AN A.S. PRATT PUBLICATION
JUNE 2024
VOL. 10 NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 5** **June 2024**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

UK's Data Protection Regulator Continues to Clamp Down on the Use of Biometric Recognition Technology

By Rob Dalling and Tracey Lattimer*

In this article, the authors discuss recent actions taken by the UK's data protection regulator, the Information Commissioner's Office, with respect to biometric technology.

The UK's data protection regulator, the Information Commissioner's Office (ICO), has issued Enforcement Notices (the Notices)[1] to Serco Leisure Operating Limited, Serco Jersey Limited (together, Serco) and seven associated community leisure trusts. The Notices ordered Serco and the trusts to stop using facial recognition technology and fingerprint scanning to monitor employee attendance.

On the same day, the ICO published new guidance on the use of Biometric Recognition Systems.[2] As the use of biometric technology increases, organizations should be mindful not to fall foul of UK and European data protection legislation.

THE SERCO ENFORCEMENT NOTICES

Serco operates leisure facilities on behalf of community leisure trusts and local authorities across the UK and Jersey. Since May 2017, Serco has been using facial recognition technology and fingerprint scanning technology for the purpose of employment attendance checks and subsequent payment for employees' timed work. From its introduction, Serco has processed the biometric data of more than 2,000 employees at 38 leisure facilities across the UK and Jersey. Serco began using biometric technology as it considered that previous systems (which included manual sign-in sheets and radio-frequency ID cards (RFID cards))[3] were prone to human error and abuse by employees (via buddy punching and falsified timecards).

Contraventions

The ICO commenced its investigation into Serco and the trusts at the end of December 2019, after an employee of the ICO observed facial recognition technology being used

* The authors, attorneys with Jenner & Block London LLP, may be contacted at rdalling@jenner.com and tlattimer@jenner.com, respectively.

[1] https://ico.org.uk/action-weve-taken/enforcement/serco-leisure-operating-limited-and-relevant-associated-trusts/.

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

[3] Physical access cards that use radio frequency to grant access to a particular area or individual.

at a facility managed by Serco. On 23 February 2024, the ICO found Serco and the trusts to be in breach of Articles 5(1)(a), 6 and 9 of the UK GDPR, as they had failed to establish a lawful basis and special category personal data[4] processing condition for the processing of biometric data.

Article 5(1)(a) of the UK GDPR enshrines the principle that personal data shall be processed lawfully, fairly, and in a transparent manner. Article 6 sets out six 'lawful bases' on which organizations can rely to process personal data lawfully. Where special category data is concerned, Article 9 provides for ten possible conditions on which organizations must further rely to lawfully process such data.

Lawful Basis for Processing – Article 6

As to the lawful bases for processing biometric data, Serco and the trusts purported to rely on contractual necessity and legitimate interests (Articles 6(1)(b) and 6(1)(f) of the UK GDPR). Whilst the ICO agreed that recording employee attendance times was necessary for Serco to fulfil its contractual obligation to pay employees, it did not consider that the processing of biometric data was necessary to achieve this purpose. Less intrusive means could be used to verify attendance such as RFID cards/fobs or manual timesheets, which Serco had failed to demonstrate were not appropriate.

Despite Serco's assertions that such alternative methods were open to abuse, the ICO noted that Serco had been unable to provide evidence of widespread abuse, nor explain why other methods, such as disciplinary action against employees found to be abusing the system, were not appropriate. The ICO was similarly not persuaded by Serco's legitimate interest arguments, concluding that the processing of biometric data was not necessary to fulfil Serco's legitimate interest of ensuring it paid its employees the correct salary for the time they worked.

In particular, the ICO noted that legitimate interests will not apply if the same result can be reasonably achieved in another less intrusive way.

Special Category Personal Data Processing Condition – Article 9

Serco and the trusts had further sought to rely on Article 9(2)(b) as their processing condition for special category data, i.e., that the processing was necessary to carry out employment law obligations/exercise employment law rights.

The ICO noted that Serco and the trusts had initially failed (both when they began processing data using biometric technology and during the ICO's investigation) to identify the specific legal obligations/rights relied upon, only later relying on the Working Time Regulations 1998 and the Employment Rights Act 1996.

The ICO commented that the Article 9(2)(b) condition does not cover processing to meet purely contractual employment rights or obligations and further noted that Serco

[4] Under Article 9(1) of the UK GDPR, biometric data is classified as "special category personal data" requiring additional safeguards for it to be lawfully processed.

and the trusts had failed to demonstrate the necessity of processing biometric data for the purpose of employee attendance checks or to comply with the laws identified.

