BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

OPEN
RIGHTS
GROUP

Big Brother Watch and Open Rights Group joint submission to the Justice Sub-Committee on Policing inquiry on Facial Recognition

November 2019

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation. We hold to account those who fail to respect our privacy, and campaign to give individuals more control over their personal data. We produce unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Open Rights Group

Open Rights Group is a UK based digital campaigning organisation working to protect the rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK. We raise awareness of these threats and challenge them through public campaigns, media commentary, legal actions, policy interventions and tech projects.

Summary

We make the following recommendations in this submission:

- We call on the Committee to **obtain clear and comprehensive information from Police Scotland, and any other public body which intends or proposes to use a type of facial recognition technology, about exactly which type of technology they propose to use and its capabilities. Any such proposals should be subject to public consultation.**
- We call on Police Scotland to **immediately remove all historic images of unconvicted people from the Criminal History System and Police National Database. We call** on the Scottish Parliament **to clarify the legal basis for the police's taking and retention of images.**
- We recommend that **any Police Scotland or other public body's use of post-event facial recognition analysis must be provided for by law, with proper statutory safeguards and guidance including independent authorisation, a requirement for any use to be proportionate and limited to a specific time period and a threshold for strict necessity with no other less intrusive means practicable.**
- We call on Police Scotland **to not use live facial recognition surveillance in public places.**

1. Introduction

1.1 **Facial recognition** technology measures and matches unique facial characteristics for the purposes of biometric surveillance or identification. However, there are several different types of facial recognition technology. There are three types of facial biometric recognition:

- **Facial matching or 'static' facial recognition:** this is the matching of an isolated, still image of an individual against a database. This is used at borders with biometric passports and by police to match images of suspects against images on the Police National Database.

- **Live facial recognition:** this technology matches faces on live surveillance camera footage against a database (such as the custody image database, or a subsidiary 'watchlist') in real time.

- **Post-event or retrospective facial recognition:** this is the use of facial recognition technology to search through recorded surveillance camera or other video footage, matching people's faces captured in that footage against a database of images.

1.2 Its important to be clear about exactly what form of facial recognition technology is being used or proposed, as each distinct use engages people's legal rights in different ways or engages different rights. In Police Scotland's Policing 2026 strategy, a description is given of an example policing day in 2026. It describes an event occurring, following which the officer

> *"access[es] the local Council CCTV app on my device and observe the assault… I download the footage I need. The suspect has been recognised by facial recognition software".*[1]

1.3 Its not clear exactly what form of facial recognition technology this refers to. This process could relate to either a form of static facial recognition, where still images from the council CCTV have been downloaded, or post-event facial recognition analysis, where a section of video footage has been downloaded and facial recognition software applied to it.

1.4 In this submission, we will consider the different uses of facial recognition technology and the different impacts these have on people's rights and freedoms,

[1] https://www.scotland.police.uk/assets/pdf/138327/386688/policing-2026-strategy.pdf

and seek to inform the Committee and parliamentarians of the significant risks facial recognition surveillance poses to human rights and the rule of law.

1.5 **We recommend that the Committee obtains clear and comprehensive information from Police Scotland, and any other public body which intends or proposes to use a type of facial recognition technology, about exactly which type of technology they propose to use and its capabilities.**

Private company facial recognition

1.6 We would also draw the Committee's attention towards the use of facial recognition by private companies in the UK. Big Brother Watch's investigations in August 2019 uncovered numerous private companies using live facial recognition in England and Wales,[2] as well as partnerships between police forces in England and Wales, such as between the Metropolitan Police and British Transport Police and the Kings Cross Estate Development.[3]

Race and gender bias

1.7 There are serious concerns about the discriminatory impact of facial recognition surveillance. A number of independent studies have found that various facial recognition algorithms, including both live and static facial recognition, have demographic accuracy biases – that is that they misidentify some demographic groups, particularly women and people of colour, at higher rates than others, such as white men. A study found that commercial facial recognition technologies, including those created and sold by Microsoft and IBM, had error rates of up to 35% when identifying the gender of dark-skinned women compared to 1% for light-skinned men.[4] A follow up study found that Amazon's 'Rekognition' software mistook women for men 19% of the time, and darker-skinned women 31% of the time.[5]

