



Code of Practice Relating to Surveillance Cameras

JUSTICE response to Home Office Consultation

May 2011

For further information contact

Eric Metcalfe, Director of Human Rights Policy

email: emetcalfe@justice.org.uk direct line: 020 7762 6415

JUSTICE, 59 Carter Lane, London EC4V 5AQ tel: 020 7329 5100
fax: 020 7329 5055 email: admin@justice.org.uk website: www.justice.org.uk

Introduction and summary

1. Founded in 1957, JUSTICE is a UK-based human rights and law reform organisation. Its mission is to advance justice, human rights and the rule of law. It is the British section of the International Commission of Jurists.
2. We welcome the Home Office's consultation on a Code of Practice governing surveillance cameras, commonly if perhaps increasingly inaccurately known as CCTV.¹ JUSTICE has long argued for much stricter regulation of the use of surveillance devices, including CCTV, by both public and private bodies. In our 1970 report, *Privacy and the Law*, for instance, we recommended that the law should be changed:²

To make the use of electronic, optical or other artificial devices as a means of surreptitious surveillance a criminal offence except in certain clearly defined circumstances;

3. In our 1998 report, *Under Surveillance: Covert policing and human rights standards*, we argued again for much closer regulation of governmental powers in this area:³

To the extent ... that CCTV impacts on privacy and other rights, it should be subject to a regulatory framework which also includes effective data protection controls.

4. Sadly, the development of effective legal and practical safeguards for individual privacy continues to lag far behind the pace of technological developments and the uptake of surveillance technologies by both the public and private sector. Indeed, the UK has the dubious reputation as a market leader in the use of CCTV, including the greatest number of surveillance cameras, both per capita *and* in absolute terms.⁴ At the same time there is no single legal framework governing their use. Although the Data Protection Act governs certain aspects of CCTV usage (specifically the handling of sensitive personal data), it does not provide – and was never intended to provide – a comprehensive legal framework governing CCTV placement and usage. Similarly, the use of covert surveillance cameras by public

¹ We use the term CCTV generically. As the Royal Academy of Engineering noted in 2007, 'the term CCTV is now for the most part a misleading label. Modern surveillance systems are no longer 'closed-circuit', and increasing numbers of surveillance systems use networked, digital cameras rather than CCTV. The continued use of the term is an indicator of a general lack of awareness of the nature of contemporary surveillance, and disguises the kinds of purposes, dangers and possibilities of current technologies' (Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p33).

² *Privacy and the Law* (JUSTICE, 1970), p42.

³ *Under Surveillance: Covert policing and human rights standards* (JUSTICE, 1998), p31.

⁴ BBC News, 'The statistics of CCTV', 20 July 2009.

authorities is governed by a Code of Practice under section 71 of the Regulation of Investigatory Powers Act 2000 but this does nothing to regulate their non-covert use, nor the everyday use of CCTV by private companies and individuals.⁵

5. We therefore welcome the proposals for a Code of Practice governing surveillance cameras as currently set out in clauses 29-36 of the Protection of Freedoms Bill, and this consultation. At the same time, in the absence of a draft Code, it remains very much open to question whether the clauses will deliver the stringent regulation of CCTV that is so plainly needed in order to check the growth of public surveillance. We have not addressed every question raised by the consultation paper but only those relevant to the issues referred to above. In outline we argue that:

- Insufficient weight appears to have been given to the importance of the right to privacy under article 8 ECHR at the pre-planning stage;
- It is essential for the Code of Practice to apply to all surveillance cameras used by public and private bodies alike;
- Although some kind of oversight arrangement is essential, we question whether the creation of a special Surveillance Camera Commissioner is necessarily the appropriate way forward. On balance, we favour regulation of CCTV and ANPR to be carried out by the Information Commissioners Office, with appropriate powers to enforce compliance;

Q1. What other preparatory checks or balances should be included?

6. In our view, the suggested list of preparatory check attaches insufficient weight to the importance of privacy. Although the checklists suggested by the consultation paper makes reference to privacy, it does so only as one of several impact assessments 'including environmental, privacy, disproportionality, etc'. Moreover, the reference to 'disproportionality' as a separate ground from privacy is unclear. Under section 6 of the Human Rights Act, it is axiomatic that a decision to install surveillance cameras in a particular case must involve

⁵ In 2003, for instance, the European Court of Human Rights found that the lack of any legal remedy for a Mr Peck whose failed suicide attempt was captured on CCTV and then distributed to the media by the local authority meant that the UK breached his right to privacy under article 8 ECHR. In another privacy case in 2004, Lord Hoffmann rejected the argument that this required the courts to develop a tort of invasion of privacy: 'Counsel for the Wainwrights relied upon Peck's case as demonstrating the need for a general tort of invasion of privacy. *But in my opinion it shows no more than the need, in English law, for a system of control of the use of film from CCTV cameras which shows greater sensitivity to the feelings of people who happen to have been caught by the lens*' (*Wainwright v Secretary of State for the Home Department* (2004) 2 AC 406, para 33. Emphasis added).

some assessment as to whether it would be a proportionate interference with an affected person's right to privacy under article 8 ECHR. The consultation paper, by contrast, appears to suggest that assessing 'privacy' and 'disproportionality' are separate exercises. In our view, the importance of the right to privacy requires much more detailed assessment of the likely impact of CCTV usage upon privacy at the outset.

