was unsurprising – people usually thought immediately of terrorism. But the list of all these circumstances, read out to respondents during the research sessions, tended to provoke rather a weary reaction: breaches of privacy seemed to be allowed willy-nilly, almost on a whim. Some of the expressions, such as ‘economic well-being of the country’, came across as so vague as to be capable of meaning anything.

“I think it gives them an open book... It gives them an excuse; it gives them too wide a brief. Any excuse.”

[Older men 50-75yrs, ABC1, Large town]

In some of the Scenarios, personal privacy was felt to have been intruded upon, in terms of unjustified accessing of personal information, including images.

But respondents also brought a sense of the protection of personal dignity and personal integrity into their understanding of personal privacy.

3 Other surveillance technologies

In the Part I research sessions, a number of newer surveillance technologies were explained to respondents, to seek their views. These are reviewed in this section of the report.

In addition, respondents themselves mentioned two technologies which seemed to them to belong under the surveillance heading: camera phones, and iris recognition. These are also reviewed at the end of this section.

3.1 Infra-red

Most understood that the point of infra-red was to “*see in the dark*”. This was entirely acceptable, even expected, to enable CCTV cameras to work effectively to carry out their main purpose – detect crime. They reasoned that crime was more than likely to take place after dark.

3.2 Microphones

The idea that CCTV cameras might be fitted with microphones was strongly rejected by many, as a gross invasion of privacy, though some were more relaxed.

Women especially regarded conversation as more personal and therefore more private than the external appearance they presented to the world. When out and about, they anticipated being seen, but not overheard – especially from a distance.

“I don’t care if they’re looking at me, but I don’t really want someone listening in to my conversations.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

In addition, there was a sense that what people said could be taken out of context and misinterpreted. In the context of surveillance, therefore – looking out for wrong-doing – this presented unacceptable risks to innocent and unsuspecting individuals.

“I think what you say can be taken completely out of context. I think what you do, physically, it’s fairly obvious what you’re doing, but if you’re saying something completely not related to what you’re being suspected of, they can actually take chunks, little bits and pieces...”

[Young women 18-24 yrs, no children, ABC1, large town]

If camera were to be fitted with microphones, then passers-by should be clearly notified of the fact.

3.3 Facial Recognition Software (FRS)

While there was little idea of sophisticated technology being involved in automatic matching, facial recognition in itself did not seem very surprising. Without some way of identifying individuals’ faces caught doing something wrong, CCTV would not be much use in detection specifically as a means of preventing crime.

When the technology was explained, by analogy to ANPR (Automatic Number Plate Recognition – see 2.4 below), many realised that FRS might not be totally foolproof, especially if the quality of the CCTV pictures themselves was less than perfect.

This realisation led a few to worry about the danger of ‘false positives’, with the matching process resulting in the wrong person being identified. Some assumed that corroboration would be necessary.

“I would assume that they wouldn’t be able to convict them on that evidence, but it points them in the right direction.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

There was some limited previous awareness of the technology, which “takes measurements all the way down your face, and matches it...”, but real knowledge was fairly rare.

Understanding more about FRS, and its potential fallibility, tended to weaken the detection argument for CCTV. If facial matching was sometimes unreliable, then how effective really was CCTV, in catching offenders?

A further train of thought for a few concerned the status of the facial images compiled for use as the database against which CCTV pictures were checked for identification purposes. Where did these images come from? Had the individuals given their consent, and under what circumstances? All this was worrying.

“Then surely they’d have to have a database of everybody’s mug shot in the country?”... “Well, they’ll get it in the end.”

[Older men 50-75yrs, ABC1, Large town]

A few, however, expressed more faith in an automatic system for facial recognition that *“takes out the middleman”*, ie. the human operator.

3.4 Speed cameras

Speed cameras were often mentioned spontaneously, and quite widely acknowledged to be another safety measure.

As such, no-one seemed actually to reject speed cameras, even those who eventually admitted to having been caught by them.

“It’s a deterrent. It makes you slow down.”

[Men with young children, 21-40 yrs, ABC1, Small town]

However, there were mutterings about whether the cameras were sometimes deliberately positioned *“in horrible places”* to catch drivers unawares, and thus raise money from fines, or whether they were always in the right place from a safety point of view. The penalties were also often judged as disproportionate.

“They are definitely all over the place aren’t they”... “Speed cameras don’t deserve a life, I don’t think... it is really mean where they put them.”

[Women with young children, 21-40 yrs, C2DE, Inner city]

“The only objection people have going against speed cameras: are they using it to stop speeding, or are they using it for an income?”... “It’s acceptable in the fact of the way it does it, but the instant justice I don’t think is acceptable... You’ve been driving clean for 30 odd years, and they take nothing like that into consideration.

[Older men 50-75yrs, ABC1, Large town]

Stories in the media about the occasional inaccuracy of speed cameras were also well known.

As with Facial Recognition systems, there was very little awareness of the automatic processes inherent in identifying numberplates, and hence keepers of offending vehicles. Learning this was found interesting, rather than surprising.

Several spoke about the practice of slowing down for the cameras and then speeding up again, which they observed in others, and in some cases indulged in themselves. This cast doubt on the effectiveness of speed cameras, but even so, there were no calls for their wholesale removal. They seemed to be accepted as a legitimate way of enforcing road safety rules.

Bus lane cameras, on the other hand, attracted much less support, at least in south London where they had recently been introduced. Being new, modern cameras, they were reported to be able to swivel round to capture numberplates, so there was more of a sense of actively hunting for offenders rather than passive recording. Bus lane cameras were criticised for being poorly signalled, especially concerning their hours of operation, which varied from street to street. So drivers had difficulty obeying the bus lane restrictions, and avoiding being caught unfairly, in their view. Because of this, there were suspicions of the cameras being there mainly for revenue raising, rather than any benefit to members of the public.

“It is money making. It has got to be for them to put it there”... “Bus fines... There is a certain bus lane and if you ever go down there shopping they are scanning the high street all the time, so they can’t only be there for the bus lane. But when the bus lane is in operation they just focus on the bus lane. The same camera... They spin in any direction you want, because I was right underneath it when it nicked me. I was doing a U-turn and I saw it through the sunroof scanning around like that, and it followed me into the other lane.”

[Men with older children, 35-54 yrs, C2DE, Inner city]

3.5 Road pricing – satellite vehicle tracking

The more people thought about satellite vehicle tracking, the less they liked it.

The idea that “*they*” could trace their whereabouts at any time was uncomfortable, and seemed like an invasion of personal privacy – with no apparent benefit to the individual.

“It’s not just about charging you, it’s also the monitoring of everybody’s activities – where they’re going... It’s part of your privacy.”

[Men with young children, 21-40 yrs, ABC1, Small town]

Moreover, other ways of relating motoring taxes paid to vehicles’ annual mileages seemed much “*less intrusive*” – for example, higher fuel duty – much as many people approved of the principle of road tax corresponding to vehicle usage.

“I think that probably is Big Brother”... “That is definitely just following people for the sake of doing it”... “I don’t think that’s right”... “If they are putting a satellite tracker up so they can track you, how many miles you’re doing a year, and they can charge you extra for that, then I’m definitely against that, because there are other simpler ways for them to do that.”

[Older men 50-75yrs, ABC1, Large town]

Some drivers were inclined to shrug off the privacy implications as no worse than with GPRS mobile phone technology, which can already pinpoint geographical location with a fair degree of accuracy.

But most were uneasy, left wondering what other uses the information from satellite vehicle tracking might be put to, and seeing no personal benefit to themselves to weigh against the potential intrusion into their private lives.

“It’s all part of the same thing. So I’m going about my normal everyday life, and I don’t break the law, but all that information about me could be misinterpreted, and it could be used against me. I don’t trust people necessarily who have that information in their hands... I don’t know who has that, or what they’re going to use it for.”

[Young women 18-24 yrs, no children, ABC1, Large town]

Incidentally, some people were under the impression that the London Congestion Charging cameras worked through satellites rather than ANPR technology.

3.6 Radio Frequency Identification (RFID)

There was minimal previous awareness of this technology, which was explained to respondents as a potential replacement to barcoding for retail inventory control.

Many found the concept hard to grasp – tiny microchips embedded in goods purchased that could be read by remote scanner.

The purpose of RFID seemed equally puzzling.

“I don’t see any point in keeping the tracker on. Why do they want to know where you are?... If the purpose is to stop shoplifting then they should deactivate it as soon as you leave the shop.”

[Men with older children, 35-54 yrs, C2DE, Inner city]

Once they understood that there was at present no obligation to remove these microchips, many became quite alarmed. The ability to locate items in purchasers’ possession once they had left the shop – at home, or elsewhere – was very disconcerting.