1.8 The Biometrics and Forensics Ethics Group warned that UK police's use of live facial recognition technology also has the "*potential for biased outputs and biased decision-making on the part of system operators*".[6]

[2] https://www.telegraph.co.uk/technology/2019/08/16/investigation-finds-facial-recognition-epidemic-across-british/

[3] https://www.bbc.co.uk/news/technology-49921175

[4] http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

[5] http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf

[6] Biometrics and Forensics Ethics Group, Interim report, February 2019

2. Static facial recognition and facial matching

2.1 As stated, this is the matching of an isolated, still image of an individual against a database of images. For example, a photograph or a still image from surveillance camera footage can be compared against mugshots on the Police National Database.

2.2 Police Scotland is using static facial recognition and facial matching. This practice was investigated by Her Majesty's Inspectorate of the Constabulary Scotland (HMICS) in 2016. At that time concerns were raised about the lack of oversight of this practice and this lead in part to the proposed Scottish Biometrics Commissioner Bill which is currently being debated.

Innocent people's images on police databases

2.3 There is an ongoing and serious concern over the continued and growing retention of innocent people's custody images on police databases, including Police Scotland, and their creation into searchable facial biometric images.

2.4 Police forces in England and Wales are holding hundreds of thousands of innocent people's custody images on the Police National Database.[7] The England and Wales High Court ruled in 2012 in *RMC & FJ* that the indefinite retention of innocent people's custody images was "unlawful".[8] In a response that took 5 years, the Home Office created a policy in their 2017 Custody Image Review whereby innocent people could write to their local police force to request the deletion of their custody image.[9] However, the new policy is little known, rarely used, and does not meet the minimum requirements set out in the 2012 judgment.

2.5 The Information Commissioner has said that *"there are potentially thousands of custody images being held with no clear basis in law or justification for the ongoing retention"*.[10] The Biometrics Commissioner for England and Wales has said in

[7] BBC News Online, 'Facial recognition database 'risks targeting innocent people', 14 September 2018 (http://www.bbc.co.uk/news/uk-41262064)

[8] *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681 (Admin)

[9] Home Office, 'Review of the Use and Retention of Custody Images', February 2017 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf)

[10] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science

evidence to the Science and Technology Committee that at the time the Custody Image Review was published, he *"was not at all sure [the Review] would meet further court challenges*" and that he still believes this is the case: "*I am not sure that the legal case is strong enough and that it would withstand a further court challenge*".[11]

Police Scotland

2.6 There is a similar issue in relation to Police Scotland's historic retention of innocent people's custody images. We welcome Police Scotland's current policy in relation to the retention of images on its Criminal History System, which aligns with the legal requirements for unconvicted people's DNA and fingerprints set out in the Criminal Procedure (Scotland) Act 1995, and differs from the 'request for deletion' approach implemented in England and Wales. In Scotland, images are not uploaded to the Criminal History System unless an individual is charged with a crime, and if there is no conviction within 6 months of an investigation concluding, the image is deleted from the Criminal History System and Police National Database.[12]

2.7 However, there is an issue over legacy custody images, left over before this policy and system was implemented in January 2017, when Police Scotland had no policy or system in place to remove the images of people who were not subsequently charged or convicted.[13]

2.8 Police Scotland does not know how many custody images it holds,[14] but it was estimated in March 2018 that it currently holds or retains "more than 1 million custody images",[15] a figure which is likely to have grown over the last 18 months. As Police Scotland is currently using this database for facial matching, and there is the possibility that it will be used for further uses of facial recognition, either for retrospective facial recognition analysis or live facial recognition surveillance,

-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/written/97934.pdf

[11] Science and Technology Committee oral evidence, 19 March 2019 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/the-work-of-the-biometrics-commissioner-and-the-forensic-science-regulator/oral/98556.pdf)

[12] https://www.gov.scot/publications/report-independent-advisory-group-use-biometric-data-scotland/pages/4/

[13] https://www.gov.scot/publications/report-independent-advisory-group-use-biometric-data-scotland/pages/4/

[14] Open Rights Group Freedom of Information request – Annex A

[15] https://www.gov.scot/publications/report-independent-advisory-group-use-biometric-data-scotland/pages/21/

innocent people are increasingly at risk of being wrongfully stopped or even arrested. This blurs the line between the innocent and the guilty, and makes a mockery of the presumption of innocence.

