Articles + Publications | April 1, 2024

U.K. Information Commissioner Issues New Guidance on the Use of Biometrics in the ?Workplace

Privacy & Cybersecurity Newsletter

WRITTEN BY

Nick Elwell-Sutton

RELATED OFFICES

London

On February 23, 2024, the Office of the Information Commissioner ("ICO"), the U.K.'s data privacy regulator, issued new guidance[1] for employers about the use of biometrics in the workplace. Along with this new guidance, the ICO gave notification of formal enforcement action taken against Serco, a major U.K. employer, for unlawfully using fingerprint scanning to monitor workplace attendance. As part of its accompanying press release, and as an obvious shot across the bow to employers, the ICO stated:

"This action serves to put industry on notice that biometric technologies cannot be deployed lightly. We will intervene and demand accountability, and evidence that they are proportional to the problem organisations are seeking to solve."

The new guidance is comprehensive and serves notice that the bar has been heightened for employers wanting to utilize biometric technology. It sets out a concise summary of the law and supplements this with not only good practice that the ICO expects to see implemented, but also some best practice tips.

As a starting point, the new guidance reinforces that biometrics covers not just the well-known digital picture, fingerprint, and iris recognition technologies – but can extend to a recording of someone talking or a video of them walking where a biometric feature (e.g., voice pattern or gait) is then extracted and utilized. It also acts as a reminder that fingerprint and face recognition access, common on business-issued phones and mobile devices, is also captured by the guidance.

The minimum core legal requirements are re-stated as follows:

- a data protection by design approach must be adopted when putting in place biometric recognition or verification systems;
- a Data Processing Impact Assessment ("DPIA") must be completed before using a biometric system;
- an assessment must be undertaken of the impact the use of a biometric system will have on the people whose information it will process;
- there must be transparency concerning who the data controller is; and
- there must be a written contract in place with all processors (i.e., third parties such as AWS hosting).

Employers assessing the impact of implementing a biometric system must consider the possible effects of any data breach given the highly sensitive nature of biometric data and the potentially significant consequences of that falling into the wrong hands and with a particular emphasis on the risks of reverse engineering.

In addition, and in a rapidly developing area, the ICO highlights the risks of discrimination through the use of biometrics. This latter point is the subject of ongoing litigation between Uber Eats[2] and delivery operatives who allege that black and ethnic minority drivers are subjected to indirect/de facto race discrimination because Uber's facial recognition technology, which is used to verify the identity of the operative, is more likely to produce a false negative (i.e., not properly recognizing a non-white operative's identity as being valid) – which places minorities at greater risk of losing their job as a consequence of failing the verification process. The substantive judgment on this issue is due later this year and will be watched closely.

The ICO's guidance also stresses the need to ensure there is a lawful basis for processing, that biometric data is fairly and transparently processed and that the additional safeguards required for special category/high risk processing are in place.

Many employers rely upon consent as a lawful basis for using biometrics, but the guidance notes any such consent must be *"specific and informed"* and *"freely given"* in order to be valid. The guidance also makes clear that even when consent is relied upon, data subject employees must still be afforded the opportunity to refuse or easily withdraw their consent at any time without detriment, that they must be offered an alternative method of verification, and that any consent must be explicit and cannot be inferred through conduct given the power imbalance.

In some respects this oversimplifies matters and arguably places too high a burden on employers. For example, an employer experiencing a substantial problem with timecard fraud in which bad actor employees clock in and out of work for one another might try to deter this conduct by implementing a biometric fingerprint scanning system in order to accurately identify which employees are clocking in and out. In this scenario, the employer might argue there is no practical alternative to combat this particular type of fraud as non-biometric options, such as unique employee pin numbers or access cards, could still be shared among the bad actors and being mandated to offer a less secure option in this circumstance would not solve the underlying problem and could leave the employer susceptible to fraud.

The employer in this scenario might look to use legitimate interests as a lawful basis for the use of biometrics and so not require or rely upon consent. However, the ICO could still ultimately find the use to be disproportionate, despite the employer having a good reason for implementing the fingerprint scanning. The ICO's view may be that the incidence of fraud was not enough to warrant the intrusive nature of the fingerprint scanning requirement and that the employer could achieve its goals using less intrusive means, such as by having employees report to a supervisor upon arrival at work for visual verification. Quite how practical this would be in a larger factory or warehouse is another matter.

Where there is a less intrusive way of achieving the same purpose, it will always be difficult to succeed on the proportionality requirement and the Serco[3] enforcement action demonstrates that, in the ICO's view, *"employers*

should not prioritise business interests over employees' privacy." Only if there is not another method that would achieve the underlying aim is the proportionality argument likely to succeed, regardless, it seems, of practicality and where reasonable views can legitimately differ.

But what is clear is that employers wishing to use biometrics will need a fully worked-up data privacy program in advance to support this, be able to demonstrate how it complies, to have properly considered less intrusive alternatives and be prepared to explain cogently why those would not achieve the same underlying purpose. Only then will the proportionality aspect tip the balance in employers' favor.

While relatively few employee data privacy claims are actually litigated, the courts have so far tended to adopt a more commonsense approach in other data privacy matters and while regard is had to guidance issued by the ICO, it is ultimately for the courts to determine the legality.

The guidance rounds off by covering some detailed security measures including some of the latest Privacy Enhancement Technologies[4] and some useful related biometric security guidance issued by the National Cyber Security Centre.[5] Employers operating in the U.K. should review their policies and procedures for compliance with these measures.

—

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/

[2] https://assets.publishing.service.gov.uk/media/62dab66b8fa8f5649dbef494/Mr_P_E_Manjang_-v-_Uber_Eats_UK_Ltd___Others_-_3206212_2021_-_Preliminary_Judgment.pdf

[3] https://ico.org.uk/media2/woalogoc/20240219-serco-leisure-operating-limited-en.pdf

[4] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/what-pets-are-there/reference-table/

[5] https://www.ncsc.gov.uk/collection/biometrics

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber