



## Revision of 6 January 2010

This document supersedes the [version of 14 October 2009](#)

### The Scope of This Policy Statement

The scope of this Policy Statement is Visual Surveillance, such as that conducted using Closed-Circuit Television (CCTV).

The term is used here to encompass **the capture and/or projection of images and video**, whether or not with audio, whether or not the images and/or audio are recorded, whether or not they are subsequently disclosed and/or published, and whether the image-resolution is high- or low-quality.

The focus is on visual surveillance **conducted in a systematic manner**, as is generally the case with its use by organisations. The scope is not intended to encompass casual use of cameras by individuals, which gives rise to privacy concerns that are of a different nature and gravity from institutionalised uses.

The focus is on **data that represents images and any associated sound**. Structured and textual data deriving from such images, including meta-data describing them, are also a source of considerable privacy concern, and must be subject to data protection provisions.

The Principles enunciated below also have broader application, to surveillance conducted using **any part of the electromagnetic spectrum** including that outside the human-visible range, such as infra-red, ultra-violet and X-rays.

### The Principles

Visual surveillance may have potential in particular circumstances to protect important human values. On the other hand, visual surveillance is highly privacy-intrusive. It has a chilling effect on human behaviour generally.

Moreover, unless it is well-designed and well-managed, visual surveillance may have little or no chilling effect on criminal or anti-social behaviour. Studies have created serious doubts about the effectiveness of visual surveillance as a technique for crime prevention, for crime detection, for criminal investigation and for criminal prosecution.

Wherever visual surveillance is applied, all of the following conditions must be fulfilled.

#### 1. Justification

Because visual surveillance is highly privacy-invasive, a Privacy Impact Assessment (PIA) must be conducted before a scheme is commenced or significantly changed. A PIA involves publication of a clear explanation, demonstrating that it is expected on reasonable grounds to have positive benefits sufficient to justify its intrusiveness, followed by public consultation.

The explanation must be based on evidence and systemic reasoning, and not merely rely on assertions.

The justification must make clear what less privacy-invasive alternatives have been considered, and why they are inadequate.

#### 2. Proportionality

The benefits identified in the justification for using visual surveillance must outweigh the negative impacts on privacy.

Visual surveillance must be no more intensive (e.g. the number of cameras), and no more extensive (e.g. across a large area) than the analysis justifies.

#### 3. Openness

The conduct of visual surveillance **in any open space** (whether it is public or is commonly used by members of the public) must be disclosed to the public, and clearly notified to individuals who enter that space. This applies to both the fact that visual surveillance is undertaken and the nature and extent of the surveillance. Any exceptions to this must be treated as covert surveillance (see below).

Before visual surveillance is conducted **in any space in which a reasonable expectation of privacy exists** (including private premises, and toilets and change-rooms in open facilities), it must be the subject of formal, specific and bounded legal authority, exercised by a judicial institution that makes its judgements in a manner demonstrably independently of the organisation that seeks to conduct the surveillance. It must also be disclosed to the public, and clearly notified to individuals who enter that space. This applies to both the fact that visual surveillance is undertaken and the nature and extent of visual surveillance. Any exceptions to this must be treated as covert surveillance (see below).

Before **covert visual surveillance** is undertaken, it must be the subject of formal, specific and bounded legal authority,

exercised by a judicial institution that makes its judgements in a manner demonstrably independently of the organisation that seeks to conduct the surveillance.

Where a recording is made, and the images and/or video are such as to identify any individual, the data must be treated as **personal data**, and must be subject to data protection laws, including access by the data subject, complaint handling, and redress.

#### **4. Access Security**

Access to images and video, both live and recorded, must be tightly controlled, ~~and a~~

Any security breaches must be acted upon promptly and effectively.

#### **5. Controlled Use**

The purposes must be clearly defined for which the images and video, both live and recorded, may be used by the organisation that collects it.

Use for any other purpose must be precluded, and must be subject to sanctions and enforcement.

The material may of course be used under legal authority.

#### **6. Controlled Disclosure**

The purposes must be clearly defined for which the images and video, both live and recorded, may be disclosed to other parties.

Disclosure for any other purpose must be precluded, and must be subject to sanctions and enforcement.

This provision applies to all parties, including law enforcement and national security agencies.

The material may of course be disclosed under legal authority, such as a search warrant.

#### **7. Controlled Publication**

Any publication of material must be justified, and must be the minimum necessary to achieve the aim. This applies with particular force to the publication of images of 'innocent bystanders' and of witnesses to an event.