2.9 There is also an issue with the legal basis under which Police Scotland takes and retains custody images. As pointed out by Her Majesty's Inspectorate of the Constabulary Scotland in 2016[16] and again by the Independent Advisory Group on the use of Biometrics by Police in 2018[17], there is no legislative power for the police to take facial images under the Criminal Procedure (Scotland) Act 1995. As these images form the basis of any facial recognition system – be it static, live, or post-event – the legal basis for their use is not clear and this must be addressed to provide clarity to Police Scotland and to the public.

2.10 **We call on Police Scotland to immediately remove all historic images of unconvicted people from the Criminal History System and Police National Database, and on the Scottish Parliament to clarify the legal basis for the police's taking and retention of images.**

3. Post-event or retrospective facial recognition analysis

3.1 The potential for facial recognition technology to be applied to the masses of CCTV footage captured in public spaces, which may be under consideration by Police Scotland as part of the Policing 2026 strategy, would have a serious impact on data protection and rights.

3.2 Used proportionately in strictly necessary cases, on limited footage of suspects and crime scenes, post-event facial recognition could be a useful forensic tool. However, unrestricted police use of facial recognition technology applied to recorded CCTV or video surveillance could transform generalised, passive video recording into mass, active biometric surveillance. In extremis, it could be used for general intelligence gathering or location-tracking of individuals, building up an intrusive picture of an

[16] Audit and Assurance Review of the use of the Facial Search functionality within the UK Police National Database (PND) by Police Scotland, Para. 30, 27 January 2016 https://www.hmics.scot/publications/audit-and-assurance-review-use-facial-search-functionality-within-uk-police-national. (accessed 1 November 2019).

[17] Use of Biometric data: report of the independent advisory group, para. 2.9 https://www.gov.scot/publications/report-independent-advisory-group-use-biometric-data-scotland/pages/4/ (accessed 1 November 2019).

individuals' whereabouts and movements. The current regulatory vacuum around this technology raises serious concerns over the protection of fundamental rights to privacy and freedom of expression. Unrestricted use of retrospective facial recognition for intelligence or location-tracking purposes would have a significant chilling effect on people's behaviour, as people would be less willing to behave freely in public spaces if they knew they were creating an identifiable record of their movements and associations by doing so .

3.3 There is a clear need for appropriate laws, policies and guidance around such use of post-event facial recognition technology on recorded CCTV or video surveillance, and clear, strong safeguards against its disproportionate use . There is clear legal authority and safeguards around the way police use other biometric identification technologies such as fingerprints and DNA, and facial biometrics should be no different.

3.4 No public body, including the police, should be able to deploy post-event facial recognition surveillance before such policies and safeguards are in place, and it must be subject to independent authorisation. Such authorisation should assess, for example, whether application of the technology is proportionate for a legitimate purpose; whether the data available in the footage in question and the database being referenced is limited to that which is strictly necessary; and whether less intrusive means are practicable. Any use of post-event facial recognition surveillance must be strictly necessary for a legitimate purpose, such as targeting an incident of serious violent crime, and there must be a proportionate reason to do so, such as there being no other less intrusive means by which to identify the individual(s) sought. The technology used must be able to accommodate these requirements. There must also be meaningful human input into any identifications made and any subsequent actions taken.

3.5 To promote transparency and accountability, any public body, including the police, using post-event facial recognition technology should publish the details of the technology its seeks to use, and its capabilities.

3.6 **We recommend that any use of post-event facial recognition analysis is provided for by law, with proper statutory safeguards and guidance, including independent authorisation, a requirement for any use to be proportionate and limited to a specific time period, and a threshold for strict necessity, with no other less intrusive means practicable.**

4. Live facial recognition

4.1 Police Scotland is not currently using live facial recognition surveillance. However, police forces in England and Wales have used facial recognition extensively in public spaces.