“That’s intruding on your privacy when you’re within your own home.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

“It’s like being tagged, isn’t it”... “When you’ve paid, take it out; no problem”...

“They’d know every movement, wouldn’t they. I wouldn’t like that.”

[Older women 50-75yrs, C2DE, Small town]

Respondents could not think of any good reason why anyone would need to know where the item had ended up, or at least any reason that would benefit them personally. Commercial purposes did not seem to them to justify such a potential invasion of personal privacy. The only possible benefit to the individual might be helping to recover tagged items if they were stolen.

All were in favour of legally obliging retailers to remove the microchips from all items as they were paid for at the till, just as security tags are now.

The notion that RFID data might be linked up with personal information from other sources, such as credit card details, did not occur to respondents unprompted. When drawn to their attention, they were even more vehemently against allowing retailers to leave the microchips in place after the goods had left the shop.

3.7 Millimetre wave imaging (MWI) or T-rays

This new technology was explained thus:

‘MWI produces images derived from passive radiation from the human body, and shows whether the person has items like weapons hidden under clothing. The effect is that the image produced look as though the person has no clothes on.’

Most respondents were shocked.

“No way!”... “Now that is an infringement on your privacy. Of course it is. People do not like to be seen in the nude... it repulses me.”

[Women with young children, 21-40 yrs, C2DE, Inner city]

The privacy implications, and potential for abuse, were too much.

“I think that is embarrassing, and some people will use it for the wrong reasons. I have a friend... and he would use that kind of thing. I think personally that is not right. He will start looking at girls. Some nasty men get pleasure out of things like that.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

In a high-risk situation such as an airport, they felt MWI was possibly justifiable on the grounds of protecting the travelling public from being killed by bombers or hijackers. The benefit might be held to outweigh the disadvantages.

“At airports I think it is justified, especially now with this terrorism thing... At an airport it serves a purpose, but outside I think it is a bit too much. Invading your privacy I think, really”... “What about the Arabic ladies with the veils and that and are not allowed to be seen? Imagine! Who looks at them when they go through there? One of their own? How do they feel?”

[Men with older children, 35-54 yrs, C2DE, Inner city]

“If that’s as a deterrent that’s only going to be used at airports, you expect those security measures at those sorts of places”... “You’d sooner have an image taken of you rather than be blown up on an aeroplane.”

[Men with young children, 21-40 yrs, ABC1, Small town]

“At an airport I wouldn’t mind that, just because of the high risks”... “I really think that’s humiliation”... “I think that’s a real infringement.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

But even in the airport instance, many resisted the idea as “degrading” – especially, but certainly not exclusively, the women in the sample.

“I’d look for alternatives first”... “I would object to it.”

[Young women 18-24 yrs, no children, ABC1, Large town]

Some felt that all passengers should be offered the option of a less intrusive security scan, such as the metal detectors in current use at airports.

Respondents also insisted that passengers should be warned in advance, preferably at the time of booking their flight, that MWI would be in operation at the airport, so that they could exercise their choice not to fly at all and avoid subjecting themselves to such humiliation.

The idea that only women should be authorised to view MWI images of female passengers, and vice versa, mollified a few.

One suggestion was that since MWI images were only for immediate use ‘now’, to show whether individuals were armed or not, recording or retaining the images should be outlawed.

In situations less risky than airports, such as the average high street or even nightclub, most considered that MWI would be completely unacceptable.

This research, by the way, was conducted several weeks before the police raids on pubs in north London using MWI – though referred to as a special kind of X-ray and with no mention of nude images – were reported in the media (last weekend in March). No-one in the sample was previously aware of MWI.

3.8 Camera phones

The newest generation of mobile telephones which are fitted with digital cameras were brought up in several of the research groups as representing a potential invasion of privacy – mainly in the context of paedophiles, though a couple of rape cases were also mentioned.

The fact that these phones are small enough to be smuggled unseen into sensitive locations, such as toilets or swimming pool changing rooms, was cause for concern among some, especially women.

3.9 Iris biometrics recognition

Unlike camera phones, which many respondents had direct experience of, iris recognition was something only heard or read about. The fairly recent movie *Minority Report* was also a source of awareness – several respondents mentioned the technology spontaneously.

*“Maybe they can have a CCTV that could take a print of your eye or something”...
“I have been looking in a lot of newspapers and basically there are technologies that
have come recently, or soon, that will be scanning the eye”... “I don’t agree with that.
I don’t want them tampering with my eye.”*

[Afro-Caribbean young men 18-28 yrs, Inner city]

Very few, however, seemed especially bothered about it; as iris recognition was understood to be able to identify individuals uniquely, there might be something positive to be said about its ability to establish your identity incontrovertibly.

*“I don’t know about the DNA thing, but there is something where they can scan
your eyes. I think that is quite a good idea.”*

[Women with young children, 21-40 yrs, C2DE, Inner city]

Respondents did not appear to see anything very sinister in the projected uses of iris biometrics for passports, driving licences or ID cards – though it seemed rather futuristic.

4 Data protection

4.1 Experience and knowledge

'Data protection' was mentioned spontaneously a couple of times in connection with personal privacy, but it was clear that for everyone, the idea that CCTV or other surveillance images counted as 'personal information', and that data protection rules would therefore apply, was new.

The term 'data protection' was familiar to all – sometimes from work; often from correspondence at home, especially direct mail from financial institutions.

"I've heard of the Data Protection Act"... "I think it's to stop your data being used willy-nilly, without your consent."

[Older men 50-75yrs, ABC1, Large town]

The main association was thus with the disclosure of personal details to third parties without the data subject's consent – this was known to be illegal.

"It is to protect you from your data being given out, and information about you."

[Men with older children, 35-54 yrs, C2DE, Inner city]

Keeping records of individuals' personal details was also covered by data protection rules.

"All I know is they can't hold your details for so long on their system. We do it on the computers, and with our customers we can only hold their information for six months and after six months they get deleted from the system, and it is something to do with the Data Protection Act"... "Is it that they are not allowed to give information about you without you knowing, or something?"

[Women with young children, 21-40 yrs, C2DE, Inner city]

Many also knew that they as individuals had the right to see personal information that related to themselves.

"You can claim your own file."

[Young women 18-24 yrs, no children, ABC1, Large town]

Awareness and knowledge of other data protection principles was slight.

Attitudes were fairly neutral. Those who had to follow data protection rules at work tended to regard this as somewhat of “*a pain*”, but restrictions on access to personal information were generally considered to be a good thing.

“I think it is a good thing that there is a Data Protection Act, but there also needs to be a protection Act that says you cannot impede on my privacy.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

4.2 Data protection Principles

Unrelated to a specific context, many of the data protection Principles of good information handling came across as vague and imprecise – they could mean anything.

“This is the whole problem. Who decides, at the end of the day, what is and what isn’t excessive?”

[Men with young children, 21-40 yrs, ABC1, Small town]

Several of the Principles made much better sense when considered in relation to the Scenarios used as stimulus in the research. The following commentary brings together people’s interpretations both pre- and post-Scenarios.

Fairly and lawfully processed

This principle was hard to disagree with, but quite what it might mean in practice was difficult to work out.

“If we don’t know what the law is, then what is ‘lawfully processed’?”

[Older men 50-75yrs, ABC1, Large town]

Some of the Scenarios appeared to break the principle, but it seemed to operate as a catch-all for condemning a variety of misuses.

Processed for limited purposes

The implication that personal data collected for one purpose should not then be used for another became much clearer in the light of several of the Scenarios, and commanded widespread agreement.

“They can’t just go and use it willy-nilly, can they... Take it home to their mates and say ‘I saw this nice girl today’. Can’t do that!”

[Women with young children, 21-40 yrs, C2DE, Inner city]

Respondents were particularly critical of CCTV footage being passed on without consent for “commercial gain”, especially “titillation”.

Adequate, relevant and not excessive

In the context of surveillance, these were regarded as three separate ideas, not one.

‘Adequacy’ related to the quality of images obtained by CCTV, and specifically whether they were good enough to be used for the purpose of identification of miscreants. This after all was the main point of CCTV so, certainly, images should be adequate for their purpose.

‘Not excessive’ was interpreted in the sense that other, less intrusive or clumsy methods of identifying possible wrong-doers should be preferred. Several of the Scenarios suggested that CCTV might sometimes be used as rather a blunt instrument, indiscriminately lumping the innocent in with the guilty. ‘Not excessive’ was therefore a good principle. But on whose authority it would be decided whether information was ‘excessive’ or not continued to be of concern.

‘Relevant’ seemed to make sense, but again it was hard to see what it might in practice, out of context.

