Sophie Linden
Deputy Mayor for Policing and Crime in London

Sent by email: enquiries@mopac.london.gov.uk

CC:
Tony Porter, Surveillance Camera Commissioner
Elizabeth Denham CBE, Information Commissioner's Office
Cressida Dick, Commissioner of the Metropolitan Police Service

Friday, 9 October 2020

Dear Sophie Linden,

We are writing to provide information and call your attention to the use of facial recognition networks that are facilitated by private companies across the UK. Specifically, we are highly concerned about the ongoing deployment of the Facewatch surveillance network, which we believe could provide UK law enforcement a 'backdoor' through which to roll out highly invasive facial recognition technology, and which requires your urgent scrutiny.

Privacy International (PI) campaigns against companies and governments who exploit our data and technologies. We expose harm and abuses, mobilise allies globally, campaign with the public for solutions, and pressure companies and governments to change.

Facewatch

Facewatch Limited, Company Number 7209931, was founded in 2010 and describes itself as a "cloud-based facial recognition security system [which] safeguards businesses against crime."[1] Premises using the system are alerted when Subjects of Interest (SOI) enter their premises through the use of facial recognition cameras. Facewatch's privacy policy states that subscribers "are able to report new SOIs through incidents which include a formal witness statement."[2] Facewatch has "a National Watchlist of Subjects of Interest" which allows them to then "create a personalised watchlist for every one of our customer's properties

[1] https://www.facewatch.co.uk

[2] https://www.facewatch.co.uk/privacy/

individually."[3] In addition to an alert system, Facewatch allows premises to run analytics through their customers, including by gender and ethnicity.[4]

According to their privacy policy, Facewatch are the data controller for all facial images collected at the premises using the Facewatch software as well as the data controller for the aforementioned watchlists, under the EU General Data Protection regulation (GDPR) and the UK Data Protection Act 2018.

How extensively the system is used is not exactly known; only one convenience store, Budgens in Buckingham Park, has publicly confirmed[5] it is using the system, while the FT reported in 2019 that the system was being tested by a 'major UK supermarket chain'.[6] In its 2016/17 annual report[7], Birmingham City Council stated that there were "757 registered FaceWatch users representing 828 businesses", which had submitted 2892 crime and intelligence reports to police and partners, resulting in 1080 Banning Notices.

In 2019, the company reported retained earnings of £6.6 million.[8]

The company also exports internationally, with distributors in Argentina, Spain and Brazil[9]; specifically, in Brazil, it is reportedly in use in three commercial centres, and in one month captured 2.75 million faces.[10]

Sharing with Police

[3] https://www.facewatch.co.uk/privacy/facewatch-and-gdpr/

[4] https://assets.digitalmarketplace.service.gov.uk/g-cloud-11/documents/92526/211868666506697-service-definition-document-2019-04-10-1043.pdf p13

[5] https://www.facewatch.co.uk/2019/06/28/facewatchs-facial-recognition-security-camera-used-by-budgens/

[6] https://www.ft.com/content/605de54a-1e90-11e9-b126-46fc3ad87c65

[7] https://bit.ly/3jW2Ow7

[8] https://beta.companieshouse.gov.uk/company/07209931/filing-history

[9] https://www.facewatch.co.uk/2020/01/06/facewatch-launches-in-spain-with-the-appointment-of-retail-technology-business-leader-sbt/

[10] https://www.ft.com/content/605de54a-1e90-11e9-b126-46fc3ad87c65

According to the FT, in 2019[11], "Facewatch is about to sign data-sharing deals with the Metropolitan Police and the City of London police, and is in talks with Hampshire police and Sussex police".

According to the founder of Facewatch, Simon Gordon, "The deal with police is they give us face data of low-level criminals and they can have a separate watchlist for more serious criminals that they plug in…" If the systems spot a serious criminal, the alert is sent directly to the police, rather than to retailers, according to the FT.

The governor of Rio de Janeiro has similarly said[12] that he "plans to allow the police to share their watch lists of members of organised crime suspects with facial recognition companies".

PI is not aware whether Facewatch has in fact entered into any such agreements with any UK police force, and has not received a response from Facewatch when we asked the company in both June and September 2020. In response to a Freedom of Information request, Reference No: 01/FOI/19/002194 (attached), the Metropolitan Police Force confirmed to PI that they did not have "a copy of any data sharing agreements or similar such contracts with FaceWatch" between 1 January 2015 and 10 May 2019.

