MAYER | BROWN

September 2019

Legal Update

The UK High Court finds police use of automated facial-recognition technology permissible

R (Bridges) v CCSWP and SSHD [2019] EWHC 2341

On 4 September 2019, the High Court in England and Wales rejected a judicial review claim brought by Edward Bridges, a civil liberties campaigner (the **"Claimant"**) regarding the use of automated facial-recognition technology (**"AFR"**) by the Chief Constable of South Wales Police's (**"SWP"**). The High Court dismissed claims that the use of AFR by SWP breached UK data protection laws and was contrary to the European Convention on Human Rights. The High Court determined that the use of AFR constituted the processing of biometric data but that the SWP had established lawful grounds and had met the other legal requirements to process it.

The decision sheds light on the types of processing activities that will constitute the processing of biometric data as well as the legal bases and other requirements that must be satisfied by businesses and other types of organisations in order to use AFR under the UK Data Protection Act 2018 and the European General Data Protection Regulation (**"GDPR"**).

Background

The SWP has been using AFR Locate in public spaces since 2017 for crime-prevention purposes. When AFR Locate is deployed, images of the faces of members of the public moving within public spaces are taken from live CCTV feeds and are processed in real time to extract unique facial features to create templates for those individuals. Each template is then compared against templates of individuals on a police watch list. The watch list templates were created from images held on databases maintained by SWP as part of ordinary policing activities.

The claim

The Claimant's claim related to SWP's use of AFR Locate in general and with respect to two particular instances where SWP used AFR Locate where the Claimant was present and his image was captured. The Claimant claimed that such use was contrary to Article 8 of the European Convention on Human Rights, the previous UK Data Protection Act 1998, the current UK Data Protection Act 2018 and the UK Equality Act 2010.

Was the use of AFR Locate contrary to the requirements of UK data protection legislation?

The Claimant brought claims under both the previous Data Protection Act 1998 and the current Data Protection Act 2018 (**"DPA 2018"**), which supplements the GDPR. None of the deployments by SWP of AFR Locate took place after the commencement of DPA 2018 but both parties requested the court consider the legality of the deployments of AFR Locate as if they had taken place after the commencement of DPA 2018.

DPA 2018

Under the DPA 2018, which supplements the GDPR in the UK by setting out the equivalent conditions and requirements under which personal data can be processed by public bodies for law enforcement purposes, the Claimant made two claims:

1. The first claim was that SWP had breached the first data protection principle under S.35 DPA 2018, which requires that the processing of personal data for any of the law enforcement purposes to be lawful and fair.

   In deciding whether the first data protection principle had been complied with, the court considered the extent to which the processing by AFR Locate constituted "sensitive processing" under the law enforcement chapter of the DPA 2018 ("sensitive processing" is equivalent to the processing of special category personal data under the GDPR, which includes the processing of biometric data).

   The first question for the court was, as a result of the manner in which AFR Locate collected facial images as well as generated and checked templates, whether the use of AFR Locate involved the collection and processing the biometric data of general members of the public in addition to biometric data relating to those individuals on the watch list.

   SWP submitted that any processing of facial images by AFR Locate of members of the public was not "sensitive processing" because the purpose of AFR Locate was not to identify non matching members of the public recorded by CCTV but only to identify those that were on the watch list (i.e. only those individuals that matched a watch list template).

   The court held that the collection and use of facial images relating to members of the public by AFR Locate did constitute "biometric data" and so was "sensitive processing". The court decided that, although SWP's overall purpose was to identify the persons on the watch list, in order to achieve the overall purpose, each member of the public needed to be uniquely identified by processing their biometric information. The court noted that the fact that facial biometric information is retained for only a very short period (except where a match is detected), does not affect this analysis.

   The second question for the court was whether a legal ground could be relied upon under the DPA 2018 to process the biometric data; namely whether (a) the processing was "strictly necessary" for the law enforcement purpose; (b) whether one of the prescribed conditions that has to be satisfied for this purpose was met under Schedule 8 DPA 2018; and (c) whether there was an "appropriate policy document" that met the requirements of S.42 DPA 2018.

The court held:

a) The processing was strictly necessary for the law enforcement purpose. The court found that:

   i. The deployment of AFR Locate was to ensure the safety of the public and detect crime. The event had previously attracted disorder and some of those involved in previous protests (who were on the watch list) had caused criminal damage and made bomb hoax calls. The apprehension of suspects wanted on warrant or on suspicion of having committed an offence in the South Wales area could not have been achieved using CCTV alone. The use of watch lists was clearly targeted, being directed only to those people who need to be located for good reason and the evidence demonstrated that, during the trial period, the new technology had resulted in arrests or disposals where the individual in question had not been capable of location by previous methods.

   ii. the two specific uses of AFR Locate that resulted in images being taken of the Claimant struck a fair balance and was not disproportionate in that AFR Locate was deployed in an open and transparent way, with significant public engagement and on each occasion, it was used for a limited time and covered a limited footprint. Any interference would be limited to the near instantaneous algorithmic processing and discarding of the Claimant's biometric data. No personal data relating to the Claimant would have been available to any police officer, or

to any human agent. No data would be retained. There was no attempt to identify the Claimant and he was not spoken to by any police officer.