Accurate and up-to-date

Certainly these criteria should apply to surveillance images, it was felt.

‘Accurate’ seemed to be more important than ‘up-to-date’, in this context.

Not kept for longer than necessary

When respondents looked first at the whole list of principles, before studying the Scenarios, this was the one they tended to pick out, somewhat derisively, as being most susceptible to interpretation, to the advantage of whoever was responsible for the surveillance.

However, with further thought, the idea that different types of footage should be kept for different lengths of time seemed quite appropriate.

Generally, though, longer periods were preferred to shorter, erring on the side of caution. Finding missing persons was often behind this preference, especially among women – there might be a long lapse of time before someone was reported missing, and CCTV recordings needing to be searched to see if they were there on film.

In some groups, the possibility was raised of CCTV being able to provide an alibi for suspects wrongly accused. This was another argument for keeping CCTV records for longer rather than shorter periods.

The case of Ian Huntley’s police records was sometimes mentioned in this connection too.

“I think the time should vary according to the crime. If you feel up young girls, that should be locked.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

Processed in line with the data subject’s rights

Despite quite widespread awareness of the data subject’s right of access to their own personal records, this was rarely put forward as an explanation of this principle.

Many were not entirely sure what these ‘rights’ consisted of, though consent was quite often implicit. Like the First Principle, this one tended to be used too as something of a catch-all to criticise instances of misuse of surveillance, exemplified in the Scenarios.

Secure

The term ‘secure’ did not always appear to convey the concept very well.

Only a minority understood it straightaway.

“No one unauthorised should look at it”... “It should be secure so that anybody can’t just walk in and get a copy.”

[Men with older children, 35-54 yrs, Inner city]

The notion that CCTV footage should be tamper-proof, and not passed on to third parties without consent, was widely applauded, once attention was drawn by the Scenarios to the possible risks of mishandling.

Not transferred to countries without adequate protection

This principle made sense and was approved of.

Most were, however, surprised to learn that data protection law in Britain had its origins in the European Union, and that therefore any personal information would be treated with as much care in other European countries as in Britain.

Occasionally spontaneous references were made to the Internet.

5 Response to Scenarios

The full text of all the Scenarios, as given to respondents to read, is given in the Appendix, together with a chart showing which group reviewed each one. Reactions to the Scenarios are detailed below.

Please note that there is no Scenario 7. The ten Scenarios are numbered from 1 to 6, then 8 to 11.

5.1 Scenario 1

Most respondents were inclined to cheer the erring husband's come-uppance in this story, when his wife saw him walking arm-in-arm with another woman she did not know, challenged him and then divorced him. Everyone took the wife's part; he was "*just a pig*", who had "*cheated*" on her and then "*lied*" to cover up.

However, the showing of CCTV crime-prevention footage to a business audience unconnected to law enforcement was readily seen as wrong and unfair, in breach of the Second Principle of Limited Purposes. At the very least the faces should have been obscured.

"Somehow they should let you know they are going to be using it, or blur out the faces. Sometimes when you see something on TV like the news or something with people just walking about and the people in the picture are like that as well. I don't know if you understand what I am saying. If they are not to do with the actual thing they are talking about, and if it is not relevant, they just blur them out."

[Women with young children, 21-40 yrs, C2DE, Inner city]

There was a debate about the feasibility of obtaining consent, to being filmed in the first place, and/or to the film being shown for promotional purposes as described in the story. While respondents did not condone the husband's behaviour, they did generally believe that consent should have been sought to showing CCTV footage for purposes other than crime prevention. But whether consent was covered by the First Principle or the Sixth Principle was not entirely obvious – not that this confusion much bothered respondents.

5.2 Scenario 2

This story was an example of how CCTV pictures could be used unfairly to round up potential suspects without corroborating evidence of wrongdoing, which most respondents deplored.

“It should be designed for the job it’s there for, well signposted – what it is there for – and not used for any other purpose, and then it should be good at what it’s there for”... “It’s presuming guilt... they had to talk their way out of it... They had to prove they were innocent rather than be proven guilty.”

[Young women 18-24 yrs, no children, ABC1, large town]

Women especially felt that the treatment of the suspects – keeping them in custody for several hours – was heavy-handed, especially for the one who was forced to miss his mother’s birthday party.

Men, on the other hand, were more likely to conclude that keeping suspects in custody on flimsy evidence was probably normal police practice, just something to be accepted – and that CCTV made no difference. Even men, however, sometimes thought that the suspects’ treatment went too far,

“My mum’s party, I think I would go spare. I don’t think I would like the police any more after that. I would be livid if that was me. I would go bonkers, mate, especially if I didn’t do it”... “They have been locking up people they shouldn’t be locking up for years, anyway”... “I think it was too excessive – these two people missing the party and the fact that they were there for 10 hours.”

[Men with older children, 35-54 yrs, Inner city]

A few, though not all, made a connection with the unreliability of Facial Recognition software, but even if the face-matching process was visual (the Scenario did not say), the quality of the CCTV images from the ATM was clearly not good enough to get the right answer.

Thus both the Third and Fourth Principles were seen as broken in this case; the images were neither Adequate nor Accurate.

This was one of the stories that made respondents conscious of the potential for CCTV to incriminate people who had nothing wrong, through circumstantial evidence alone.

5.3 Scenario 3

This story was widely condemned as racist. Only Asian men were said to have been picked out by the railway station CCTV cameras, and they were apprehended as possible culprits without any other corroborating evidence of drug-dealing.

“They say that many of them were Asian, which shows that some of them weren’t. So they shouldn’t have just picked out the Asian people...It seems very racist”... “What’s the evidence against them? What have they done, other than get off a train and walk through the station?”... “You haven’t really got to interview every single person coming through to make them all feel guilty, have you”... “The more you’re getting this lump of people, and only one or two are the criminals and the rest are innocent people, then you’re going to get people’s backs up. They’re going to say, ‘Well, it is Big Brother watching you.’”

[Older women 50-75yrs, C2DE, Small town]

The fact that only one of the twenty suspects turned out in the story to be in possession of drugs confirmed that CCTV in this case was a very blunt instrument for catching dealers, “hit and miss”, and an inadequate replacement for more active policing.

“This is a cheap way of catching criminals... not actually catching them in the act.”

[Asian young men 18-28 yrs, Inner city]

In terms of data protection, therefore, the main perceived breach was of the Not Excessive part of the Third Principle. Many respondents felt that less clumsy, quicker methods such as following suspects, perhaps with sniffer dogs, would be preferable – “proper” and fairer.

“It is just one person carrying whatever it is, illegal or whatever. I think the police should be there looking, instead of the CCTV”... “ There needs to be some hard evidence, doesn’t there. Hard evidence. You can’t just be walking through a station every night and become a drug dealer. I go through a station every night and I would hate to think that since I have a bald head and glasses that I was one of the 20 picked.”

[Men with older children, 35-54 yrs, Inner city]

Others, however, felt that the tactic of rounding up a large number of suspects only to find most of them innocent was commonplace – CCTV was almost immaterial.

Nevertheless, being detained by the police was no small matter – perhaps leading to difficulties with your employer, loss of earnings and so on. Ensuring that innocent people were not picked up unfairly was therefore deemed very important, in a practical sense as well as in the interests of natural justice.

The reactions of the young Asian men in the sample were similar to others'. However, there were signs that this story tapped into concerns about undifferentiated targeting of members of their community, without much actual evidence of criminal activity against individuals. "*Harassing*" was the term they used.

5.4 Scenario 4

Broadcasting on the Internet of sexual activity between private individuals, without their consent, was strongly criticised as “outrageous”, “disgusting”.

The use of microphones to record sounds as well as images on film, was felt to by many to make the offence described in the Scenario an even worse intrusion into personal privacy, whatever the original justification.

“Why microphones? That is not right”... “It is your freedom of speech”... “They might be wanting to listen to you saying you were going to nick that”... “But you could stand there and say we are going to nick that, but until you do nick it, it is not a crime, is it”... “The microphones are excessive use.”

[Women with young children, 21-40 yrs, C2DE, Inner city]

Most considered that the individuals concerned would not only have a case against the Internet broadcaster, but also against their employer, on the grounds of gross breach of privacy. Having sex on your employer’s premises might not be advisable, but was certainly not a crime.

This story emphasised the importance of clear signs to advise people of the presence of cameras, and indeed microphones. For some, it also reinforced the fear that CCTV operations were out of control.

“You can’t just put them up and not tell anyone!”... “You don’t know who’s watching the footage of you.”

