GROUNDS OF COMPLAINT TO THE INFORMATION COMMISIONER UNDER SECTION 165 OF THE DATA PROTECTION ACT 2018

LIVE AUTOMATED FACIAL RECOGNITION BY FACEWATCH LTD AND THE SOUTHERN COOPERATIVE LTD

A. Summary

I. Background

1. AWO is instructed by Ms Silkie Carlo (the "complainant") to complain to Information Commissioner's Office (ICO) about infringements by Facewatch Limited ("Facewatch") and The Southern Cooperative Limited ("Southern Co-op") of her data rights on 31 March 2022. AWO is also instructed by the complainant to bring to the Commissioner's attention wider concerns about how Facewatch, Southern Co-op, and other Facewatch clients implement Facewatch's technology, in particular the creation and maintenance of "watchlists" involving the processing with a high degree of risk to data subjects' rights – including under the UK GDPR – for private benefit.

2. Facewatch describes itself and its service as follows[1]:

> *"Facewatch is one of the UK's leading facial recognition companies. Facewatch's cloud-based facial recognition security system safeguards businesses against crime. Our facial recognition technology sends you instant alerts when subjects of interest enter your business premises."*

3. Facewatch's clients include range of well-known retail and grocery providers across the UK, including Southern Co-op, Budgens and Nisa, as well as petrol station forecourts and garden centres[2].

4. The complainant has both a personal and professional interest in this complaint. She is the Director of Big Brother Watch ("BBW"), a non-profit limited company registered in England and Wales. BBW is a non-partisan UK civil liberties campaign group working to protect individuals' privacy. Ms Carlo is an expert in the ethics of digital surveillance.

5. The purpose of this complaint is to seek investigative and corrective action by the ICO to address (i) the infringements on the complainant's data rights, and (ii) unlawful processing of personal data by Facewatch and its clients (including Southern Co-op) that is infringing the data rights of an unknown (but significant) number of other UK data subjects. The complainant asks the ICO take urgent

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

action to protect individuals from this unlawful and unfair processing of their personal data.

II. Summary of complaint

6. Facewatch's system uses novel technology and highly invasive processing of personal data, creating a biometric profile of every visitor to stores where its cameras are installed. It enables retail outlets – including those belonging to Southern Co-op – to create and enforce ad hoc and dynamic blacklists of individuals they wish to exclude from their stores, or otherwise 'intervene' with. In practical terms, an individual can enter a Southern Co-op store and, unknown to them after their visit, be added by a member of staff to a watchlist containing allegations of 'crime or disorder', if that member of staff 'reasonably suspects' them.

7. That individual then becomes a 'subject of interest'. Their biometric profile is used to enable Southern Co-op to share their allegations of criminal conduct between their staff in different stores, and with members of staff of any other Facewatch client, within a certain radius of the first location. Shop staff alerted to Southern Co-op's allegations may then take unspecified action against the individual, e.g. excluding them from a store, asking to search their bag, or leading to confrontations with security staff; all of which happens in public. The 'subject of interest' may never know why this is happening or what they can do about it. They will remain on the watchlist for two years, with no proactive steps by Facewatch to confirm whether Southern Co-op's allegations have been confirmed or disproved by police action.

8. The risks to data subjects' rights and freedoms from this kind of processing are significant. As the Commissioner's own guidance[3] makes clear, the bar for such processing to be lawful is high, and Facewatch and Southern Co-op fail to meet that bar.

9. The complainant was subject to this system. Her personal data was unlawfully processed (and it follows that the personal data of all other individuals entering

[3]https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf The 'ICO LFR Guidance' herein.

Southern Co-op stores where Facewatch's system is used is being unlawfully processed daily):

i. Facewatch and Southern Co-op purport to rely on their legitimate interests for the processing under Article 6 UK GDPR, but the processing is not necessary or proportionate to those interests, and they are overridden by the interests of data subjects.

ii. Facewatch and Southern Co-op purport to rely on conditions exempting their processing from the prohibition in Article 9 UK GDPR (and authorising it under Article 10 UK GDPR), but those conditions are not met because the processing is not necessary for crime prevention, and it is not in the substantial public interest.

iii. Through poor signage, lack of staff training, and incomplete information online, Facewatch and Southern Co-op fail to provide the transparency about the processing required by Articles 5(1)(a) and 13 UK GDPR.

iv. The processing was not within in the complainant's reasonable expectations and was therefore in breach of the principle of fairness in Article 5(1)(a) UK GDPR.