We note that following the October 2019 revelations that a property developer was using facial recognition software around the King's Cross site for two years from 2016 without any apparent central oversight from either the Metropolitan police or the office of the mayor, the Met Police produced a report admitting that images of seven people were passed on by local police for use in the system in an agreement that was struck in secret. In the same report, the Met Police underlined that "The MPS is not currently sharing images with any third parties for the purposes of Facial Recognition[13]."

[11] https://www.ft.com/content/605de54a-1e90-11e9-b126-46fc3ad87c65
[12] https://www.ft.com/content/605de54a-1e90-11e9-b126-46fc3ad87c65
[13] https://www.london.gov.uk/sites/default/files/040910_letter_to_unmesh_desai_am_report_re_kings_cross_data_sharing.pdf

However, Facewatch has uploaded a template Information Sharing Agreement (ISA) to the government G-Cloud system, which states "Based originally on Met Police Template."[14] As explained in the ISA:

"Facewatch also enables the Police to upload images to the Watchlist and be alerted to Major Crime SOIs and Missing Persons if they enter Subscriber Premises. These Major Crime SOI's and Missing Person SOI's and any alerts related thereto are not shared with Facewatch Subscribers."

The ISA envisages further the use of a segregated watchlist system only available to the police. This would in effect transform what is a retail crime alerting system into an extensive, potentially nationwide, police facial recognition surveillance system.

As of March 2019, Facewatch pricing list[15] makes clear:

"Police may upload Subjects of Interest for Major crime, CT incidents knowing that this is completely secure and under their control as they will manage the cloud servers hosting the segregated system.

Algorithmic probes from cameras sited in Facewatch Subscriber properties of all persons entering will be sent to the segregated system to compare against the police confidential watchlist.

Police will receive alerts to specified users.

Police will also have access to the main Facewatch business system to search for intelligence (eg Stop and Search, take a photo to see if individual is on Police or Business system)."

The ISA clarifies how this system would work:

[14] https://assets.digitalmarketplace.service.gov.uk/g-cloud-11/documents/92526/211868666506697-terms-and-conditions-2019-04-10-1045.pdf

[15] https://assets.digitalmarketplace.service.gov.uk/g-cloud-11/documents/92526/211868666506697-pricing-document-2019-04-10-1138.pdf

"In a segregated system Police are provided with a stand-alone copy of the Facewatch system in a segregated cloud server under their own control. Only Police can upload, view and remove SOI's in this server.

Facewatch will transmit Probes of individuals entering Subscriber premises directly to the segregated system. The Probes are compared to the segregated system watchlist(s) and if there is a match the segregated system requests the "just seen" image from the Edge Equipment and an alert is sent to Police showing the watchlist image and the just seen image with a percentage match score. If there is no match the Probe is deleted immediately from the segregated system."

The ISA outlines the sharing of three types of batch data. Category A, Low risk, would allow Police to upload "images extracted from *Police* custody imaging system, CCTV or Body Worn Camera footage of individuals... who are believed to be committing criminal acts within the area and are considered low risk." Category B would allow *Police* to upload images to separate police watchlist(s) in a segregated system which only alert *Police*, and would cover more serious crimes. And Category C would allow police to "create watchlists for their own purposes without reference to Facewatch.

Facewatch makes clear that Police authorities may also use the system as an intelligence tool:

"Police may use Alerts and information available by logging into the Facewatch system to identify SOIs and to support enquiries, operations and crime prevention. Police will consider the application of relevant legislation to the circumstances."

Concerns

If such a system were to be widely deployed it would be a radical extension of the police's surveillance powers. It would extend police use of live facial recognition, currently under legal challenge, into every participating shop, restaurant, or bar.

The outsourcing of facial recognition to the private sector in such a way would enable the surveillance of drastically higher amounts of people while offering them less legal safeguards.

For example, the Metropolitan Police have so far insisted[16] that use of facial recognition would be at "specific locations…focused on a small, targeted area… clearly signposted [and] not linked to any other imaging system, such as CCTV, body worn video or ANPR [i.e. Automatic number-plate recognition]."

Given that Facewatch reportedly captured some 2.75 million faces in Brazil in one month, across what is presumably only three commercial centres, it is clear that such a network would give police access to drastically more facial recognition cameras, raising urgent questions around transparency, legality, necessity and proportionality. While the deployment of facial recognition by police may be "clearly signposted", it is not clear if this will be the case if the police use Facewatch's system, as it is questionable whether the use of the latter can abide by existing legal frameworks. And while the Met Police claims their deployment won't be linked to CCTV, body worn video or ANPR, Facewatch's ISA explicitly claims images may be obtained from CCTV or Body Worn Camera footage.