[Young women 18-24 yrs, no children, ABC1, large town]

Many of the data protection Principles were considered to have been broken in this story:

- the Second Principle of Limited Purposes
- the Third Principle of Relevance
- the Sixth Principle about Data Subjects’ Rights (consent, specifically)
- the Seventh Principle of Security
- the Eighth Principle about Overseas Transfer

5.5 Scenario 5

In this story, passengers being covertly filmed by CCTV at the airport departure gate was not objected to nearly as vociferously as having their credit card details handed over by the airline to the Immigration service of the Republic of Omber.

Clearly, concerns about fraud were uppermost in respondents' minds. Also, they could not understand why Immigration officials would need credit card details, unless to check on passengers' financial status, in which case bank account evidence would surely be more useful.

"I think the story with the airline is putting yourself up for fraud, isn't it – giving your credit card details and a picture of you before you even got there... By the time you are on the plane and you have landed they could have emptied your account. They have all your details and passport number and everything."

[Men with older children, 35-54 yrs, Inner city]

"I don't think credit cards have anything to do with immigration."

[Asian young men 18-28 yrs, Inner city]

"There's no crime been committed. So perfectly innocent people, data is being gathered on them, their identity, all being pulled together – picture, passport, credit cards details, where they live. I'm uneasy about that... What I'm uneasy about is the corner that criminals have pushed us all into."

[Women with older children, 35-54 yrs, ABC1, Suburban]

Respondents were firmly of the opinion that passengers should be warned about these requirements at the time of booking their flight, so that they could choose whether or not to travel to Omber at all. They also felt that some kind of explanation should be given as to why all this information was needed, what would be done with it, and how long it might be kept for. Without it, it was hard to tell whether there was *"any benefit... for you, at the end of the day"*.

Several maintained that the information should all be destroyed once the passenger had returned home, after which, of course, any risk of illegal immigration would be past. They were looking for a *"guarantee"* on this point.

Against the worries about credit cards, CCTV filming seemed a relatively minor issue. However, advising passengers about this in advance, or even at the time, seemed fairer to respondents, to obtain consent.

The more thoughtful realised too that if the provision of all this information was meant to deter illegal immigrants, then not advising passengers in advance would frustrate this intention – so there would be no point in not telling people. Potential lawbreakers would “*think twice*” if they knew beforehand that all these measures were being taken against illegal immigration. This applied equally to CCTV filming.

Without explanation from Omber’s Immigration service about why they wanted this information from passengers, it would be difficult to judge whether any of the data protection Principles, including the Second Principle of Limited Purposes, was being obeyed or not.

5.6 Scenario 6

In the groups given this Scenario to read, this was usually the one that had stuck in respondents' minds and the one they wanted to talk about first in the re-convened research session.

The story was very close to home – many, especially women, could identify with the characters in the story who repeatedly returned goods to A&B clothing stores.

They could therefore vividly imagine themselves in the situation described in the story – being called in from the Customer Service desk for interview by security staff, having their personal details checked by the police, and so on – on suspicion of shoplifting.

“Has the shop got a right to ask you to come into the shop for a interview with their security staff?”... “Personally, I wouldn’t go into that shop”... “I would feel absolutely gutted... taken and questioned.”

[Older women 50-75yrs, C2DE, Small town]

Like Scenario 3 (see 4.3 above), this seemed like overkill, treating large numbers of innocent shoppers as suspects, with no corroborating evidence of wrongdoing. The Third Principle was thus comprehensively broken – using CCTV images in the way described was neither Adequate nor Relevant, and was certainly Excessive.

Alternative ways of curbing shoplifting were suggested, including better use of in-store CCTV cameras or security guards to catch offenders in the act, or insisting on the production of receipts for items the shopper wished to return. Neither of these presented an affront to the personal dignity of innocent customers, in the way the treatment meted out to those returning goods in the story came across.

“You’ve done absolutely nothing wrong, and suddenly you are being told that you have to provide your name, address and date of birth... You’d be mortified... You’d never set foot in the place again!”... “If they’re paying for a CCTV camera on the cash desk, they can pay for it to roam the store.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

The final twist in the story – that customers found to be innocent had their details added to A&B’s marketing database – heaped insult upon injury, and flew in the face of the Second Principle about Limited Purposes.

Even without this, nevertheless, many claimed that following such an experience as described in the story, they would never darken the doors of that store again.

5.7 Scenario 8

Several respondents, especially men, expressed some sympathy with the CCTV operator in this story, who had cut out of the footage of a violent incident all reference to his friend, one of the protagonists. They felt that in this situation, they might well have been tempted to do the same. Nevertheless, all considered his actions to be wrong.

“You’re still going to try and cover your mate up, aren’t you”... “I wouldn’t”... “Legally it’s wrong”... “It is wrong”... “He shouldn’t have doctored the tape.”

[Young men 18-24 yrs, no children, C2DE, Suburban]

What the operator had done broke the Fourth Principle regarding Accuracy, and the Seventh Principle, about Security.

While the friend had gained an advantage, the other men involved in the fight were seen as disadvantaged by their friend getting off scot-free, and the public interest was undermined too.

The solution seemed to most people to lie with the camera technology, which they felt should be tamper-proof. At the very least, the CCTV footage should be time-coded, so that any tampering would be obvious.

One or two respondents remarked that if CCTV footage could be altered to cut personal images out, then it might be just as vulnerable to putting them in – clearly this was more worrying.

This Scenario reinforced in some minds the need for CCTV operators to be checked out, including reference to the Criminal Records Bureau, to ensure their honesty, integrity and reliability.

“If you’re going to have operators doing this, you must have some sort of vetting, for previous past records.”

[Men with young children, 21-40 yrs, ABC1, Small town]

In some groups there was also a related discussion about whether CCTV operators had to sign confidentiality agreements, preventing them from disclosing details about individuals seen on camera. While it was recognised that *“having a laugh with your mates”* at the expense of people whose images were caught by the cameras would contravene data protection law, no-one was certain whether confidentiality agreements were mandatory for CCTV operators, or not.

5.8 Scenario 9

In this story, where theft of mobile phones was displaced from the town centre when CCTV cameras were installed, to a nearby housing estate, respondents expressed considerable sympathy with the residents of the estate. All agreed that their request for CCTV to be introduced to protect them, should be granted.

But they asked, somewhat wearily, “*Where does it all end?*”. At the first research session, the fact that Britain has the highest incidence of CCTV in the world had already been explained, and this Scenario went some way to showing why.

“It may make you feel safe in that area, but as you say because it pushes it to the next street and then you put a camera there and it pushes it to the next street, then you are going to know when you walk down the road it will be quite safe here, but as soon as I go round that corner I am going to be mugged and raped. You wouldn’t want to walk around there, would you. What happens if you have to walk around there?”

[Women with young children, 21-40 yrs, C2DE, Inner city]

On a more positive note, the effectiveness of CCTV in combating street crime was demonstrated, as far as the town centre was concerned, especially as CCTV was credited in the story with having alerted the police to the problem of mobile phone theft in the first place – a crime which commonly goes unreported by teenagers who are the usual victims.

However, the story also underlined, for many, the need for more police on the beat, to deter criminal activity.

5.9 Scenario 10

The use of speed camera footage to evict rough sleepers from the central reservation of a dual carriageway road, as described in this story, was widely held to break the Second Principle of Limited Purposes.

“It is an abuse of the camera as well, though. It was put there to do number plates. It wasn’t put there to move down-and-outs on”... “It has been used to spy on something else.”

[Men with older children, 35-54 yrs, Inner city]

“The cameras were put there for speeding, and then they decided they were going to pick up these people that were sleeping rough. If they were put there for speeding, it should be for speeding... That’s not what the cameras were for.”

[Older women 50-75yrs, C2DE, Small town]

Everyone agreed that sleeping rough was not a crime.

But opinions diverged as to whether the Council had overstepped the mark in sending the police to turn the rough sleepers out and move them on. The difference of view turned on the perceived danger of camping on the central reservation, and therefore whether the Council and police could be said to be acting in the rough sleepers’ own best interests. Concerns about their safety would justify interfering with their personal privacy, and in this case the Relevant and Not Excessive provisions of the Third Principle would not be breached. However, even when safety concerns were assumed to be the main motivating factor behind the Council’s decision, some felt that there should be ‘No Camping’ notices put up on the central reservation before the police went in, to warn the rough sleepers and rationalise the police action.

If alternative accommodation, such as a hostel or even a campsite, were offered to the rough sleepers – and the story did not say – then most respondents would have felt happier about the actions of the police.

“In a way it was unacceptable, because it was used for other purposes”... “They have nowhere else to go; they’re disadvantaged; I think it’s actually quite wrong to move people along”... “The Council should provide more accommodation for them.”