4.2 There are significant concerns over the legality of police use of live facial recognition, particularly the likely infringement of people's fundamental rights, the aggressive over-policing witnessed during deployments, its use for non-criminal purposes, as well as the spurious nature of the police's 'trial'. The emergence of live facial recognition in policing in the UK has caused national and international controversy and undermined public trust in the police.

4.3 Big Brother Watch has revealed that the police's use of live facial recognition has been staggeringly inaccurate, based on Freedom of Information requests to the police, resulting in thousands of innocent people having their photos taken by police without their knowledge and many people stopped and made to prove their innocence to police.[18]

No legal basis

4.4 There is no explicit statutory basis for England and Wales police use of live facial recognition surveillance. When Layla Moran MP posed a written question to the Home Office about current legislation regulating *"the use of CCTV cameras with facial recognition and biometric tracking capabilities*", Nick Hurd MP (Minister for Policing, responding for the Home Office) answered: "*There is no legislation regulating the use of CCTV cameras with facial recognition*".[19]

The threat to human rights: A threat to the right to privacy

4.5 Live facial recognition cameras, acting as biometric identification checkpoints, are a clear threat to both individual privacy and privacy as a social norm.

[18] https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf; https://bigbrotherwatch.org.uk/all-media/campaigners-urge-met-to-drop-disastrous-facial-recognition/

[19] https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-09-04/8098/

4.6 The Human Rights Act 1998 requires that any interference with the Article 8 right to a private life is both necessary and proportionate. However, the use of live facial recognition with CCTV cameras in public spaces appears to fail both of these tests.

4.7 Live facial recognition cameras scan the faces of every person that walks within the view of the camera; the system creates, even if transitorily, a biometric scan of every viewable person's face; it compares those biometric scans to a database of images; and it retains photos of all individuals 'matched' by the system, despite 96% of matches inaccurately identifying innocent people. This effectively subjects members of the public to an arbitrary police line up.

4.8 Members of the public who have been scanned by live facial recognition are unlikely to be aware that they were subject to the identity check, and do not have a choice to consent to its use. The Biometrics Commissioner commented:"*(…)unlike DNA or fingerprints, facial images can easily be taken and stored without the subject's knowledge.*"[20]

4.9 The Surveillance Camera Commissioner has said that "*overt use of such advancing technology (AFR) [live facial recognition] is arguably more invasive than some covert surveillance techniques*."[21]

4.10 Proportionality is a particular concern in relation to live facial recognition due to the general and indiscriminate nature in which the camera biometrically scans the public, often without their knowledge and always without their consent or indeed any objective evidence of wrongdoing.

4.11 The Information Commissioner"s Office released the results of her investigation into UK police use of live facial recognition in October 2019. She has said that she is concerned with facial recognition due to the:

> *"scale of privacy intrusion, with the potential to affect large numbers of people, in many cases without their knowledge, as they go about their daily lives"*
>
> *(…)*

[20] Biometric Commissioner, *Annual Report 2016*, September 2017, para. 305

[21] https://www.gov.uk/government/publications/surveillance-camera-commissioner-newsletters/april-2019

> *"the potential for facial recognition technology to enable surveillance on a mass scale, and the impact this has on individuals' human rights and information rights"* [22]

4.12 In a recently published Opinion on the use of live facial recognition by police in public places, the Information Commissioner also stated:

> *"...a controller has to be able to clearly explain why the use of LFR* [live facial recognition]*, which is an intrusive tactic, is strictly necessary where other less intrusive options may be available."* [23]

The threat to human rights: A threat to the right to freedom of expression

4.13 The right to go about your daily activity undisturbed by state authorities, to go where you want and with whom, and to attend events, festivals and demonstrations, is a core principle of a democratic society protected by Article 10 of the Human Rights Act 1998. The biometric surveillance and identification of individuals in public spaces and at public events, in particular political demonstrations, is clearly incompatible with that fundamental right.

4.14 We are concerned that the use of live facial recognition with CCTV has a chilling effect on people's attendance of public spaces and events, and therefore their ability to express ideas and opinions and communicate with others in those spaces.

