UK Court Ruling: CCTV Audio Recording Features Breach UK Data Protection Rules

Date : October 20, 2021

Introduction

CCTV/video camera surveillance and data protection is a perennial topic, which we've written about in detail here https://www.corderycompliance.com/client-alert-using-cctv-on-business-premises-dp-implications/. This area can carry considerable compliance risk, as shown by the €10.4m penalty imposed in Germany notebooksbilliger.de AG for video surveillance used to monitor employees, which we've written about here https://www.corderycompliance.com/german-cctv-fine/.

The recent court ruling in the case of Fairhurst v Woodward has highlighted CCTV/video camera surveillance and data protection issues, including the new one of when audio-recording is also used. It features the court's analysis of the status of the Ring doorbell system owned by Amazon. This article sets out highlights of the ruling.

What's this all about?

The parties in the case, Mrs. Fairhurst and Mr. Woodward, were neighbours who were in dispute over a number of issues, notably Mr. Woodward's use of security cameras at and around his property, including a Ring combined doorbell and video and audio surveillance system.

Mrs. Fairhurst considered the use of surveillance an invasion of her privacy which she said had caused her such distress that she had left her home and not returned to reside there again. She brought legal proceedings and claimed, amongst other things, breaches of the UK Data Protection Act 2018 (DPA 2018), damages and an injunction against Mr. Woodward mandating the removal of some of the systems and forbidding the installation of further surveillance cameras.

What was the court's ruling?

The court ruled as follows:

- The first data protection principle had been breached because Mr. Woodward hadn't processed data fairly or in a transparent manner, and, the second data protection principle had been breached because Mr. Woodward had not collected data for a specified or explicit purpose (he had instead misled Mrs. Fairhurst about the focus of a particular camera and another particular camera was collecting Fairhurst's personal data although Mr. Woodward had claimed that it wasn't);
- The fact that Mr. Woodward collected data outside the boundaries of his property meant that it was for him to satisfy the (GDPR) lawful processing grounds of "legitimate interests" test which the court ruled that he had satisfied "because any video personal data [about Mrs. Fairhurst] is likely to be collected only incidentally as she walks past, unless [Mrs. Fairhurst] stands on [Mr. Woodward's] door and rings his doorbell, and I consider that his legitimate interest in protecting his home whether he is there or not are not overridden by her right to avoid such incidental collection on a public street, albeit in the vicinity of her home";
- But, the judge ruled that, as regards another camera "which was trained on [Mrs. Fairhurst's] property including her side gate, garden and her car parking spaces, I do not consider that [Mr. Woodward] has satisfied me that this is necessary for the purposes of his "legitimate interests". [That camera] only collects data from outside [Mr. Woodward's] property";
- In relation to the audio personal data collected by two cameras and the doorbell, the judge considered the third data protection principle under which personal data "shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" and concluded that: "[…] the extent of range to which these devices can capture audio is well beyond the range of video that they capture, and in my view cannot be said to be reasonable for the purpose for which the devices are used by [Mr.

Woodward], since the legitimate aim for which they are said to be used, namely crime prevention, could surely be achieved by something less. A great deal of the purpose could be achieved without audio at all, as is the case with the bulk of CCTV systems in use in public places in this country, or by a microphone that only picks up sound within a small diameter of the device". "[…] The extent of the range means that personal data may be captured from people who are not even aware that the device is there, or that it records and processes audio personal data, or that it can do so from such a distance away, [is] in breach of the first [data protection] principle. "[…] The living individuals whose conversation it captures may well be identifiable from the data itself or from other information which can be obtained from the data controller particularly in a case such as this where [Mr. Woodward] knows and is familiar with his neighbours and can probably identify many of them by voice alone, and certainly identify them with both the audio and video data that these devices capture";

- In conclusion, the judge ruled that Mr. Woodward had breached the UK Data Protection Act 2018 and the UK GDPR and that Mrs. Fairhurst was entitled to compensation and orders preventing Mr. Woodward from continuing to breach Mrs. Fairhurt's rights in the same or a similar manner in the future.

The claim for damages and the orders will be dealt with separately by the court.

What are the takeaways?

Although this was a claim concerning domestic premises the issues in question could equally apply to a business and so the takeaways are that businesses should consider addressing the most privacy-compliant way to set up their CCTV/video surveillance cameras, including addressing the following:

- What areas the cameras should capture;
- How to position cameras to avoid intruding on the property of others or any shared or public spaces;
- Whether to record the images or just have a live feed;
- If the system has an audio-recording facility consider whether that use is justifiable in a given set of circumstances and if not consider disabling it;
- Carry out a Data Protection Impact Assessment – this is the best way to address CCTV/video surveillance camera privacy risks; and,
- If there's a UK dimension, address registration, i.e. under the ICO's register of fee payers and pay the data protection fee. There's more information on this system here https://www.corderycompliance.com/solutions/privacy-registration-and-renewal/.

Resources

Cordery's GDPR Navigator subscription service is an expansive set of resources and a community of peers helping companies deal with GDPR and related issues. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

Some of our articles about CCTV/video camera surveillance can be found here https://www.corderycompliance.com/cj-interprets-dp-ligitimate-interests-re-cctv-video-surveillance/ and here https://www.corderycompliance.com/client-alert-another-european-court-cctv-damages-judgment-2/ and here https://www.corderycompliance.com/client-alert-european-court-cctv-damages-judgment/ and here https://www.corderycompliance.com/client-alert-court-awards-damages-for-distress-caused-by-breaches-of-data-protection-rules/.

The court's judgment can be found here https://www.judiciary.uk/judgments/fairhurst-v-woodard/.

We report about data protection issues here https://www.corderycompliance.com/category/data-protection-privacy/.

We report about compliance issues here https://www.corderycompliance.com/news/.

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

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com