Assigning pre-emptive policing functions or endorsing the existence of private surveillance networks distorts long-established societal premises of privacy and perceptions of authority. In absence of a precise and public legal framework, as well as clear safeguards, the existence of facial recognition networks will inevitably blur the lines between public and private spaces, allowing for the erosion of our privacy rights, but also fundamental freedoms.

Request

Given these concerns, we are writing to ask that you confirm:

- Whether you are aware and have reviewed any privacy as well as any other fundamental rights concerns related to the use of Facewatch or similar such surveillance system, and whether you have made any related recommendations;

- Whether you believe the legal framework governing the use of Facewatch or similar systems is currently sufficiently clear and able to satisfy the requirements of clarity, foreseeability and accessibility as well as the legal tests of necessity and proportionality under the GDPR and the UK Data Protection Act 2018;

[16] https://techcrunch.com/2020/01/24/londons-met-police-switches-on-live-facial-recognition-flying-in-face-of-human-rights-concerns/?guccounter=1

- Whether, to the best of your statutory authority, you will investigate whether or not Facewatch or any such company has in fact entered into official or unofficial agreements involving the sharing of facial images or other biometric data with any police force in the UK;

- In case you share our concerns, whether you will initiate a thorough investigation and publish an opinion on the lawfulness of any such deployment;

- Whether you will ascertain whether Facewatch, or any other private company offering similar facial recognition technology solutions for retailers and business owners, has in fact entered into such a data sharing agreement with the Metropolitan Police or whether it is likely to in the near future;

- If the Metropolitan Police has entered into such an agreement, whether you will fully investigate the circumstances and provide to the public as much information as possible about this as well as any other facial recognition arrangement that the Metropolitan Police has entered or will be entering with private companies offering facial recognition solutions.

We would like to thank you for your attention to this matter and we are mindful of the challenging commitments your office faces at the moment. We would appreciate a response at your earliest convenience.

Yours sincerely,

Edin Omanovic
Advocacy Director

Dear Mr Omanovic

Freedom of Information Request Reference No: 01/FOI/19/002194

I write in connection with your request for information which was received by the Metropolitan Police Service (MPS) on 25th of April 2019. I note you seek access to the following information:

YOUR REQUEST:

Initial Request

"I would like a copy of any data sharing agreements or similar such contracts with FaceWatch (https://scanmail.trustwave.com/?c=7089&d=IlDB3N7RCgE8SD_NXhyjrQvrJiRu6Nhhqi8X3pI67Q&u=https%3a%2f%2fwww%2efacewatch%2eco%2euk%2f)"

Clarification – 10/05/2019

"The time period can be from 1 January 2015 to today's date 10 May 2019.

Clarification – 21/05/2019

"The Information Commissioner's Office describes a data sharing agreement as the following (https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf):

Data sharing agreements – sometimes known as 'data sharing protocols' – set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis. A data sharing agreement should, at least, document the following issues:•the purpose, or purposes, of the sharing;•the potential recipients or types of recipient and the circumstances in which they will have access;•the data to be shared;•data quality – accuracy, relevance, usability etc;•data security;•retention of shared data;•individuals' rights – procedures for dealing with access requests, queries and complaints;•review of effectiveness/termination of the sharing agreement; and•sanctions for failure to comply with the agreement or breaches by individual staff.

So my request can be interpreted to mean any agreement with FaceWatch which "*set[s] out a common set of rules to be adopted by the various organisations involved in a data sharing operation.*". This can include a document is formally called a 'data sharing agreement', but it may also include any document which sets out common rules but is not formally called a 'data sharing agreement'. "

SEARCHES TO LOCATE INFORMATION

To locate the information relevant to your request searches were conducted within the Metropolitan Police Service (MPS).

DECISION

I have written to the Information Sharing Support Unit (ISSU) that acts as the single point of contact for the MPS for information sharing advice generally and the compliance of Data Sharing Agreements (DSA) by business groups. This unit creates and maintains the corporate searchable DSA Registry.

ISSU have informed me that the search within the ISSU file area has failed to retrieve any data sharing agreements with FaceWatch for the requested period.

This notice concludes your request for information. I would like to thank you for your interest in the MPS.

Should you have any further enquiries concerning this matter, please contact me on 0207 161 4029 or via email at collin.hazeley@met.police.uk, quoting the reference number above.

Yours sincerely

Collin Hazeley
Information Manager