b) A condition under Schedule 8 was met, namely that the processing was necessary for the exercise of a function conferred on a person by an enactment or rule of law, and was necessary for reasons of substantial public interest. The relevant rule of law was SWP's common law duty to prevent and detect crime and the necessity test was satisfied as explained above; and

c) The court was unable to decide whether SWP's document titled "Policy on Sensitive Processing for Law Enforcement Purposes", was an "appropriate policy document". The court stated that although the document provided some explanation of SWP's policies for securing compliance, it was brief and lacking in detail, and that there was no systematic identification of the relevant policies and no systematic statement of what those policies provided. In particular, the document did not appear to address the position of members of the public. Nonetheless, the court was reluctant to make a decision as to whether the document constituted an "appropriate policy document". Given the role of the UK Information Commissioner and the prospect of future guidance, the court did not think it was necessary for it to rule either way and said that the development and specific content of that document was, for the time being, better left for reconsideration by SWP in the light of further guidance from the UK Information Commissioner's Office.

2. The second claim was that SWP had failed to carry out a data protection impact assessment, as required under S.64 DPA 2018.

   The court held that the impact assessment prepared by SWP met the requirements of S.64, noting the following points:

   a) The court felt there was a clear narrative that explained the proposed processing, which referred to the concerns raised in respect of intrusions into privacy of members of the public when AFR Locate was used; and

   b) That whilst the treatment of the personal data of those on watch lists was a particular focus of the document, the document did recognise that personal data of members of the public would be processed and identified the safeguards in place in terms of the duration for which any such data would be retained, the purpose for which it would be used and considered other requirements that had to be met.

Was the use of AFR Locate contrary to The European Convention on Human Rights?

The Claimant also argued that the use of AFR Locate interfered with the Claimant's rights under Article 8(1) of the European Convention on Human Rights (right to private life) and that, for the purposes of Article 8(2) the interference was neither "in accordance with the law" nor "necessary" or "proportionate".

The court held:

1. The use of AFR Locate did infringe the Article 8(1) rights of those in the position of the Claimant; but

2. The use of AFR Locate was necessary and proportionate as explained above and so met the requirements of the Human Rights Act given that the actions of SWP were subject to sufficient legal controls.

Conclusion

It is clear from the High Court's decision that the use of AFR constitutes the processing of biometric data under the GDPR and DPA 2018, not just in relation to those individuals on a watch list, but importantly, in the case of any other members of the public who can be identified from the relevant camera or sensor using AFR technology. In a statement, the UK Information Commissioner's Office welcomed the court's decision that the use of AFR involves the processing of biometric data of members of the public and said that it will now consider the court's findings before finalising their recommendations and guidance to police forces in their use of the technology.

In this case, while the court found that the SWP was processing biometric data, it determined that the SWP had complied with its data protection obligations when processing it for law enforcement purposes.

However, it is unlikely that businesses operating in the private sector will be able to reply on the same legal grounds as the SWP for the range of purposes for which they may seek to deploy AFR and similar technologies. As a result of biometric data becoming categorised as special category personal data under the GDPR from 25 May 2018, organisations currently using or seeking to use AFR and similar technologies must demonstrate that they comply with additional, more restrictive legal requirements in order to use it. Organisations currently using or seeking to use AFR or similar technologies should consider whether they can comply with these additional, more restrictive requirements with respect to the entire population that may be identified by the relevant cameras or other sensors utilising these technologies. The decision also provides useful guidance on the factors a court will take into account when determining whether an appropriate data protection impact assessment has been conducted in the context of AFR, which should be considered by organisations looking to use these types of technologies.

If you have any questions about the issues raised in this legal update, please get in touch with your usual Mayer Brown contact or:

Mark Prinsley

Partner, London
E: mprinsley@mayerbrown.com
T: +44 20 3130 3900

Oliver Yaros

Partner, London
E: oyaros@mayerbrown.com
T: +44 20 3130 3698

Charles Albert Helleputte

Partner, Brussels
E: chelleputte@mayerbrown.com
T: +32 2 551 5982

Regine Goury

Partner, Paris
E: rgoury@mayerbrown.com
T: +33 1 53 53 43 40

Ulrich Worm

Partner, Frankfurt
E: uworm@mayerbrown.com
T: +49 69 7941 2981

Guido Zeppenfeld

Partner, Frankfurt
E: gzeppenfeld@mayerbrown.com
T: +49 69 7941 1701

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our "one-firm" culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

Please visit mayerbrown.com for comprehensive contact information for all Mayer Brown offices.

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the "Mayer Brown Practices") and non-legal service providers, which provide consultancy services (the "Mayer Brown Consultancies"). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown.

© 2019 Mayer Brown. All rights reserved.

Attorney Advertising. Prior results do not guarantee a similar outcome.