Has privacy and CCTV surveillance become out of focus?

07/12/2015

IP & IT:

The Guardian carried a report on 22 September 2015 summarising the efforts that Keith Spiller had made to obtain footage from CCTV cameras following a routine walk about a British city. These requests were made under the data subject access provisions in the Data Protection Act 1998 (DPA). He encountered resistance in exercising these rights. With the increasing prevalence of CCTV cameras on British streets, what are the rights and responsibilities of CCTV operators? What is the legal position and are we about to see legislative change in this field? David Bowden, freelance independent consultant, examines the implications and talks to data protection expert Viktoria Protokova of Charles Russell Speechlys LLP in London on the legal position on CCTV.

Original news

On 22 September 2015 the Guardian newspaper published a piece called "What happens when you ask to see CCTV footage". At the same time Channel 4 television has been broadcasting a series called "Hunted" on Thursday nights at 9pm where 14 volunteers attempt to be a fugitive in Britain and avoid detection by cameras or other digital fingerprints left by mobile phone or bank records.

In the Guardian report, Keith Spiller walked round a British city and then made requests to obtain CCTV footage from the operators of those cameras. These requests were made under the data subject access request provisions of the DPA. He encountered mixed results in exercising these rights. Surveillance by CCTV cameras remains a concern to privacy campaigners. Whilst the law in this field seems relatively clear, it does not appear to be applied in a consistent manner. In Brussels the negotiations continue with a view to finalising the EU Data Protection General Regulation. When this is in force, this will mean changes will have to be implemented.

Under what circumstances can an individual ask to see CCTV footage of themselves?

David Bowden (DB): This is dealt with in section 7 of the DPA. The relevant part of which provides as follows:

> "*7.**Right of access to personal data.***
>
> *(1) Subject to the following provisions of this section and to sections 8, 9 and 9A, an individual is entitled—*
>
> *(a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller,*
>
> *(b) if that is the case, to be given by the data controller a description of—*
> *(i) the personal data of which that individual is the data subject,*
> *(ii) the purposes for which they are being or are to be processed, and*
> *(iii) the recipients or classes of recipients to whom they are or may be disclosed,*
>
> *(c) to have communicated to him in an intelligible form—*
> *(i) the information constituting any personal data of which that individual is the data subject, and*
> *(ii) any information available to the data controller as to the source of those data, and*
>
> *(d) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking.*
>
> *(2) A data controller is not obliged to supply any information under subsection (1) unless he has received—*

(a) a request in writing, and
(b) except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require."

Viktoria Protokova (VP): Data captured on CCTV camera footages very often contain personal data. An individual can exercise this right to access personal data whenever (s)he wishes to do so. It is applicable for accessing footage held by either private entities or public authorities.

Can an individual request for footage of them to be destroyed?
DB: There is provision for this in section 10 of the DPA.

> ***"10 Right to prevent processing likely to cause damage or distress.***
> *(1)Subject to subsection (2), an individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject, on the ground that, for specified reasons—*
> *(a) the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another, and*
> *(b) that damage or distress is or would be unwarranted.*
> *….*
> *(3) The data controller must within twenty-one days of receiving a notice under subsection (1) ("the data subject notice") give the individual who gave it a written notice—*
> *(a) stating that he has complied or intends to comply with the data subject notice, or*
> *(b) stating his reasons for regarding the data subject notice as to any extent unjustified and the extent (if any) to which he has complied or intends to comply with it."*

VP: The effect of this provision is that an individual can request for CCTV footage to be destroyed if the processing of personal data on that footage is likely to cause "substantial distress" to him or another and that damage or distress is unwarranted.

DB: The meaning of the word "substantial" has recently been considered in another context by the House of Lords. In *Majorstake Ltd v Curtis* **[2008] UKHL 10** Baroness Hale of Richmond in the lead judgment held as follows

> "40. *'Substantial, is a word which has a wide range of meanings. Sometimes it can mean 'not little'. Sometimes it can mean 'almost complete', as in 'in substantial agreement'. Often it means 'big' or 'solid', as in a 'substantial house'. Sometimes it means 'weighty' or 'serious', as in a "substantial reason". It will take its meaning from its context. But in an expression such as a 'substantial part' there is clearly an element of comparison with the whole: it is something other than a small or insignificant or insubstantial part. There may be both a qualitative element of size, weight or importance in its own right; and a quantitative element, of size, weight or importance in relation to the whole. The works intended by this landlord are substantial in relation to each of the flats involved, but those flats do not in my view constitute a substantial part of the whole premises*."

Judge Wikely in the Upper Tribunal in *ICO v Niebel* **[2014] UKUT 255 (AAC)** criticised part of the guidance that the ICO had published (ICO guidance about the issue of monetary penalties prepared and issued under s55C(1) of the DPA) in which there was some expansion on the interpretation of "substantial distress". Although this guidance sets out the ICO's views under the 2003 Regulations there may be some read across for s10 too. The ICO says:

> "*The likelihood of damage or distress suffered by individuals will have to be considerable in importance, value, degree, amount or extent. The Commissioner will assess both the likelihood and the extent of the damage or distress objectively. In assessing the likelihood of damage or distress the Commissioner will consider whether the damage or distress is merely perceived or of real substance. The Commissioner does though consider that if damage or distress that is less than considerable in each individual case is suffered by a large number of individuals the totality of the damage or distress can nevertheless be substantial. In other words, the term substantial has a quantitative and a qualitative dimension and it is ultimately a question of fact and degree."*

At first instance Tugendhat J suggested in *Vidal-Hall v Google Inc* **[2014] EWHC 13 (QB)** that "damage" within section 13 of the DPA could be read to include "moral damage" connoting the right to compensation for breach of individual rights even where the rights are non-pecuniary. This decision is the subject of a pending appeal to the Supreme Court.