[Young women 18-24 yrs, no children, ABC1, Large town]

5.10 Scenario 11

Many found this story quite upsetting, and sympathised with Kim's plight. She was turned down for a job as a primary school teacher, as police checks made at the time of applying had turned up a CCTV picture of her at an anti-airport demonstration, labelled simply as 'troublemaker'.

In the first place, respondents asserted quite forcefully that Kim had done nothing wrong – peacefully demonstrating was judged to be a civil right, and certainly not a crime.

“That is condemning someone who is innocent. That is really out of order... It wasn't fairly and lawfully processed, I don't believe. They have just picked people out and now they are down, as that lady the teacher, as potential troublemakers. She is not. She is expressing herself. That is wrong. That is really wrong... It is defamation of her character as a teacher, I believe.”

[Women with young children, 21-40 yrs, C2DE, Inner city]

Respondents were concerned that surveillance images recorded in these circumstances might be kept for future reference, especially without notification to the individuals, let alone their consent.

The Second Principle of Limited Purposes was clearly breached in this case – the pictures were retained by the police for possible use at future anti-airport marches if clashes broke out, not for employment checks.

The lack of transparency and absence of consent manifest in the story were condemned, contravening the terms of the Sixth Principle about Data Subjects' Rights. The label of 'troublemaker' seemed quite inappropriate., especially without explanation.

“I don't think they should have done that unless they were giving a file attached with it of what happened, and when it happened – but that is still wrong, anyway.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

“She was branded a troublemaker and she didn't know why. She didn't really do anything wrong ... It's freedom of speech, isn't it.”... “She should have been able to find out why they'd knocked her back for the job.”

[Young men 18-24 yrs, no children, C2DE, Suburban]

A few also felt that the Fifth Principle was broken, in that Kim's picture had been kept for 'longer than necessary'.

6 Post-deliberation views on surveillance

6.1 Misuse of CCTV

Reading and thinking about the Scenarios given to them during the course of the research certainly opened many people's eyes to the possibilities of misuse of CCTV.

"It does make you wonder just how much you are being watched."

[Older women 50-75yrs, C2DE, Small town]

"I suppose you think more now that there probably is more of a risk of someone doing something, now when you think about it, than you did before... To doctor it, to take someone out; someone could doctor it to put you in."

[Young men 18-24 yrs, no children, C2DE, Suburban]

However, their own experience counted for more. Most did not know of real-life cases of misuse – certainly not as regular occurrences – and they tended to trust their own knowledge.

"I don't believe it is as controlled as it should be; however, it has the ability to make you feel safer"... "It is a mental thing. You know if you have your dad watching you walking down the road, you feel all right. You don't know what your dad is doing behind you, but you feel all right."

[Afro-Caribbean young men 18-28 yrs, Inner city]

The main risk of misuse seemed from the Scenarios to lie in the potential for CCTV and other surveillance to incriminate innocent people who were simply in the wrong place at the wrong time. This contravened the natural justice principle of 'innocent until proved guilty', frequently cited and obviously dearly held.

Remedying this was partly a question of technology – ensuring that facial recognition systems, visual or automatic, were properly up to job of accurate identification – and also partly a question of how suspects were treated by the police. This latter point is probably beyond the strict remit of the Information Commissioner, but bears taking seriously if public confidence in surveillance is to be maintained.

“Where’s the principle that says, ‘you shall not gather information and keep it on me unless you have reason to suspect I’ve done something wrong?’”

[Women with older children, 35-54 yrs, ABC1, Suburban]

Other than this, the 8 data protection Principles seemed to deal adequately with the cases of misuse featured in the Scenarios. If the Principles had been strictly adhered to, then misuse would not have occurred.

Transparency and consent may be implicit in the data protection Principles, although not really explicit in the summary handed out to respondents. The importance attached to these emerged strongly from the debates on the Scenarios.

6.2 Surveillance acceptability

Surveillance measures and technology found acceptable were those which protected the individual's own personal safety.

This was the key criterion, more important even than the protection of other people's safety.

Approval for CCTV in public places rested on the perception that its presence made the streets safer 'for me'.

The limits to acceptability excluded measures which:

- incriminated or "framed" innocent people
- led to innocent people being treated as criminals
- laid people open to the possibility of fraud, through access to their financial details
- invaded personal space
- intruded into private homes
- failed to offer protection to individuals and their personal safety

People's own knowledge and experience of CCTV did not demonstrate any breaches of these limits to acceptability.

Thus even after exposure in the Scenarios to possible examples of misuse, respondents reverted to their support and enthusiasm for CCTV on the grounds of enhanced personal safety – obviously a major benefit, with no real disadvantages to weigh against it.

However, the balance of advantage was less clear with many of the other newer surveillance technologies discussed in the research sessions, which made some feel nervous.

"They shouldn't take it much further than they're doing... all microphones and all that... It should be better quality, like at the moment they're all fuzzy, but they don't need to advance it."

[Young men 18-24 yrs, no children, C2DE, Suburban]

Personal benefits accruing to the individual from RFID, satellite vehicle tracking and even speed cameras were uncertain at best, while they might easily broach one or more of the limits to acceptability listed above, leading to negative effects for the individual.

Another factor in acceptability was whether people felt that they had any choice over submitting to surveillance. Many argued that with CCTV on the streets, you could decide to keep away from the town centre and thus avoid being caught on camera – though not everyone agreed that this was truly a choice.

“Like if there is something on TV that is going to offend you, don’t watch it. Same way as if that particular place has a camera, and you don’t want to be on it, don’t go there”... “But sometimes there are places that you won’t be able to go at all, because there are so many cameras. What about if you just want to go just shopping? You can’t!”... “But if I am going to go shopping it doesn’t bother me then”... “Some people it might”... “Well then, don’t go there, go somewhere else!”

[Women with young children, 21-40 yrs, C2DE, Inner city]

With satellite vehicle tracking on the other hand, for example, there would be no choice, and this was another major objection to its introduction. While the element of choice with CCTV might be more illusory than real, people still clung to the idea of being able to exercise some degree of control over the way they lived their lives by claiming that they did not have to submit to CCTV surveillance if they did not choose to.

Since popular support for CCTV relied so heavily on the balance of advantage being perceived to weigh in favour of ordinary people, because their own knowledge and experience did not tell them otherwise, it appears arguable that these positive attitudes might be vulnerable to bad publicity about:

- ineffectiveness of CCTV in preventing or solving crimes, specifically those involving physical harm to innocent victims
- breaches of personal privacy
- other instances of unfairness or misuse of personal images

If such stories were to gain currency, then confidence in CCTV, let alone other surveillance technologies, might begin to melt away.

“You never hear any bad words about CCTV”... “If you had few adverts on telling people how incriminating it can be in different circumstances, then I’m sure you’d get a few more voices raised.”

[Men with young children, 21-40 yrs, ABC1, Small town]

6.3 Desired rules for surveillance

From the discussions about the Scenarios in particular, a number of clear rules were put forward for CCTV and, by extension, other surveillance technologies.

In the main, these desired rules are already covered in the ICO's current CCTV Code of Practice, if not always in so many words. Divergences are pointed up in the following commentary.

Clear signs

Clear signs to advise the public of the presence of cameras were required, for a number of reasons. Transparency in this matter indicated that members of the law-abiding public were being treated civilly and respectfully, as was their due. Signs also demonstrated that consent was acknowledged – that people could choose whether or not to submit themselves to the cameras' gaze.

"If someone doesn't know they're being filmed, it's like an invasion of privacy."

[Young women 18-24 yrs, no children, ABC1, large town]

"At least if you know, then you know, don't you"... "They know they're going to be on camera. You can't say it's an invasion of privacy if they've told you they're going to do it; do you know what I mean?"

[Young men 18-24 yrs, no children, C2DE, Suburban]

Finally, if there were no signs to alert wrong-doers, then the prime purpose of surveillance, to deter criminal activity, would be frustrated. So signs were essential to prevent crime.

"They should let everyone know that there are cameras, so therefore when a person walks into a room they know not to do anything."

[Afro-Caribbean young men 18-28 yrs, Inner city]

A few felt that signs might be unnecessary in public places where the presence of CCTV cameras would normally be expected, because people would already know they were there.

"It is just to make people aware that there are CCTV cameras in operation that you would not normally find as general knowledge. Like we have said, generally people know they are in shops. I mean you go to a car park and it says 'this car park is operated by CCTV', and that to me is a good thing because I think if there is CCTV it feels safer."

[Women with young children, 21-40 yrs, C2DE, Inner city]

Perhaps because of the low saliency of much CCTV activity, respondents were not generally sure whether current signage was adequate, or not. However, the finding that they were so uncertain as to who was mainly responsible for the operation of CCTV in public places (see Section 1.6 above) indicates that signs were possibly not as prominent as the current Code of Practice appears to recommend.