Q3. Do you think it would be beneficial to establish a common technical standards baseline for the surveillance camera industry?

7. We can see some benefits to promoting common technical standards for the surveillance camera industry. However, we believe that compliance in this area should be voluntary. Certainly private manufacturers of surveillance equipment should not be obliged to 'facilitate the integration of systems where this was deemed desirable' by government, nor should they be required to make 'the collection of evidence for law enforcement purposes easier and more efficient'.

Q7. What other (non-technical) issues might benefit from the adoption or development of key standards?

8. We welcome the consultation paper's suggestion that the Code could also 'seek to deal with expectations on individuals operating surveillance systems or handling the data captured by them, including core training issues'.⁶ In our view, training requirements should include detailed guidance concerning relevant human rights standards, especially in the field of privacy and data protection.

Q8. Would it be helpful to combine the existing Information Commissioner's CCTV Code into a new single CCTV code, or maintain a distinction between data protection issues and other technical CCTV operational issues through separate codes?

9. We believe the provisions of the Information Commissioner's CCTV Code should be incorporated into the new Code. More generally, we would support the Information Commissioner having powers to enforce the Code's provisions, both in relation to data protection issues and other operational issues. Although any move to strengthen independent oversight of CCTV usage is something to be encouraged, we question whether the creation of a separate Commissioner in the field of surveillance cameras necessarily the best way to provide this oversight. Plainly, the extent of CCTV usage in the UK is significant and therefore oversight will inevitably require a certain level of resources. But the existing oversight framework of surveillance is already highly fragmentary and lacking in coherence. We strongly

⁶ Consultation paper, p14.

doubt that further fragmentation of oversight arrangements is desirable. Although we can see the case for a Surveillance Camera Commissioner to be appointed as an interim step, we believe that the most effective way forward in the medium and long-term is for the establishment of a more coherent scheme of independent authorisation and oversight of surveillance, including reform of RIPA itself.

Q9. Are there other issues relating to the collection, storage and subsequent use of data which should be included in the Code?

10. We agree with the Consultation Paper's suggestion that it would be helpful for the Code to provide further guidance on data retention periods, especially ANPR data; data sharing provisions and restrictions; and appropriate training levels for system operators.

Q13. How best can organisations be persuaded to adopt the principles of a new Code on a voluntary basis?

11. In our view, the Code should be mandatory.

Q14. Are there specific aspects of the proposed Code that should be made mandatory for all organisations?

12. In our view, the Code should be mandatory in its entirety.

Q15. Is there a need to regulate the use of CCTV and similar systems by private individuals? What issues should be covered?

13. All surveillance cameras operated by public bodies and all fixed surveillance cameras operated by private bodies should be governed on the same basis. Private companies and individuals account for a substantial number of surveillance cameras in the UK. And, as the consultation paper itself notes:⁷

In many local areas, there has been a deliberate integration and networking of publicly and privately owned systems in recognition of the blended nature of the space in which we conduct many of our day to day activities and in order to maximise the benefits of CCTV coverage of these areas.

⁷ P6.

The consultation paper similarly highlights the lack of regulation governing the use of ANPR by private companies.⁸

There is much less clarity around the use of ANPR by private companies, for example in monitoring private premises and car parks and how data is then used or exchanged with other parties. Whilst the Police Service has agreed standards for the quality of data it collects, no such standards exist for private companies.

In light of the above, it is evident that any failure to regulate the use of CCTV and ANPR by private companies and individuals would drive coach and horses through the very purpose of the Code of Practice as a safeguard against unwarranted interference with the right to privacy.

Q16. Are there other surveillance camera technologies in operation or development for which guidance or legislation may be required?

14. The consultation paper draws attention to a broad range of surveillance camera technologies, including 'the mounting of cameras in helicopters and aircraft'; 'body worn' personal video cameras used by individual officers in particular situations'; and 'emerging technology such as remote controlled unmanned airborne vehicles'.⁹ Although these may raise some novel issues, we see no reason why such new technologies should be exempted from the framework for regulation surveillance cameras.

ERIC METCALFE
JUSTICE
25 May 2011

⁸ PP8-9.

⁹ P11.