The law on using CCTV on your premises

Date : June 5, 2015

The Guidelines on CCTV and Surveillance

Closed circuit TV (CCTV) and other surveillance systems are now commonplace in most businesses. It's worth remembering however that using CCTV on corporate premises in the UK is subject to the Data Protection Act 1998 ('the DPA 1998'). If the DPA 1998 is breached by improper use of a CCTV system then companies and individuals risk an investigation, or even prosecution by the data regulator The Information Commissioner's Office ("The ICO"). Similar requirements exist in other countries.

In addition, with the growing prospects of data protection class actions and private litigation companies can open themselves up to civil claims and reputational damage if they illegally collect or misuse CCTV footage.

The legal situation has become more complex with advances in technology. Along with CCTV organisations employ Automatic Number Plate Technology, bodily worn cameras and even drones. The ability to stream live video using applications like Periscope and Meerkat increases the risk. Companies sometimes feel they are at a loss to understand what they can and cannot do.

The ICO Issued guidelines in October 2014 called "A Data Protection Code of Practice for Surveillance Cameras". The ICO have a track record in looking at CCTV breaches and they work alongside another regulator called the Surveillance Camera Commissioner in regulating the use of CCTV cameras.

The Law

The 8 principles of data protection appear in the DPA 1998. These apply to the collection, use, processing and deletion of CCTV footage. Before an organisation installs CCTV they should first consider whether the CCTV is necessary and what the purpose of the system is. Organisations should complete a Data Protection Impact Assessment (also known as a DPIA or PIA) to decide whether CCTV is the best solution. A company should consider whether the objective could be achieved a less intrusive way. The ICO gives a good example; if people are worried about the security of cars in the car park then perhaps a better lighting system would solve the problem rather than installing CCTV.

Letting People Know that CCTV is in Operation

If the PIA process determines CCTV is justifiable thought must be given to how to inform those who could be seen by the system. One of the principle rules is fairness. Under the DPA 1998, information has to be processed fairly. That means that the organisation should make "readily available":

1. The identity of the organisation collecting the CCTV footage
2. The purpose for its collection
3. Any other information which is necessary to make the processing fair.

So if a company is using CCTV it should put up prominent notices advising people about the system, the reason for its use and giving contact details should anyone wish to make a complaint or want to view the footage.

Keeping CCTV footage Secure

The 7th data protection principle says *"appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"*. This means that the technology used must be secure and that employees with access to CCTV footage are properly trained on data security.

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

In terms of the technology;

- If footage is being stored it should probably be **encrypted** to prevent unauthorised access
- If it is stored using a cloud service provider then **checks** should be made to ensure that the service provider uses proper security
- If **wireless** or **WiFi** transmission is used then these networks should be kept secure
- Footage should only be able to be viewed in a **restricted environment**. For example, hotel guests should not be able to see footage from the corridors and the bedroom doors from the lobby

Employees should be trained on:

- What the policies are for recording and retaining the information
- How to handle the information securely
- What to do if they receive a request from a person to see the footage
- Employees should be advised about the law; they should be advised that to misuse or access footage can be a criminal offence

Retention

The 5th data protection principle says *"personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".*

As a result you should reflect on why the information is collected and how long it is needed in order to achieve its purpose. You should have a policy (including a time limit) for when the CCTV footage is to be deleted.

This is something that can be difficult. For example if there was a police investigation and the CCTV footage was needed then obviously it should likely be kept until the conclusion of the investigation. However it would not be necessary to keep footage from a hotel lobby for several months without any compelling reason and to do so and this may well be a breach of DPA 1998.

Requests to See Footage

Where footage is taken of any person he or she is allowed access to the footage and to be given a copy of the footage subject only to some limited exceptions (s7 DPA 1998). Failure to comply with this right is one of the most common reasons for complaints to the ICO. An organisation may be able to refuse such a request if it believes that the privacy of other individuals on the footage may be compromised. It is wise to take legal advice in difficult situations such as these. Companies should satisfy themselves as to the identity of the individual requesting the footage concerned before releasing it. Companies have 40 days to comply with these requests once they have received a written valid request.

Other laws

It is worth remembering that other laws could also apply. For example the UK also has a separate regulatory system governing security operatives. The Private Security Industry Act 2001 set up a statutory regulatory scheme for the private security industry. It may be necessary for individuals viewing CCTV footage to be licensed under the Security Industry Authority Regime in addition to complying with the DPA 1998.

Conclusion

Companies do not have a right to film and to store CCTV footage on their premises as they see fit. With the increase in the privacy law rights of individuals companies should make sure that the collection, use, storage and deletion of CCTV footage is complaint with the law.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.