Heddlu Police
DYFED-POWYS

FOI Reference: 1022/2019

Request:

1. When did your police force introduce facial recognition technology? Please provide a month and year.
2. How does your police force use facial recognition technology? Please confirm if it is used for any of the following use cases and provide information of any additional use cases: event management, riot policing, to monitor train stations, in airports, to monitor public spaces (please confirm the type of public spaces it is installed in – i.e. shopping mall), body-worn cameras, etc.
3. How much money was invested in facial recognition technology over the previous five years. Please share the figure broken down by each year for 2015, 2016, 2017, 2018 and 2019
4. Does your police force plan to use facial recognition technology in 2020?
5. If your police force plans to use facial recognition technology in 2020, how much money is expected to be spent on the technology and what percentage of the force's technology budget does it represent?
6. If your police force does not use facial recognition technology, by the end of which year do you plan to introduce it (i.e. by end of year 2020, 2021, 2022, 2023, 2024, 2025 etc.)?

Clarification:

Yes, my request is in relation to the use of Live Facial Recognition Technology. I would define this as a technology that is capable of identifying or verifying a person from a digital image or a video frame from a video source. This could be live capture (hardware with LFR on it) or software running on captured images /video.

Responses 1 - 3:

I can confirm that there is no information held by Dyfed-Powys Police due to the fact that Dyfed-Powys Police does not use live facial recognition technology.

Responses 4 - 6:

I can confirm that there is no information held by Dyfed-Powys Police due to the fact that there are no current plans in place to introduce the use of Facial Recognition Technology.

Please note: all of the above responses relate to overt use only.

In addition, with regards to any information relating to the use or trial of covert facial recognition software, Dyfed-Powys Police Force neither confirms nor denies that it holds any other information relevant to the request by virtue of the following exemptions:

Section 24(2) National Security
Section 31(3) Law Enforcement

Sections 24 and 31 are prejudice based qualified exemptions and there is a requirement to articulate the harm that would be caused in confirming or denying that any other information is held as well as carrying out a public interest test.

Overall Harm for NCND

Any disclosure under the FOI Act 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 use or trial of covert facial recognition software 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, which would 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 three 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 Substantial.

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.

Factors favouring confirmation or denial for Section 24:

The public are entitled to know how public funds are spent and by confirming or denying whether any other information is held could lead to a better informed public that can take steps to protect themselves.

Factors against confirmation or denial for Section 24:

By confirming or denying the use or purchase of covert facial recognition software could render security measures less effective. This could lead to the compromise of ongoing or future operations to protect the security or infra-structure of the UK and increase the risk of harm to the public.

Factors favouring confirmation or denial for Section 31:

Confirming or denying whether any other information is held regarding the use or trial of covert facial recognition software would provide an insight into the police service. This would enable the public to have a better understanding of the effectiveness of the police and about how the police gather intelligence. It would greatly assist in the quality and accuracy of public debate, which could otherwise be steeped in rumour and speculation. Where public funds are being spent, there is a public interest in accountability and justifying the use of public money.

Factors against confirmation or denial for Section 31:

By confirming or denying that any other information is held regarding the use or trial of covert facial recognition software would compromise law enforcement tactics which would hinder the prevention or

detection of crime. This would impact on police resources, more crime would then be committed and individuals placed at risk. It has been recorded that FOIA releases are monitored by criminals and terrorists and so to confirm or deny any other information is held concerning specialist covert tactics would lead to law enforcement being undermined.

Balance Test

Confirming or denying whether any information is or isn't held relating to the trial or use of covert 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. 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.
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.

Therefore it is our opinion that for these issues the balancing test for confirming or denying whether any information is held regarding covert facial recognition software is not made out.

None of the above can be viewed as an inference that the information you seek does or does not exist.