Quality of images

Unless surveillance images were of sufficiently good quality to identify correctly the miscreants caught by the camera, they were no use for crime prevention.

Just as important was that innocent people should not be mis-identified by mistake.

Some respondents knew from personal experience that the quality of images was not always up to the job; others were made aware of this possibility through participating in this research. Either way, they were adamant that minimum quality standards should be imposed on organisations responsible for surveillance, and that inadequate equipment should be upgraded, or withdrawn.

“Surely there should be a standard brought in for ‘cameras ought to be able to do that’ – calibration of cameras”... “If they’re going to use something for prosecution purposes, it should be of a certain standard.”

[Men with young children, 21-40 yrs, ABC1, Small town]

The strictures in the ICO’s current CCTV Code of Practice on quality of images would appear, from the testimony in this research, to be widely flouted.

Corroboration evidence

Because of the possibility of surveillance images leading to mis-identification and ‘false positives’, many respondents, from all ethnic and demographic backgrounds, felt that additional evidence of wrongdoing should be required before suspects were apprehended.

“When the camera moves and catches us... when there was mis-identification because it looked like the person it wasn’t, then I am trying to think of what else they might have to have. Another form of evidence, not just the camera.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

Treating people as criminals simply on the basis of having been present at the scene of a crime, even if the images were good enough to identify faces, was also criticised.

Young men from ethnic minority communities were already conscious of the risks of “stereotyping”, and CCTV was sometimes felt to increase the likelihood of being unfairly targeted.

This rule, that surveillance images should be corroborated by independent evidence, was considered to apply at the investigation stages of a case – long before a potentially innocent individual was taken to court.

This is the one case of a rule desired by ordinary members of the public, not being covered in the ICO’s current CCTV Code of Practice.

Security of images

Respondents considered that surveillance images should be proof against tampering, theft, or unauthorised disclosure, because of the risks of incrimination or other harm to innocent individuals.

Security seemed to them to be mainly a question of technology: surely it was possible for equipment to be designed to prevent human interference with recordings, or at least to show that interference had occurred, and/or to register occasions on which recordings were played back or tape was removed.

“You could just make it so like you can’t doctor the tape, the tape goes onto like a computer database, and you can’t get access to it.”

[Young men 18-24 yrs, no children, C2DE, Suburban]

Operators

The standard and professionalism of operators was recognised to be a key to the proper capture and processing of surveillance images.

“They’re probably not dishonest; they’re probably really nice people, but they’re not the brightest sparks if they’re doing that.”... “Security staff should be screened.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

The obligation to protect the confidentiality of personal images was perhaps the major issue for respondents.

If operators did not know how the equipment worked, or what were their data protection or other responsibilities towards the people whose images were caught on camera, then mistakes or worse might happen.

“They should have some sort of check, like schoolteachers have police checks. You could have a dirty pervert on there just getting his kicks looking at people.”

[Women with young children, 21-40 yrs, C2DE, Inner city]

Insofar as operators had previously been thought about at all, it was widely assumed that they would be low-paid and therefore probably low calibre, with few other employment options. But ideally, given their responsibilities, operators should be skilled, honest, reliable and motivated workers.

Minimum standards for selecting and training operators were therefore required, even if respondents could not be much more precise than this about the details.

Some also felt that applicants ought to be vetted by the Criminal Records Bureau or equivalent body, especially if they would have access to footage of children.

“They need to be security checked, because at the moment we have a lot of people getting hold of a lot of information – they are getting a lot of data and getting to see us through CCTV, and we don’t know what kind of background they have.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

The ICO’s current CCTV Code of Practice does not cover selection and training of operators as such, though it does allude in several places to standards of conduct.

Disclosure

Respondents insisted that consent ought to be obtained from the individuals portrayed to their images being shown to third parties, especially for a purpose different from why they had been recorded in the first place.

“My details are mine, personal... If I want to give it to somebody I’ll say yes to them, or sign a bit of paper.”

[Older women 50-75yrs, C2DE, Small town]

This rule was prompted by Scenario 1 in particular, and the events described in some of the other stories too verged on the unjustified interference with personal privacy.

Redress

As well as access to their own personal images, many respondents went further and wanted rules about redress for individuals harmed by misuse of surveillance information.

“If there was somebody that you could complain to, if you weren’t happy with what was going on, and they could then take up that case – like these Ombudsmen, etc. etc. – I think there should be somebody somewhere who should be able to take it up on your behalf.”

[Men with young children, 21-40 yrs, ABC1, Small town]

“I’d like to know what to do if I felt my personal liberty had been infringed, or misused, by CCTV.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

They seemed fairly vague about what compensation wronged individuals might be able to claim and, more importantly, how they might go about complaining – to whom, and how.

This emphasises the need for signs in situ to state clearly the contact details of the organisation responsible for the surveillance equipment – as prescribed in the ICO’s current CCTV Code of Practice.

6.4 Data linkages

There were sporadic references spontaneously to the proposed ID cards for UK citizens, but mostly in fairly approving terms.

“Fine with me, if that can cut down on fraud”... “They’re not going to actually follow up on anybody that’s not done anything wrong, are they... I want them just to home in on whoever’s doing what they shouldn’t be doing.”

[Women with older children, 35-54 yrs, ABC1, Suburban]

The idea of being able to prove one’s identity incontrovertibly was appealing, rather than worrying.

A few respondents questioned the need for ID cards, given that driving licences and even passports were going over to laminated photocard format, capable of being read electronically – surely these were good enough?

But no-one seemed to object to ID cards on principle, nor to foresee any dangers in the potential for ID cards to link into personal information from a variety of official databases to build up an overall picture of an individual’s history and circumstances. On the whole, people felt that if the authorities wanted to be able to do this, they would do it anyway, with or without the help of ID cards. But the perceived risks seemed small and distant.

The thought of commercial organisations being able to link personal data from different sources was more objectionable. The capacity to target marketing materials to individuals was already fairly formidable, without commercial organisations acquiring yet more tools in their armoury. Responses to the concept of RFID (section 3.6 above) exemplified their views.

7 Young people

While most of the young people in the sample shared many of the same assumptions and attitudes with regard to surveillance as their elders, it was noticeable that mistrust was mainly to be found with this age-group.

“We don’t know who is using it, who in particular is watching us, and what it is used for.”

[Young women 18-24 yrs, no children, ABC1, Large town]

“You think most people aren’t doing anything, this is the thing... They shouldn’t be followed”... “This is the dilemma, isn’t it – you want to catch people who are doing something... So what do you do? How can you identify them without watching everybody?”... “Because like CCTV cameras, it’s just like a policeman that doesn’t move, isn’t it. It looks around and it sees what’s going on and it’s like cheaper than a policeman. But when they start getting microphones and lasers and tagging and everything else, it’s not like an extra policeman that’s cheap, it’s like evil. They’re watching things that don’t need to be watched.”

[Young men 18-24 yrs, no children, C2DE, Suburban]

They were also sometimes more sceptical about the effectiveness of CCTV in preventing crime, than their elders.

“If I know there’s a camera there it doesn’t bother me, because I’m just shopping and they can watch me if they want, whereas if it’s a thief then they’ll be aware of it. I don’t think it would really deter them.”

[Young women 18-24 yrs, no children, ABC1, Large town]

The views of a handful of the young people, especially from minority communities, tended almost towards paranoia.

“There has to be a day where you have to have privacy. I genuinely believe that England is becoming a place where everything will be monitored, everything is logged. When I first saw CCTV years ago do you realise how big cameras were? They were massive. Now you can get small size cameras. A pen can be a camera and I have actually seen it in real life where you have a conversation and someone set a pen up like that and a camera is looking right in your face”... “It bothers me so much but there is nothing you can do about it. I heard that these Freemasons can tell from the moment you leave your house, they can tell if you go to the continent and for how long. They can tell where you work”... “Bill Clinton and everybody is in the club”... “And Michael Jackson. Seriously. They have got control over the whole world.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

This may have been partly due to a profound ignorance about legal constraints, processes and regulation surrounding surveillance, leading to a misinterpretation of purposes and powers. Some young people knew even less about controls over CCTV than older people, and possibly expected less in the way of protection. So it was easy to imagine the worst – that surveillance was a tool to spy on their privacy, for unknown reasons.

This perception resonated with the anti-authority, non-conforming mindsets and indeed lifestyles of some young people. Adult rules and codes of behaviour were to a large extent beyond understanding. They were accepted in the sense that disobedience was known to lead to punishment, but this did not mean you had to agree with them. Surveillance was simply another aspect of this mysterious adult world, which imposed its own strange and incomprehensible rules on the young.

