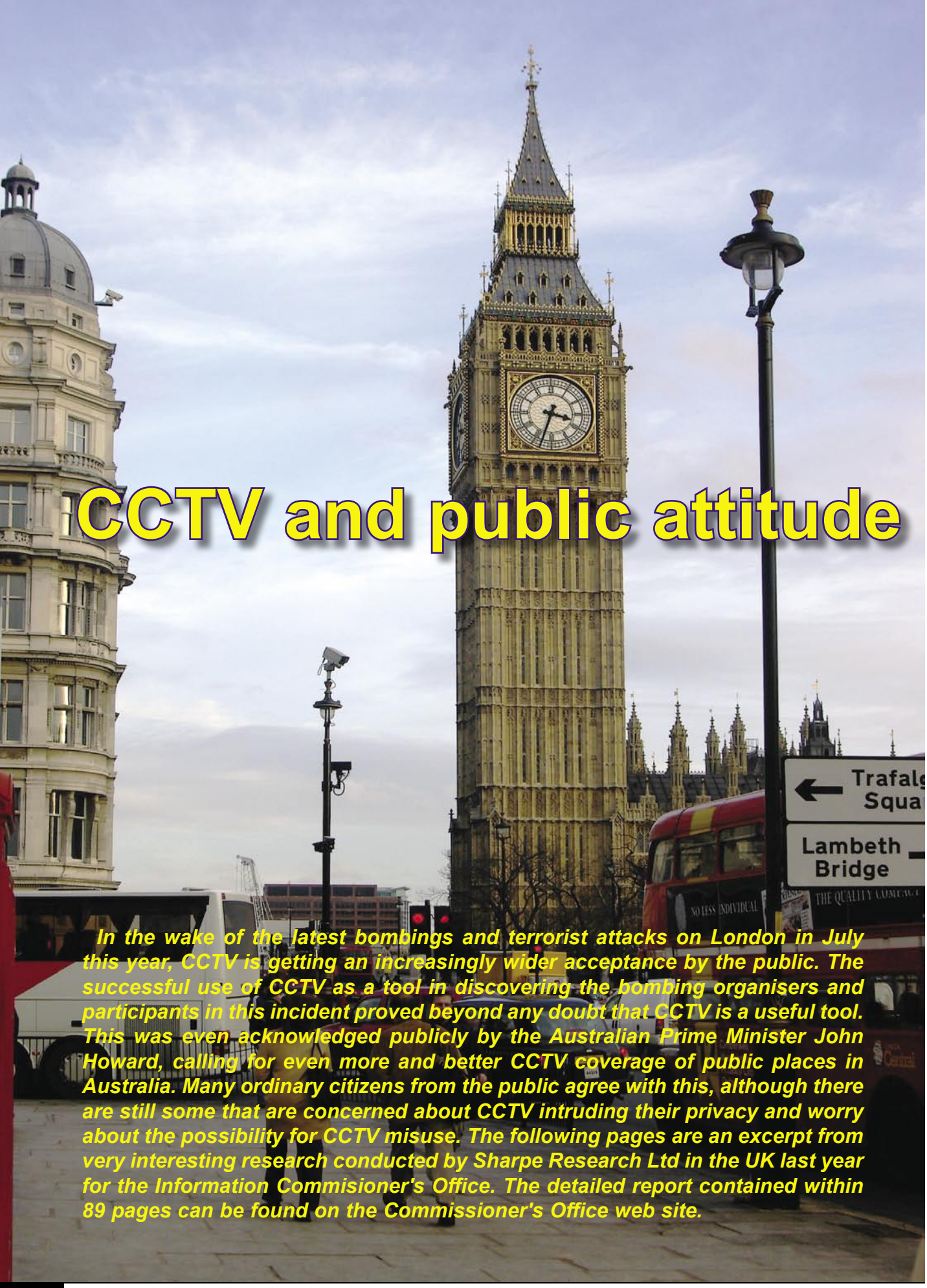

CCTV and public attitude

In the wake of the latest bombings and terrorist attacks on London in July this year, CCTV is getting an increasingly wider acceptance by the public. The successful use of CCTV as a tool in discovering the bombing organisers and participants in this incident proved beyond any doubt that CCTV is a useful tool. This was even acknowledged publicly by the Australian Prime Minister John Howard, calling for even more and better CCTV coverage of public places in Australia. Many ordinary citizens from the public agree with this, although there are still some that are concerned about CCTV intruding their privacy and worry about the possibility for CCTV misuse. The following pages are an excerpt from very interesting research conducted by Sharpe Research Ltd in the UK last year for the Information Commisioner's Office. The detailed report contained within 89 pages can be found on the Commissioner's Office web site.

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 wellinformed 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.

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 can be found in the original 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.

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


GOWINGS
George St
367 - 427
Monorail Station
WORLD CUP
RUGBY
2003
COLLECTION
GOWINGS

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 crimeprevention purpose of surveillance, if they are unable correctly to identify the perpetrators.

Corroboration evidence

The possibility of surveillance images leading to misidentification 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 surveillanceequipment 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. [•]

Source:
Iinformation Commissioner's Office
"Public attitudes to the deployment of surveillance techniques in public places,"
http://www.informationcommissioner.gov.uk