Wherever possible, images of 'innocent bystanders' and of witnesses must be anonymised. The same principle applies to all other forms of information that may identify an individual, such as images showing number plates.

#### **8. Cyclical Destruction**

Any recordings that are made as a result of visual surveillance must be retained only for a brief period.

A defined program must be in place to ensure destruction of recordings.

Failure to destroy recordings in compliance with the program must be subject to sanctions and enforcement.

The material may of course be retained where a legal requirement exists to do so. However, the terms of the legal authority must be subject to Principles 1 and 2 (Justification and Proportionality).

#### **9. Review**

All aspects of a visual surveillance program must be reviewed, both periodically and as circumstances warrant, in order to establish whether these Principles are being complied with, and a review report prepared.

Where the review identifies problems, corrective action must be taken.

To ensure that this Principle is honoured, authority for visual surveillance must be subject to a sunset clause.

The sunset clause must include the requirement that a comprehensive review report be input to the re-authorisation process.

Review reports must be made publicly available, or at least sufficient information from them must be made publicly available, in order to enable informed public debate.

#### **10. Withdrawal**

A visual surveillance scheme and associated infrastructure must be de-commissioned and removed where it has demonstrably not fulfilled its objectives, where resources necessary to enable its objectives to be fulfilled are not available, or where an alternative with superior effectiveness and/or a superior privacy trade-off is available.

---

#### **Some Resources**

- **Guidelines**

EDPS (2009) ['Video-Surveillance Guidelines, \\*\\*Consultation Draft\\*\\*'](#), European Data Protection Supervisor, 7 July 2009

ICO (2008) ['CCTV Code of Practice'](#) Information Commissioner's Office, UK, 2008

NSW (2000) ['CCTV in Public Places'](#) NSW Government Policy Statement and Guidelines, 2000, and the [Review](#), 2001

NZPC (2009) ['Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations'](#) New Zealand Privacy Commissioner, October 2009

OPCC (2006) ['Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities'](#), Office of the Privacy Commissioner of Canada, March 2006

'Standards' – BSI guidelines, BS 7958:1999

- **Evaluations**

BBC (2008) ['CCTV boom 'failing to cut crime''](#), BBC News, 6 May 2008

CITRIS (2008) ['CITRIS Report: The San Francisco Community Safety Camera Program'](#), University of California, Berkeley, 17 December 2008

Webster C.W.R. (2009) ['CCTV policy in the UK: reconsidering the evidence base'](#) Surveillance & Society 6, 1 (March 2009) 10-22

Wells H., Allard T. & Wilson P. (2006) ['Crime and CCTV in Australia: Understanding the Relationship'](#) Centre for Applied Psychology and Criminology, Bond University, 2006 – short media report in Kerin L. (2008) ['Doubts raised over using CCTV cameras'](#), ABC News, 7 May 2008

Welsh B.C. & Farrington D.P. (2004) 'Evidence-based Crime Prevention: The Effectiveness of CCTV' Crime Prevention and Community Safety: An International Journal (2004) 6, 21–33; doi:10.1057/palgrave.cpcs.8140184

Whitehead T. (2009) ['CCTV only effective at cutting car crime'](#) The [London] Daily Telegraph, 18 May 2009

- **Resources**

CofE (2007a) ['Opinion on Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights'](#) European Commission for Democracy through Law (Venice Commission), Study no. 404/2007, 16-17 March 2007

CofE (2007b) ['Opinion on Video Surveillance by Private Operators in the Public and Private Spheres and by Public Authorities in the Private Sphere and Human Rights Protection'](#) European Commission for Democracy through Law (Venice Commission), Study no. 430/2007, 1-2 June 2007

EU Article 29 Committee (2004) ['Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance'](#) Article 29 Data Protection Working Party, Document 11750/02/EN WP 89, 11 February 2004

Urbaneye (2004) [The Urbaneye Working Papers Series](#), Centre of Technology and Society, Technical University of Berlin, August 2004

APF thanks its site-sponsor:



This web-site is periodically mirrored by [the Australian National Library's Pandora Archive](#)



Created: 2 September 2009 - Last Amended: 6 January 2009 by Roger Clarke - Site Last Verified: 11 January 2009  
 © Australian Privacy Foundation Inc., 1998-2011 - [Mail to Webmaster](#)  
[Site Map](#) - This document is at <http://www.privacy.org.au/Papers/Media-0903.html> - [Privacy Policy](#)