“You know we are in a day now where you don’t know what is right or wrong. There is that thin line... There used to be a big line, like for example, you smacking your child, whatever you do to your child. When I was younger I used to get licked with a pot and things like that. Now you can’t shout at a child in a certain way, or you can’t spank them on their bottom because it is classed as assault. There is a thin line between what is right and wrong nowadays. I could take a picture of you just out of the blue with my camera phone and you could turn around and say that is invasion of privacy.”

[Afro-Caribbean young men 18-28 yrs, Inner city]

Another factor may be the childhood exposure of today’s young people to science-fiction entertainment – good guys and bad guys fighting each other with efficient and sophisticated weapons and other technology that defied explanation. There were signs among a few of the young people in the sample of exaggerated fears about the power of surveillance equipment, and its prevalence, and this may have been why.

Although such extreme responses were rare, the finding that young people tended to be more mistrustful of surveillance, and its whys and wherefores in civil society, may give future cause for concern. Young people may be even more susceptible to bad publicity about misuse of surveillance, and withdraw their acceptance more readily.

APPENDIX I

Discussion Guides

SR080
January 2004

DISCUSSION GUIDE
Part I

1. Introductions

Purpose of research
Respondent names, occupations, family at home

2. CCTV experiences

Personal experiences of CCTV: where and when
NB: CCTV IN PUBLIC PLACES
BUT CHECK FOR MENTIONS OF PRIVATE PLACES
Other experiences – eg. TV: news items; crime programmes; entertainment
Private showings??

Any other examples of surveillance technologies?

3. CCTV knowledge and awareness

Where is CCTV installed? UNPROMPTED, KEEP PROBING
(petrol forecourts, schools, railway stations, kerb crawling)

Why is CCTV there? What are the systems for?
CHECK FOR MENTIONS OF CRIME PREVENTION/DETECTION
(As you say) most CCTV systems are installed for the purposes of crime prevention or detection.

Thinking first about crime prevention, tell me how you think CCTV works to prevent crime?

How do the police use CCTV to prevent crime?

Who installs/operates CCTV systems?
CHECK FOR MENTIONS OF LICENSING/AUTHORISATION

What happens to the recordings?
Who looks at them, and why?
How long are they kept for?
CHECK FOR MENTIONS OF SECURITY

How do you think Britain compares with other countries in terms of CCTV coverage? HIGHEST PER CAPITA COVERAGE IN THE WORLD
Reactions to prevalence

4. Public spaces

“We are mainly interested in people’s thoughts about CCTV in public places, or public spaces. Tell me what you would think of as included in the term ‘public spaces?’” MAKE LIST

If or when you know that there is CCTV installed in a public place, how does that affect your behaviour, or your mood or how you feel?

“Some people really object to CCTV in public places. What sort of people do you think they are, and why do you think they object?”

5. Associated technological developments

What other surveillance technologies can you think of, similar to CCTV, or used in association with CCTV?

SPONTANEOUS, THEN PROMPTED

- Infra-red – for low light, darkness
- Facial Recognition systems (identifying the patterns created by the structure of a face)
- Speed cameras and Automatic Number Plate Recognition
- London Congestion Charging cameras
- Road pricing cameras with ANPR
- RFID (READ OUT DESCRIPTION)
- MWI (Millimetre Wave Imaging)
“This produces images derived from passive radiation from the human body, and shows whether the person has items like weapons hidden under clothing. The effect is that the image produced looks as though the person has no clothes on.”

6. Misuse of CCTV

Do you know of any examples of CCTV recordings being misused?
Can you think of any ways in which CCTV recordings might be misused?
What disadvantages/damage to individuals are caused/brought about by these examples of misuse?

7. Data Protection

What controls on CCTV do you know about? SPONTANEOUS
What authority exercises control, or grants licences?

Do you think that local people should have a say in deciding whether CCTV is installed in a particular place?

What about local businesses, such as shops or pubs?

Have you heard about the Data Protection Act 1998?

What do you know about the Act, or about data protection generally?

Have you heard of the Information Commissioner, who is responsible for enforcing the Data Protection Act 1998?

“The principles of data protection apply to all forms of personal information, including CCTV recordings that can be used to identify individuals. Does this make sense to you?”

Let’s look at each of the 8 data protection principles, one at a time, and see how they could or should apply to CCTV recordings of ordinary people, in public places.”

SHOW DATA PROTECTION PRINCIPLES – one at a time

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date
- not kept for longer than necessary;
- processed in line with the data subject’s rights;
- secure;
- not transferred to countries without adequate protection.

What do each of these principles mean?

Is each one a good thing, or not?

CHECK FOR SPONTANEOUS MENTIONS OF INFRINGING
PERSONAL PRIVACY

What effects do you see for personal privacy? Self/others (who?)

“NB: Personal privacy is one of the rights guaranteed by the Human Rights Act 1998.”

Tell me more about what you think about ‘personal privacy’. Is it a good thing? Always?

Do you think everyone should be entitled to privacy? Celebrities?

OVERALL:

Breaking any of these principles could imply misuse of CCTV recordings – can you think of any examples of how this might happen?

What disadvantages/damage to individuals might be caused by these examples of misuse?

“The data protection laws allow for some circumstances in which personal privacy can be intruded on, or interfered with, by the state. Can you think of any circumstances in which you think it would be acceptable to intrude on personal privacy by the use of CCTV?”

SPONTANEOUS

THEN PROMPT, SHOWING CARD/S:

- national security
- public safety
- economic well-being of the country
- prevention of disorder or crime
- protection of health or morals
- protection of rights and freedoms of others

What do each of these mean?

Is each one an acceptable reason for ignoring or overriding people’s personal privacy, or not?

What effects do you see for personal privacy? Self/others (who?)

INTRODUCE TASKS FOR NEXT WEEK’S SESSION:

“I am going to give you four case histories to think about over the next few days, and we will discuss what you make of them at next week’s session. These are fictional, made-up stories, though they are based on real life.

Please by all means show them to family or friends to see what they think, though it will be your opinions that we will be interested in discussing next week.”

DISTRIBUTE CASE HISTORIES, PLUS COPY OF DP PRINCIPLES

SR080
January 2004

DISCUSSION GUIDE
Part II

1. First scenario – discussion

What did you think about the story?
Was CCTV misused in this story; if so how?

PROBE SPECIFICALLY THE ASPECTS REPRESENTED IN THE
SCENARIO (see attached Analysis):

What did you think about this (SPECIFIC ASPECT)?

LOOKING AT DP PRINCIPLES CARD

Any other aspects involved?

What changes to the story would have made CCTV more acceptable?

What would have made it less acceptable?

2. Second, third, fourth scenarios – discussion

AS ABOVE

3. Issues Revisited

Have you had any further thoughts about:

- Where CCTV is installed; acceptable for CCTV to be installed: PUBLIC SPACES
- Feelings of safety where CCTV is installed: FEAR OF CRIME
- Objectors to CCTV – who and why; sympathy with objectors: CIVIL LIBERTIES
- Who benefits from CCTV
- Who suffers from CCTV, or is disadvantaged: CIVIL LIBERTIES
- Controls on installation of CCTV: LICENSING
- Technological developments
 - Facial Recognition systems
 - Roadside cameras
 - Satellite cameras which identify vehicles
 - RFID
 - MWI

4. CCTV acceptability

Now that we have talked and thought about CCTV a bit more, would you say that you were in favour, or not? A lot or a little?

What rules do you think would make the use of CCTV better, or more acceptable to the general public?

Who benefits from CCTV?

SPONTANEOUS THEN PROMPT:

The general public?

The police and other law enforcement agencies?

What do you imagine is the attitude of the police towards CCTV?

What would say are the risks of CCTV being misused?

Is it a high risk, ie. very likely, or a low risk, ie. very unlikely?

Do you think that CCTV threatens personal privacy?

Whose privacy? Yours, other people's?

How can any risks be minimised?

5. Summary of response

APPENDIX II

Scenarios:

- 1
- 2
- 3
- 4
- 5
- 6
- 8
- 9
- 10
- 11

Scenario allocation table

SCENARIO 1

CCTV footage from Middlebury town centre was included in a promotional video aimed at a business audience to attract retail investment into the town.

At one of the exhibitions during which the video was shown, a member of the audience recognised her husband, filmed walking along arm-in-arm and apparently in intimate conversation with a woman she did not know.

That evening at home she challenged her husband, who denied ever having visited Middlebury. She did not believe him, and walked out of the house.

Shortly afterwards she instigated divorce proceedings and took her children away from their father.

The husband was on the point of finishing the affair with the other woman, and was distraught by the break-up of his marriage.

SCENARIO 2

Lobby ATMs for Noreast Bank were fitted with CCTV, which routinely photographed people using the ATM to get out cash.

