



<p>I write to request information and records under the FOIA, regarding Merseyside Police’s use of live, automated facial recognition technology and collaboration with external companies.</p>	
REQUEST	RESPONSE
<p>1. Has your force collaborated or cooperated with any external companies (National Museums Liverpool) in their use of live facial recognition? If yes, please provide details including the name of the companies, manner of collaboration (e.g advice, sharing images), the time period of the collaboration, locations, any costs involved, and which uses have ceased or are continuing.</p> <p style="padding-left: 20px;">a. If yes, did your force share images as part of the collaboration? Please provide the number of images, the source or datasets from where the images came from, a full list of purposes for which the images were shared, the legal basis on which the images were shared, and data security/management protocols around the handling of the shared data.</p> <p style="padding-left: 20px;">b. If yes, what was the rank of the officer who authorised the collaboration? What process was followed before the collaboration was authorised?</p>	<p>Merseyside Police has not collaborated with any external companies (including National Museums Liverpool) in their use of live facial recognition.</p>

<ul style="list-style-type: none"> c. If yes, what was the protocol arranged for the event of a match alert? d. If yes, how many times were you alerted to a match alert? How many of those led to further police action being taken? e. If yes, how many true positive matches were there during the collaboration? f. If yes, how many false positive matches were there during the collaboration? 	
<p>2. Does your force have any policy guidance relating to collaboration with external companies using live facial recognition and/or the retention of images resulting from the use of live facial recognition?</p> <ul style="list-style-type: none"> a. If yes, when were the policies created? (Please provide a copy of said policies) b. How many images captured in the course of using live facial recognition technology have been retained for storage? 	<p>No.</p>
<p>3. Has your force completed a privacy or data protection impact assessment in relation to collaboration with external companies using live facial recognition technology? If so, please provide a copy.</p>	<p>No.</p>

<p>4. Has your force completed a privacy or data protection impact assessment in relation to any use of live facial recognition? If so, please provide a copy.</p>	<p>No.</p>
<p>5. Has your force scrutinised a privacy impact assessment conducted by any external companies operating live facial recognition with whom you have collaborated? If so, please describe when and provide a copy.</p>	<p>No.</p>
<p>6. Is your force currently using or collaborating with external companies on the use of live facial recognition?</p>	<p>No.</p>
<p>7. Does your force have any plans to use or trial live facial recognition or plans to collaborate with any external companies in the future?</p>	<p>No.</p>
<p>8. Your force has been publicly identified as collaborating with National Museums Liverpool in using live facial recognition in 2018. We sent an FOI to your force in October 2018 asking whether your force had used or planned to use live facial recognition, including whether your force had collaborated with external companies, and you responded on 3 November 2018 (FOI Application DM2018/1152) stating that “No information held. Merseyside Police does not use facial recognition.” Please can you explain why you gave this response.” (Question as amended on 12th September 2019)</p>	<p>This question seeks an opinion rather than information held, and so does not constitute a valid request under the terms of the Freedom of Information Act. However, as assistance, the query is addressed as follows:</p> <p>The response was provided because it was believed, and is still believed, to be correct.</p> <p>A media statement from National Museums Liverpool originally stated that facial recognition technology was used at the World Museum “following advice from Merseyside</p>

	<p>Police and local counter terrorism advisors”.</p> <p>Although National Museums did indeed seek advice from Merseyside Police, the Force did not give any advice to install facial recognition technology.</p> <p>When National Museums Liverpool were reminded of this, their media statement was subsequently amended to the effect that facial recognition technology “was put in place after seeking advice from Merseyside Police and local counter terrorism advisors”.</p> <p>Careful reading of the amended statement will demonstrate that it does not actually state that Merseyside Police in any way collaborated with National Museums Liverpool in using live facial recognition.</p> <p>For the avoidance of doubt, Merseyside Police made no recommendations to National Museums / World Museum in relation to the use of Facial Recognition Technology and no photographs or database was provided to the museum by Merseyside Police to be used in conjunction with any facial recognition system.</p>
<p>By virtue of Sections 24(2) and 31(3) of the Freedom of Information Act, Merseyside Police can neither confirm whether any additional information is held in relation to this request, such as whether such technology is used covertly by Merseyside Police.</p> <p>Section 24 states that information which could affect national security is exempt from disclosure.</p> <p>Section 31 states that information which could affect law enforcement functions is exempt from disclosure.</p> <p>Please see the Harm and Public Interest Tests on the following pages of this response for details as to how these exemptions apply in this case.</p>	

Police forces in the United Kingdom are routinely required to provide statistics to requestors of information. The systems used for recording these figures are not generic, nor are the procedures used locally in capturing the data. It should be noted that for these reasons this Force’s response to your questions should not be used for comparison purposes with any other response you may receive.

HARM IN CONFIRMING OR DENYING THAT ANY ADDITIONAL INFORMATION IS HELD

Any disclosure under FOI is a release to the public at large. Whilst not questioning the motives of the applicant, confirming or denying that any other information relating to the covert practise of facial recognition would show criminals what the capacity, tactical abilities and capabilities of the force are, allowing them to target specific areas of the UK to conduct their criminal/terrorist activities. Confirming or denying the specific circumstances in which the Police Service may or may not deploy the use of technology such as facial recognition would lead to an increase of harm to covert investigations and compromise law enforcement. This would be to the detriment of providing an efficient policing service and a failure in providing a duty of care to all members of the public.

The threat from terrorism cannot be ignored. It is generally recognised that the international security landscape is increasingly complex and unpredictable. Since 2006, the UK Government has published the threat level, based upon current intelligence and that threat has remained at the second highest level 'severe', except for two short periods during August 2006, June and July 2007, and more recently in May and June 2017, following the Manchester and London terrorist attacks, when it was raised to the highest threat, 'critical'. The UK continues to face a sustained threat from violent extremists and terrorists and the current threat level is set at 'severe'.

It is well established that police forces use covert tactics and surveillance to gain intelligence in order to counteract criminal behaviour. It has been previously documented in the media that many terrorist incidents have been thwarted due to intelligence gained by these means.

PUBLIC INTEREST TEST		
Exemption	Factors favour complying with Section 1(1)(a) confirming that information is held	Factors against complying with Section 1(1)(a) confirming or denying that information is held
Section 24(2) National Security	If the public are kept informed of policing techniques then they will be better able to take steps to protect themselves, aiding national security. Police accountability would demonstrate how public funds are being spent.	Confirming or denying whether any information is held relating to the covert use of facial recognition technology would limit operational capabilities as criminals/terrorist would gain a greater understanding of the police’s methods and techniques, enabling offenders to take steps to counter them. It may also suggest the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing potential vulnerabilities. This detrimental effect is increased if the request is made to several different law enforcement bodies.
Section 31(3) Law Enforcement	Confirming that information exists relevant to this request would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce these attacks.	In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to ‘map’ where the use of certain tactics are or are not deployed. This can be useful information to those committing crimes. It would have the likelihood of identifying location-specific operations which would ultimately compromise police tactics, operations and future prosecutions as criminals could counteract the measures used against them.
Balance Test	When balancing the public interest it is necessary to consider the release of the requested information into the public domain. The public interest is not what interests the public, but what would be of tangible benefit to the public as a whole. Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both National Security and Law Enforcement. The decision of Merseyside Police is therefore to neither confirm nor deny that any further information is held.	