

DPA: Clarified or Confused?

Following a recent court case the Information Commissioner has issued a Guidance Note clarifying when a CCTV system does or does not need to be registered under the Data Protection Act¹. In this article, Ian Fowler, Norbain's Technical Training Manager, reviews the Information Commissioner's latest advice and suggests that rather than clarifying the law, the IC may have inadvertently put the industry back a step in its crusade to raise standards.



The case of *Durant v Financial Services Authority*² is totally unrelated to CCTV systems and yet its influence is already being felt throughout an industry that has long struggled to fully understand its relationship with the DPA. Recent industry press coverage has focused on the suggestion that users of smaller, simpler CCTV systems may no longer be required to register under the Data Protection Act. The latest Guidance Note³ issued by the Information Commissioner (IC) however, whilst sincere and genuine in its attempt at clarity, is in danger of creating confusion and leaving users unnecessarily vulnerable. It reveals implies an incomplete understanding of the nature of modern CCTV systems and the direction in which the CCTV industry is heading.

Privacy defined

The court case – the detail of which is not relevant to CCTV users – attempts to clarify when information relating to an individual is, or is not, covered by the DPA. Central to the court's judgment is that in order for information (in our case, CCTV images) to come under the terms of the act, the information must affect the subject's privacy. The court decided that two issues are central to deciding when this occurs:

- a) that a person has to be the focus of the information
- b) that the information tells you something significant about them.

The IC has deduced from the court's ruling that whether or not these conditions are met, and therefore whether or not the user needs to be registered under the DPA, depends on how large and sophisticated the CCTV system is and how it is used.

¹ All relevant documents are available as downloads from www.informationcommissioner.gov.uk

² *Durant v Financial Services Authority* [2003] EWCA Civ 1746, Court of Appeal (Civil Division), decision of Lord Justices Auld, Mummery and Buxton dated 8th December 2003

³ CCTV Systems and the Data Protection Act 1998 (DPA); Guidance Note on when the Act applies, JB v.5 01/02/04 available at www.informationcommissioner.gov.uk

To quote the IC's Guidance Note:

"If you have just a basic CCTV system, your use may no longer be covered by the DPA. This depends on what happens in practice. For example, small retailers would not be covered who:

- only have a couple cameras,
- can't move them remotely,
- just record on video tape whatever the cameras pick up, and
- only give the recorded images to the police to investigate an incident in their shop.

The shopkeepers would need to make sure that they do not use the images for their own purposes such as checking whether a member of staff is doing their job properly, because if they did, then that person would be the focus of attention and they would be trying to learn things about them so the use would then be covered by the DPA."

By focusing upon how a surveillance system is used as the determining factor in deciding whether the DPA applies, the IC has interpreted the court's thinking in a particular way that has both positive and negative repercussions. Moreover it changes fundamentally the existing understanding as to how to ascertain whether the DPA applies in a particular situation.

Image use

Prior to the IC's latest advice it has been commonly understood that any organisation processing data – including the capturing, monitoring and recording of CCTV images – requires the organisation to register with the IC and adhere to the terms of the DPA. One interpretation of the latest guidance however is that unless you can or intend to identify the individuals covered by the system, there is no need for registration or compliance with the DPA.



At this point it is important to distinguish between systems used solely for crime prevention and systems used for additional purposes. Whether or not a system is registered with the IC under the terms of the DPA, images that record criminal activity can be handed to the police as evidence. However, CCTV systems are increasingly used for purposes other than crime prevention and all such activity requires compliance with the DPA.

The most prevalent of these additional uses is staff management and monitoring. As the IC makes clear in the Guidance Note quoted above, CCTV footage from a system not registered under the DPA cannot be used in any civil tribunal or civil court and any such intentional recording or attempted use could be considered unlawful.

Clearly, if there is any intention to use CCTV footage as part of a management process specific to an identifiable individual, then the system must be registered under the DPA.

Identifying individuals

Rather than considering how the system is used, let us for a moment return to the two determining facts identified by the court. That is, that for personal data to come under the terms of the act, the person has to be the focus of the information and that the information tells you something significant about them.

It is reasonable to assume that if an individual is identifiable on the CCTV footage then both of the court's conditions detailed above are met. That is, if a person can be recognised, he or she is both the focus of the information and the information is telling you something significant about them.

This interpretation suggests that every CCTV system that records good quality images must be registered under the DPA regardless of its size or how the system is used. If the potential to identify an individual exists, then registration is essential in advance of an occasion when an individual is or needs to be identified. The type of CCTV system in use, the number and type of cameras and the type of recording technology involved is all irrelevant. What matters is the capability of the system to be used to identify an individual.



This line of thought opens the industry to the unwelcome possibility that an unscrupulous installer could promote their services as enabling a user to remain outside of the terms of the DPA, thereby increasing the number of poor quality CCTV installations. Any system that cannot identify individuals under surveillance need not register, but neither, of course, will any such recording be of much use to the police as evidence of criminal activity. Such a development is

neither in the interests of crime prevention nor an industry set on improving standards at every level. Nor is this simply a question of the quality of image capture and recording. A strict reading of the IC's guidance note is not going to help advance, for example, the installation of modern speed dome camera systems. Given that the whole technical thrust of the industry is towards quality image capture and the identification of individuals, any implicit encouragement not to register with the IC is unhelpful to the CCTV industry and to crime prevention.

Subject Access Rights

In one specific area, the IC's latest guidance on CCTV and the DPA will cause a huge sigh of relief throughout many a CCTV control room. The right of subjects to request access to a copy of their image are now considerably reduced. To quote direct from the IC (my italics):

*"In many CCTV schemes, such as are used in town centres or by large retailers, CCTV systems are more sophisticated. They are used to focus on the activities of particular people either by directing cameras at an individual's activities, looking out for particular individuals or examining recorded CCTV images to find things out about the people in them such as identifying a criminal or a witness or assessing how an employee is performing. *These activities will still be covered by the DPA but some of the images they record will no longer be covered. So if only a general scene is recorded without any incident occurring and with no focus on any particular individual's activities, these images are not covered by the DPA.* In short, organisations using CCTV for anything other than the most basic of surveillance will have to comply with the DPA but not all their images will be covered in all circumstances. The simple rule of thumb is that you need to decide whether the image you have taken is aimed at learning about a particular person's activities."*

The requirement to provide subject access rights to stored images 'on demand' has long given rise to concerns amongst users about the cost involved in fulfilling such requests. The IC now appears to be saying that not all such requests now need to be fulfilled as not all images recorded on a system registered under the DPA are necessarily subject to the DPA. This will require users to re-examine the policies and procedures in place to manage the fulfilment of subject access rights and could significantly lessen the burden of responding to such requests.

Conclusion

In summary, the IC's guidance note following the case of *Durant v FSA* does not provide sufficiently clear and robust advice for users to act upon it in complete confidence. Until the IC completes the extensive review of the existing CCTV Code of Practice currently in progress, it is strongly recommended that users act on the side of caution and presume the need to register in all circumstances. It could prove to be £35 well spent.