Overpolicing

4.15 In observations of the Metropolitan Police's trials, Big Brother Watch observers have witnessed numerous individuals being treated unfairly by police in the course of misidentifications and wrongful stops. Here are two case studies:

> *Case study 1*
>
> A 14 year old black school child, wearing school uniform, was wrongly identified by the facial recognition system and subsequently surrounded by four plainclothes police officers. He was pulled onto a side-street, his arms held, questioned, asked for his phone, and even fingerprinted. He was released after ten minutes when police realised they had the wrong

[22] https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf
[23] https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

person. The child appeared frightened and said he felt was being harassed by police.

Case study 2

A man was stopped for covering his mouth and chin with his jacket after seeing facial recognition signs and expressing his objection to the deployment. His reaction was observed by a plainclothes police officer who followed him and radioed through to other officers to make a stop. Police demanded his ID and the man complied. However, protesting against the facial recognition cameras, he was issued with a £90 public order fine for 'shouting profanities in public view'. The man was not wanted for any crime, and after being fined, he was released. This was captured by a BBC film crew present.[24]

Independent report on the Metropolitan Police"s use of live facial recognition

4.16 An independent review into the use of live facial recognition commissioned by the Metropolitan Police found that over the four-year trials, 81% of 'matches' had wrongly identified innocent people as 'wanted'. The review concluded it was *"highly possible"* that the force's use of the technology would be found unlawful if challenged in court.[25] Big Brother Watch has initiated a legal challenge which is currently stayed pending the Metropolitan Police"s decision as to whether to use live facial recognition surveillance again or not.

Joint statement on police and private companies' use of live facial recognition

4.17 Leading MPs from across the political spectrum and 25 rights, race quality and expert technology groups, as well as academics and lawyers, have called for UK police and private companies to immediately stop using live facial recognition surveillance in public spaces.[26] This includes David Davis MP, Diane Abbott MP, Jo Swinson MP, and the chair of the Science and Technology Committee, Norman Lamb MP.

[24] https://www.youtube.com/watch?v=0oJqJkfTdAg

[25] https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

[26] https://bigbrotherwatch.org.uk/wp-content/uploads/2019/09/Statement-to-stop-live-facial-recognition-surveillance-BBW-September-2019.pdf

4.18 The Science and Technology Committee has also called for a moratorium on the use of live facial recognition.[27]

4.19 **We call on Police Scotland to not use live facial recognition surveillance in public places.**

5. Other emerging surveillance technologies

5.1 An area of emerging technology in Scotland is the Suspect Search system which was installed by Community Safety Glasgow, a collaboration between Glasgow City Council and Police Scotland.[28] This emerging technology again reiterates the need for clarity around the technologies being used; while media reports stated this was a form of 'facial recognition', it appears not to utilise biometric facial recognition nor compare facial images. The system, provided by NICE (now Qognify), allows for individuals to be tracked across a camera system after a photo is uploaded, or an avatar created, that is then searched against available captured recordings.[29]

5.2 The system is not yet deployed as current legal requirements have not been completed. The Suspect Search system also raises the question of a private or public sector body deploying surveillance technology that Police Scotland subsequently have access to or rely on. We encourage the Justice Sub-Committee to consider this, as the ICO has also recently highlighted this an area they are preparing to focus on.

[27] https://www.bbc.co.uk/news/technology-49030595

[28] NICE Safe City Solutions Deployed in Glasgow to Bolster Security, Safety, and Operations Management, June 11 2014, https://www.nice.com/protecting/press-releases/NICE-Safe-City-Solutions-Deployed-in-Glasgow-to-Bolster-Security-Safety-and-Operations-Management-137.

[29] Big Brother-style facial recognition cameras installed on Glasgow CCTV, Evening Times, 27 April 2019, https://www.eveningtimes.co.uk/news/17601662.big-brother-style-facial-recognition-cameras-installed-on-glasgow-cctv/ .

ANNEX A

Our Ref: IM-FOI-2019-2053
Date: 23 September 2019

FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

I refer to your recent request for information which has been handled in accordance with the Freedom of Information (Scotland) Act 2002.

Before I answer your specific questions, I have provided some additional information which may provide additional context to the answers below.

The Scottish Criminal History System (CHS) is a tool to aid police with crime detection, prevention and administration by providing access to structured data about individuals. All data held is subject to legislation contained in the Data protection Act 2018, and the Computer Misuse Act 1990.