A stolen card showed up on the Bank's records as having been used at one particular ATM, and the Bank passed the CCTV film over to the police. They matched every face recorded at the ATM against their video database of local suspects, and found two who looked similar to faces captured on the CCTV film from the ATM. Both these individuals were brought into the police station and kept overnight for questioning. Both denied the offence.

One of the men was due at a party that evening to celebrate his mother's birthday, and was not allowed to attend.

The following week the stolen card was found in a rubbish dump and fingerprints were taken. These did not match either of the two suspects who had been brought in the previous week. The offender was eventually caught and successfully prosecuted, as a result of the fingerprint evidence.

SCENARIO 3

The Redbush area of big city was suffering from an upsurge in on-street drug-dealing. The problem was believed by local residents, many of them Asian, to be caused by members of a particular gang based in another area of the city, seeking to expand their territory. The gang consisted mainly of young Asian men.

Redbush had a busy railway station, where CCTV was installed at the exit. The police had reason to believe that members of the gang were travelling to Redbush by train rather than driving. The CCTV footage was used by the police to identify all the young Asian men using the station to get to Redbush in the evenings after the rush hour, more than once in a particular week.

Around 20 individuals were identified, and brought into the police station for questioning and told about the CCTV evidence against them. Drugs were found on one of the suspects and he was arrested. The others were all released.

SCENARIO 4

Hizview, a company specialising in Internet broadcasting, came up with the idea of obtaining footage of people at work by persuading employers to install CCTV cameras to protect their premises – against break-ins, theft and vandalism, etc.

Cameras were installed in warehouses, car parks, and staircase and lift lobbies. Microphones were also fitted, so that conversations could be recorded too.

Hizview monitored all the CCTV recordings back in their own offices.

For the employers, ie. their customers, they provided footage of any incidents that looked suspicious in terms of possible criminal activity – theft or break-ins, for example – for the employer to investigate and follow up.

In addition, Hizview also looked for CCTV footage of employees having sex in the areas covered by the cameras, together with the audio recordings. They put together a film of these sex scenes, which they then broadcast on the Internet. For a fee to Hizview, anybody anywhere in the world could watch this film.

No attempt was made to disguise the identities of the people or companies involved, though they were not actually named.

SCENARIO 5

The government of the Republic of Ombria was worried about illegal immigration.

Officials decided that airlines operating flights into Ombria from outside the country should be required to supply advance information about all their passengers.

At the beginning, the airlines were asked to provide details of individual passengers' names, passport numbers and credit card accounts.

Shortly afterwards, the government demanded CCTV footage of airline passengers, filmed close-up on boarding the aircraft, to be sent over to the arrival airport's immigration officials before the aircraft landed.

Passengers were not advised that the filming was taking place.

SCENARIO 6

A&B, a chain of clothing retailers, had a policy of not providing changing rooms where customers could try on garments, because it was too expensive in staff supervisory time. Instead they could take them home, and return them if they did not fit or the customer did not like them.

A&B was suffering from trading losses because of shop-lifting, which in some stores was reaching high levels.

They suspected that some of the stolen goods were later being returned and exchanged for credit notes, and that some of these shop-lifters were probably persistent offenders.

So the company decided to try and identify shoppers who regularly returned goods to exchange for credit notes, to see if they could catch the shop-lifters.

They set up CCTV cameras to film every customer returning unwanted purchases at the Customer Service desk.

Facial images of all these customers were stored.

Every customer returning goods for the third time in a six-month period was identified at the Customer Service desk, and called in for interview by security staff.

These customers all had to prove their name, address and date of birth, and this information was then sent to the police to be checked for any criminal record. The customers were also questioned in detail about their purchases from the store.

Customers who were found not to have committed any crime had their personal details added to A&B's marketing database. This meant that they would in the future be sent direct mail packs.

SCENARIO 8

CCTV cameras were installed in the shopping centre at Bunton.

The images were monitored by operators based in a control room on the site.

One day, a disturbance broke out on the main floor of the shopping centre, involving threats and punches. Someone pulled a knife. The security personnel were called and broke up the fighting.

Joe, one of the CCTV operators watching the film as these events were happening, recognised one of the attackers as a friend.

Joe realised that the CCTV footage would be used as evidence in prosecuting the attackers. To protect his friend, therefore, he decided to doctor the film so that he could not be identified. He simply removed all traces showing his friend – as if he had never even been there.

The other men involved in the fight were identified from the CCTV footage, and arrested by the police.

SCENARIO 9

The high street of the town of Littleborough had CCTV cameras installed, because of minor crime in the area.

CCTV footage revealed that there were occasional incidents of snatching mobile phones. It looked as though there was a small gang of thieves involved, different people sometimes working alone, and sometimes in twos and threes. The police had not previously been aware of this problem, because the victims of these thefts, mostly teenagers, had not generally bothered to report the loss of their mobile phones.

Once the police became aware of the problem, they decided to concentrate on catching the thieves. One ended up in court and was convicted and fined.

This case received quite a lot of local publicity.

Shortly afterwards the problem of mobile phone theft disappeared from the high street. Reports then started coming in to the police from a nearby housing estate, where there were no CCTV cameras. Not only mobile phones were being grabbed from passers-by, but bags and rucksacks as well. Sometimes the owners were threatened with violence.

Local people began to think that maybe CCTV cameras should also be installed on the housing estate.

SCENARIO 10

The town of Greenborough had been planned with a network of dual-carriageway roads.

The Council decided to enforce the 50mph speed limit on these roads more strictly by installing speed cameras. They put up the correct signs, showing the words 'SPEED CAMERA' and a picture.

The cameras were in continuous operation, day and night. They were linked to an ANPR system (Automatic Number Plate Recognition), which identified through DVLA records the keeper of every vehicle breaking the speed limit. Fines were imposed on offending drivers.

After a few months, viewing of the camera footage showed that images had been picked up of people sleeping rough on the central reservations. These areas were quite wide, and had been planted up with shrubs to make the roadscape look attractive. There was also a water supply, with taps for hoses to help the landscape gardeners with watering the plants during dry spells.

The Council decided that they did not want people sleeping rough on the central reservations, and sent the police in before dawn one morning to round them up and disperse them.

SCENARIO 11

A demonstration march was taking place on the streets of the capital, to protest about plans for a new airport.

The march was covered by CCTV.

There were some minor disturbances when demonstrators were prevented from going down particular streets, but no arrests were made and on the whole the march passed off peacefully.

The CCTV film was afterwards used to make individual portraits of the marchers, which were then filed by the police for future reference, as they were expecting more anti-airport demonstrations to take place.

One of the demonstrators whose picture was filed in this way was in training to be a teacher. Her name was Kim. A few months later she applied for a teaching job in a primary school, and so police checks were made to ensure that she was a fit and proper person to work with children. At the time of applying for teacher training, similar background checks had been done on Kim, and no problems had been identified.

The new check, on behalf of the primary school, turned up Kim's picture at the demonstration, under the label of 'troublemaker'. The school was simply informed that Kim was a troublemaker, with no other explanation, and she was turned down for the post she had applied for.

Kim had no idea why she had been labelled as a troublemaker, and had great difficulty finding out what had happened.

SCENARIO ALLOCATION

| Scenario No: | 1 | 2 | 3 | 4 | 5 | 6 | 8 | 9 | 10 | 11 |
|--|---|---|---|---|---|---|---|---|----|----|
| Group No: | | | | | | | | | | |
| 1 Males, 18-24 years, C2DE, Suburban | | | ✓ | | | | ✓ | | ✓ | ✓ |
| 2 Females, 18-24 years, ABC1, Large town | | ✓ | | ✓ | | ✓ | | | ✓ | |
| 3 Males, 21-40 years, ABC1, Small town | ✓ | ✓ | | | ✓ | | ✓ | | | |
| 4 Females, 21-40 years, C2DE, Inner city | ✓ | | | ✓ | | | | ✓ | | ✓ |
| 5 Males, 35-54 years, C2DE, Inner city | | ✓ | ✓ | | ✓ | | | | ✓ | |
| 6 Females, 35-54 years, ABC1, Suburban | | | | | ✓ | ✓ | ✓ | ✓ | | |
| 7 Males, 50-75 years, ABC1, Large town | ✓ | | | ✓ | | ✓ | | | | ✓ |
| 8 Females, 50-75 years, C2DE, Small town | | | ✓ | | | ✓ | | ✓ | ✓ | |
| 9 Asian young men, C1C2D, Inner city | ✓ | | ✓ | | ✓ | | | ✓ | | |
| 10 Afro-Caribbean young men, C1C2D, Inner city | | ✓ | | ✓ | | | ✓ | | | ✓ |