In *Halliday v Creation Financial Services*, **[2013] EWCA Civ 333** the Court of Appeal awarded £750 compensation under DPA s13 for failure of a data controller to comply with the DPA's requirements. This is likely to be a starting point if a request for destruction of CCTV image is not actioned.

What storage requirements do local authorities have to comply with?
VP: Local authorities must ensure that footage containing personal data is processed in compliance with the DPA. The DPA states that data controllers (such as local authorities) must process personal "fairly and lawfully". This means that local authorities have to have legal grounds for processing personal data and have to inform individuals their images are being processed. Further amongst other obligations, local authorities have to process data only for defined purposes. Local authorities have to implement "technical and organisational measures" against unauthorised or unlawful processing of personal data. Importantly local authorities have to ensure that an individual can access his or her data. This parallel right is also set out in the Freedom of Information Act 2000.

How does the position differ for private CCTV operators?
VP: Private individuals are exempted from complying with the DPA requirements as long as (s)he uses CCTV cameras only for the purposes of their personal, family or household affairs. However, the DPA still applies to the extent that a UK local authority may investigate if someone seems to have gone beyond the scope of the exemption, and it may take enforcement action where necessary

DB: The Court of Justice of the EU has recently had to consider what the concept of "in the course of a purely personal or household activity" means in the framework EU Data Protection Directive (95/46/EC) that underpins the DPA. In a case remitted to it from the Czech Republic (*František Ryneš v Úřad pro ochranu osobních údajů*), the CJEU gave a ruling **[2014] EUECJ C-212/13** on Article 3(2) of the Directive. It said this must be interpreted as meaning that the operation of a CCTV system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, **but which also monitors a public space**, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision.

What are the rumblings from Europe and the US?
DB: On 25 January 2012 the European Commission published (**COM (2012) 11 final)** a 119 page proposal for a Regulation ("the General Data Protection Regulation" or GDPR) on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It is intended that the GDPR will replace the 1995 Directive entirely. As it is a Regulation it will be directly enforceable in all member states and will not need to be transposed into national law by implementing legislation. This draft Regulation has now been amended extensively by both the European Parliament and the Council of Ministers.

On 15 June 2015, it was announced that EU Ministers in Luxembourg who met in its Justice Council have sealed a general approach on the GDPR but that trilogue negotiations with the Parliament and the Council would re-start in June 2015 with the shared ambition to reach a final agreement by the end of 2015.

VP: The GDPR re-affirms the importance of protection of personal data and puts additional obligations on entities that process personal data no matter what format be they hard copies, electronic copies or CCTV footages.

DB: On 6 October 2015 the Grand Chamber of the CJEU handed down its judgment in the case of *Schrems v. Data Protection Commissioner and Digital Rights Ireland Ltd* **[2015] EUECJ C-362/14.** The CJEU had to consider the validity of the "safe harbour" agreement by which companies based in the EU transferred data to or through the US for processing. In a stark but clear ruling, safe harbour was struck down with the CJEU concluding that Article 25 of the 1995 Directive:

> *"….read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State …. from*

examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection."

VP: The *Schrems* judgement declared that the Safe Harbor framework represents an invalid mechanism to transfer personal data from the EU to US. One of the reasons was the fact that US law enforcement agencies were not subject to the Safe Harbor framework themselves. Moreover, various agencies were able to access personal data of European citizens beyond what was strictly necessary and proportionate to ensure public security. The CJEU added that US legislation permits law enforcement agencies to access (on a very generalized basis) electronic communications. It said this must be regarded as compromising the essence of a fundamental right to respect for private life. More importantly, individuals did not have any administrative or judicial means of redress – Safe Harbor didn't allow individuals to access their data, erase it or rectify it. This was the point that tipped the scales leading the CJEU to declare Safe Harbor invalid.

Is the legal position around CCTV likely to change in light of the concerns around mass surveillance?

DB: Final agreement has not been reached between all 3 institutions on the GDPR. In the continuing trialogue discussions, a solution will need to be reached on transferring data to the US and to put on a satisfactory legislative footing what safe harbour sought to achieve. This may impact on the timetable. Whilst this trialogue continues this also presents a window for other changes. There remains unease about the disclosures that Snowden has made and the mood music in the UK is changing when people realise just how transparent their lives are in a digital age.

The recent rulings from the Investigatory Powers Tribunal have been unsatisfactory. The *Lucas* ruling on the *Wilson* doctrine **[2015] UKIPTrib 14_79-CH** seems to reach a startling decision on parliamentarian's correspondence that seems to be contrary to what was long thought to be the position. Similarly, what has come out in the rulings in the *Liberty v GCHQ* case **[2015] UKIPTrib 13_77-H** highlights a number of systemic weaknesses that (absent a ruling from the European Court of Human Rights) the EU legislature is likely to have to resolve sooner rather than later.

Interviewed by David Bowden of David Bowden Law (www.DavidBowdenLaw.com).

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.