CHS holds images of persons who have been arrested and charged with a crime or offence and appropriate weeding policies are in place as outlined in the answers provided below.

Police Officers have the power to obtain a range of samples, including images/photographs, of arrested persons regardless of whether they are subsequently charged or not. Only those images of persons charged with a crime or offence are uploaded to CHS.

For ease of reference, your request is replicated below together with the response.

- The number of individual images currently held in the Criminal History System and the number of individuals these images relate to.

As of 2 September 2019, there were 658,727 images of 365,972 people held on the Scottish Criminal History System (CHS).

It should be noted that the weeding of images held on CHS is a continuous process whereby data (including images) is managed as stated within the Recording, Wedding and Retention of Information on Criminal History System (CHS) Guidance. This is a public document which can be accessed via the following link:

Recording, Weeding and Retention of Information on Criminal History System

Accordingly, the number of images added and removed will vary continuously and there will be multiple reasons why images are being removed, including the decision not to proceed with a prosecution or a finding of non-guilt.

- The number of custody photographs currently held.

You have confirmed that by this you mean photographs of individuals when detained or arrested, prior to CHS images being created.

As you may be aware the current cost threshold is £600 and I estimate that it would cost well in excess of this amount to process your request.

As such, and in terms of Section 16(4) of the Freedom of Information (Scotland) Act 2002 where Section 12(1) of the Act (Excessive Cost of Compliance) has been applied, this represents a refusal notice for the information sought.

It is not possible to provide this information as due to legacy practices, processes and various IT systems this would require a significant amount of time. To give you an estimation of how long this would take, each year we process approximately 150,000 nominals, to check each record,w even at 1 minute per record would still equate to 2500 hours of work.

However, work is currently at an advanced stage to modernise this approach and implement a single approach for Police Scotland.

- A copy of weeding and retention policies in relating to facial images held by Police Scotland.

Our interpretation of 'facial images' is CHS images and custody photographs. As already stated above, the following link provides information on weeding and retention policies with respect to CHS images:

Recording, Weeding and Retention of Information on Criminal History System

In relation to custody images / photographs obtained prior to the CHS images being created, there is currently no existing weeding and retention policy. However, one is being developed and will be incorporated into the next review of the Police Scotland Records Retention Standard Operating Procedure.

- If a weeding and retention policy is available, the results of the application of that policy to the CHS and custody photographs systems at any time since January 2017.

FOI requests only relate to the information held at the time the request is made. However, in relation to CHS this is not something that is possible to count. Weeding of images is a continuous process with images being added and removed continuously and there will be multiple reasons why images are being removed, including the decision not to proceed with a prosecution or a finding of non-guilt. The CHS system therefore does not allow for this type of data to be collated and extracted from the system.

In relation to custody photographs, as referred to above there is no such policy in existence just now however one is at an advanced stage of development. In practice, as soon as such an image is no longer required for operational purposes and is either not being uploaded to or is uploaded to CHS, it should be deleted. It is not possible to provide data in respect of this practice as no single system or approach is in place (one is being developed) and therefore it is not possible to track the process of deletion of such images.

Should you require any further assistance please contact Information Management - Edinburgh on 0131 311 3901 quoting the reference number given.

If you are dissatisfied with the way in which Police Scotland has dealt with your request, you are entitled, in the first instance, to request a review of our actions and decisions.

Your request must specify the matter which gives rise to your dissatisfaction and it must be submitted within 40 working days of receiving this response - either by email to foi@scotland.pnn.police.uk or by post to Information Management (Disclosure), Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH.

If you remain dissatisfied following the outcome of that review, you are thereafter entitled to apply to the Office of the Scottish Information Commissioner within six months for a decision. You can apply online, by email to enquiries@itspublicknowledge.info or by post to Office of the Scottish Information Commissioner, Kinburn Castle, Doubledykes Road, St Andrews, Fife, KY16 9DS.

Should you wish to appeal against the Office of the Scottish Information Commissioner's decision, there is an appeal to the Court of Session on a point of law only.

As part of our commitment to demonstrate openness and transparency in respect of the information we hold, an anonymised version of this response will be posted to the Police Scotland Freedom of Information Disclosure Log in seven days' time.