Subjects of Interest (SOIs) – Detailed Privacy Notice to be read in conjunction with our General Privacy Notice

What is Facewatch and why is it unique?

Facewatch is the only national crime prevention system for businesses using facial recognition technology. Because of our unique position as a national data controller and our strict deletion of data to protect privacy we are one of the very few private sector organisations able to satisfy the "Substantial Public Interest" test required under the General Data Protection Regulations which enables us and our customers to use facial recognition for crime prevention.

What makes someone a Subject of Interest?

Business subscribers and police can upload images and basic data of individuals reasonably suspected to have committed crime or disorder – we refer to these as "Subjects of Interest" or SOIs. A Business subscriber's reasonable suspicion will ordinarily be based on witnessing the alleged offence in person or from CCTV. We also add SOIs publicly posted on police websites and on the Crimestoppers website for the prevention of crime to our watchlists and update the images on a monthly basis so they are up to date.

We hold personal data about SOIs because we and our business customers are lawfully allowed to do so to prevent and detect unlawful acts in their businesses and processing SOI information and using facial recognition to create alerts is necessary to achieve this. It is also in the substantial public interest to prevent and detect crime.

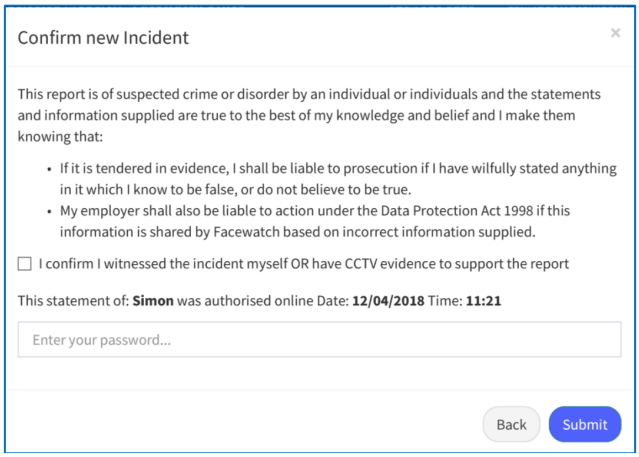
We cannot ask SOIs for consent to process their data because it would prejudice the purposes of the processing, namely preventing and detecting unlawful acts.

How SOI data is added to the Facewatch system

We have legal agreements with businesses and police forces allowing them to share data with us for the purposes of preventing and detecting crime. Each business/police force appoints users to the system who can only login with their own usernames so we know exactly who enters information. The users can only upload SOI personal data to our system through incident reports which contain:

- The date of the offence or suspected offence
- A picture of the SOI face
- The SOI name if known
- A short summary of what happened

The user is then required to confirm a statement as follows and they then have to re-enter their password:



We believe that these precautions will prevent a user from uploading information in error or maliciously. However, should this be found to have happened it will be considered both a breach of our terms of use and a data security breach which may be notifiable to the Information Commissioner's Office (ICO). Possible consequences are that the company be removed from our system and be subject to censure or fines from the regulator (the ICO).

Sharing through Watchlists

We share the pictures of SOIs (with just a tag for their crime types and no other information) with businesses by creating Watchlists which are unique to each business property. Watchlists contain pictures of SOIs that might try to commit crime in that property and are calculated using algorithms to estimate where an SOI is most likely to carry out crimes (normally using a geographic radius).

For commercial confidentiality reasons we do not publish the precise method of sharing SOI images but the key point is that we aim to do this in a proportionate manner - so, to take an extreme example, if a shop thief normally steals from shops in Kingston then goes on holiday in Glasgow their face will not appear on any watchlists in Glasgow unless they have been reported for actual or suspected crimes there already.

How long is SOI data kept on the system?

Every incident is deleted from our live system after a maximum of 24 months and is then backed up for 30 days (but not available to users) after which it is permanently deleted. The only exception is if the police have specifically requested us to keep an SOIs data on the system.

Is SOI data ever used for other purposes, made public or shared overseas?

No, all data remains in the UK on highly secure servers and is only available to businesses through watchlists and to police forces and crime prevention organisations which have entered into legal agreements with us specifying that the only reason for sharing the data is for the prevention and detection of unlawful acts.

How do Facial Recognition Alerts work?

Each business property subscribing to Facewatch Real Time Alerts has a camera or cameras pointing at entrances or pinch points. The cameras are connected to secure local servers and the faces of everyone passing in front of the cameras are turned into facial recognition templates (ie measurements of a face) which are securely transmitted to our cloud service. No facial recognition data or images are held for more than 10 seconds on our systems unless there is a match to an SOI.

The facial recognition template of the people entering our customers' properties are used to compare to the templates of the SOI images on the watchlists and if there is a match the system creates an alert. The alerts show the image of the person who has just entered the premises and the SOI image from the watchlist side by side. The user receiving the alert can either:

a. Confirm the alert is correct and take action depending on their company policy (Eg to communicate with or observe the SOI)
b. Click an option to say the suggested match is wrong (it is then deleted instantly) or
c. if no verification is entered within 1 hour the alert is deleted.

The facial recognition algorithms we use are extremely powerful so the chances of an incorrect alert are slim. However, by having the user verification process we ensure that there is no fully automatic processing and so the chance of mistaken identity is absolutely minimal. Even if in the highly unlikely situation where an alert was wrong and a user also

made the same mistake it doesn't mean the SOI is deemed to be guilty and instantly carted off to prison! The aim is simply to make the shop aware that an SOI is on their premises.

Facial Recognition and the law

We and our business customers have to comply with a higher threshold of compliance when processing using facial recognition algorithms because these are deemed to be biometric data which falls under what is called Special Category data for data protection purposes.

We can lawfully process facial recognition data because we are able to demonstrate that it is in the Substantial Public Interest at a national level for us to prevent and detect crime.

Can you or the police track SOI movements using the facial recognition system?

No, we cannot track SOI movements because alerts are removed from the system after 24 hours. They are backed up for record keeping purposes for up to 60 days but are not accessible unless the police obtained a court issued warrant.

Your Rights if you are (or believe you may be) on Facewatch as an SOI

We will always try to ensure that your rights are respected whoever you are. The General Data Protection Regulations set out a list of your rights which are shown on the summary Privacy Notice on our website and a link to them on the ICO website is included below. If you feel that you are on our system and you shouldn't be, please do not hesitate to contact us through our Subject Access Request form and we will do our utmost to sort it out as quickly as possible. We will probably need to ask you for a current photograph so that we can search for you on the database because your name is unlikely to be on the system.

Every organisation that controls or processes data is regulated by the Information Commissioners Office (ICO). The full text of the rights of individuals and more explanation about them is included in the ICO's website and if you have any concerns about the way your data is being handled by us you can raise these with ICO here.

And finally

If you are on hard times and have fallen into a life of crime there are many organisations who can help you – try to talk to them. Here are a few:

Prince's Trust | YOUTH CAN DO IT

Unlock for people with convictions

together FOR MENTAL WELLBEING