Serco was further criticized for not having in place an appropriate policy document as required by the UK Data Protection Act 2018.[5]

Lawful, Fair, and Transparent Processing – Article 5

Considering the above, the ICO concluded that Serco and the trusts had unlawfully processed biometric data in contravention of Article 5(1)(a) of the UK GDPR. Further, Serco and the trusts had failed to process personal data fairly. The ICO commented that the processing of biometric data is highly intrusive and has the potential to cause distress to data subjects.

Alternative mechanisms for logging attendance had not been sufficiently brought to Serco employees' attention; rather, employees were "expected" to use biometric technology and could be subject to disciplinary action if they refused. The ICO further concluded that, due to the imbalance of power between Serco and its employees, it was unlikely that employees would feel able to object to such processing in any event.

Terms of the Notices

As a result of the Notices, within three months, Serco and the trusts were required to cease processing biometric data for the purpose of employment attendance checks and were further required to destroy all biometric data that they are not legally obliged to retain.

Commenting on the Notices, John Edwards, the UK Information Commissioner, 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 organizations are seeking to solve."[6]

THE ICO'S NEW GUIDANCE ON THE USE OF BIOMETRIC RECOGNITION SYSTEMS

The Notices were issued on the same day that the ICO published new guidance on the use of biometric recognition systems. The ICO's guidance explains how data protection law applies to the use of such systems and covers, amongst other things:

- How to process biometric data lawfully and fairly.
- How the accuracy principle applies to biometric data.

---

[5] Schedule 1, Part 1, paragraph 1(1)(b), which relates to the processing of special category personal data in an employment context.

[6] ICO orders Serco Leisure to stop using facial recognition technology to monitor attendance of leisure centre employees, at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-orders-serco-leisure-to-stop-using-facial-recognition-technology/.

- How to ensure the processing of biometric data is transparent.
- How to deal with data subject rights requests for biometric data.
- How to keep biometric data secure.

As to how organizations can process biometric data lawfully, the guidance notes that explicit consent is likely to be the most appropriate condition available. The ICO does appreciate, however, that consent can be difficult to obtain in an employer-employee context as employees may feel they have no choice but to agree.[7] The ICO comments that this does not mean that employers can never rely on consent, but that they need to carefully consider the specific scenario in order to ensure they can offer a genuine choice without detriment. In order to rely on any lawful basis other than consent, organizations must be able to demonstrate that processing biometric data is "necessary" to achieve their overall purposes. Whilst necessity does not mean that the processing of the data much be absolutely essential, it does need to be more than just useful or desirable.

In connection with the fairness principle, the guidance states that whether biometric recognition systems are effective depends on their statistical accuracy. If organizations do not address the risk of inaccuracy, they may contravene the fairness principle and other equalities legislation. The guidance notes, for example, that biometric recognition systems should be tested for bias and, if detected, such bias should be mitigated.

As with all personal data, the guidance provides that organizations must implement appropriate security measures when using biometric data. Given the sensitive nature of biometric data, and the risks associated with unauthorized access by nefarious actors, "appropriate" is a higher bar than for personal data more generally. The guidance states that organizations must encrypt any biometric data they use and should consider the use of privacy enhancing technologies (PETs).

Commenting on the guidance, John Edwards said, "Our latest guidance is clear that organizations must mitigate any potential risks that come with using biometric data, such as errors identifying people accurately and bias if a system detects some physical characteristics better than others."[8]

LESSONS

With the use of biometric technology becoming increasingly common, organizations must ensure they do not fall foul of UK and European data protection legislation. Some of the key lessons that organizations can take from the Serco Notices and the ICO's new guidance include:

---

[7] In order to be valid, the UK GDPR requires that consent be "freely given" (Article 4(11)).

[8] ICO orders Serco Leisure to stop using facial recognition technology to monitor attendance of leisure centre employees, at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-orders-serco-leisure-to-stop-using-facial-recognition-technology/.

- When not relying on consent as the lawful basis for processing biometric data, it is crucial to consider whether the processing is "necessary." Organizations must ensure that they have considered whether other less intrusive means could be used and must clearly document and evidence why such alternative means are not appropriate.

- When relying on consent or legitimate interests as the lawful basis for processing biometric data, organizations must offer alternative options to those that decline to provide consent/object to the processing of such data.

- When relying on Article 9(2)(b) as the special category condition to process biometric data for employment purposes, prior to processing such data, organizations must clearly identify the laws that contain the right/obligation requiring such processing.

- Connected with the above, robust data protection impact assessments[9] must be completed prior to the processing of biometric data via biometric recognition systems.

- Where biometric data is being processed in an employment context, such as for employee monitoring, organizations must ensure they have appropriate policy documents in place.

- Organizations that are processing biometric data must have more robust security measures in place.

[9] An assessment of the impact that the proposed processing operation will have on the protection of personal data.