10. Other matters indicate that Facewatch and Southern Co-op's processing of the personal data of other UK data subjects is unlawful:

i. Facewatch and Southern Co-op do not provide the transparency required by Articles 5(1)(a), 13, and 14 UK GDPR to subjects of interest when their data is processed by being added to (and maintained in) watchlists.

ii. There are significant risks of unfair bias in the creation of watchlists and the deployment of Facewatch's system which neither Facewatch nor Southern Co-op appear to mitigate, breaching the fairness principle in Article 5(1)(a) UK GDPR.

iii. There are risks to the accuracy and security of the processing involved in the creation of watchlists and deployment of Facewatch's system, which neither Facewatch nor Southern Co-op appear to mitigate, breaching Articles 5(1)(d) and (f) UK GDPR.

iv. Southern Co-op and Facewatch process more data than is necessary when generating and storing watchlist entries, in breach of the principle of data minimisation (Article 5(1)(c) UK GDPR).

11. Facewatch, Southern Co-op and other Facewatch clients are at the forefront of using new technology to wield significant new power over members of the public as they go about their daily lives. In doing so, they are pushing and exceeding the boundaries of what the law permits. The complainant urges the ICO to act to uphold data subjects' rights.

B. Processing by Facewatch and Southern Co-op

I. Creation and maintenance of the National Watchlist

12. Facewatch maintains a database and/or databases of personal data relating to "individuals reasonably suspected to have committed crime or disorder" (the 'National Watchlist'), whom Facewatch refer to as "subjects of interest (SOIs)".[4] While this complaint adopts this terminology for ease, this should not be interpreted as an acceptance of Facewatch's categorisation of individuals on any of its watchlists as legitimate "subjects of interest" for the purposes of the prevention of crime and disorder.

13. The Watchlist is created and maintained, according to Facewatch, through (i) uploads of images and other information from its business subscribers, including Southern Co-op; (ii) uploads of images and other information from UK police forces with which Facewatch has 'legal agreements'; (iii) downloads of data of publicly available information on police websites; (iv) and downloads of data from a website maintained by Crimestoppers, a non-governmental charity organisation.[5] The Watchlist is composed of entries relating to alleged incidents. Each entry is said to contain at least:

- *"The date of the offence or suspected offence*
- *A picture of the SOI face*

[4] *Subject of Interest Detailed Privacy Notice ('SOI Notice'):* https://www.facewatch.co.uk/wp-content/uploads/2018/09/Subjects-of-Interest-Detailed-Privacy-notice.pdf and Bundle Section B p1; https://www.facewatch.co.uk/privacy/
[5] *SOI Notice* p1

- *The SOI name if known*
- *A short summary of what happened"*[6]

14. Based on how individual client location watchlists are created (see para 7), it can be inferred that each entry also contains a record of the location at which an alleged incident is said to have taken place.

15. Facewatch provides conflicting information about the length of time for which entries are retained, but the *SOI Notice* indicates the period is as long as two years.

16. In its Privacy Notice[7] (herein "the Facewatch Privacy Notice"), Facewatch states that the images of faces on its Watchlist are converted to:

> *"facial recognition algorithm templates which are used to compare to the facial recognition template of people seen on CCTV entering [Facewatch's] Subscribers' premises and create alerts if there is a potential match."*

17. This complaint uses Facewatch's term 'feature vector' to describe these biometric templates. The creation and storage of feature vectors is processing of 'biometric data for the purposes of uniquely identifying a natural person' (Article 9(1) UK GDPR).

18. The Facewatch Privacy Notice states that its subscribers "*appoint users to the system*" who are able to upload incident reports to the National Watchlist. That is, individual members of staff working at the locations of Facewatch's clients (including Southern Co-op's stores) are able to add entries to the National Watchlist that include feature vectors and data on alleged 'crime or disorder' (without this being subject to any apparent meaningful safeguards). The Facewatch User Guide (at page 13, see Bundle Section B) indicates that Facewatch clients can upload reports of incidents that took place at any time in the two years preceding the date on which the report is made.

19. It follows that the creation and maintenance of the National Watchlist involves the processing of personal data under UK GDPR. It also involves the processing of data covered by Articles 9 and 10 UK GDPR:

---

[6] *Ibid*
[7] https://www.facewatch.co.uk/privacy/ and Bundle Section B

i. The creation, storage and use of feature vectors constitutes processing of 'biometric data for the purpose of uniquely identifying a natural person' (Article 9(1) UK GDPR)[8].

ii. The inclusion in incident reports of data on 'crime and disorder' constitutes "Processing of personal data relating to criminal convictions and offences or related security measures" (Article 10 UK GDPR). This remains the case even where incident reports contain only allegations of offences (s.11(2)(a) Data Protection Act 2018 ('DPA')).

20. This processing takes place whenever an employee of Southern Co-op (or any other Facewatch client) creates and uploads an incident report to – or receives an alert from – the National Watchlist. It takes place whenever entries on the National Watchlist are added by way of upload by or download from a police force or Crimestoppers. It continues for as long as the incident report remains on the National Watchlist and concerns an unknown number of UK data subjects who have been added to the National Watchlist.

II. Individual client location watchlists

21. Facewatch also states that it maintains a "*personalised watchlist for every one of [its] customer's properties individually*" based on algorithms that "*estimate where an SOI is most likely to carry out crimes (normally using a geographic radius)*".[9] The Facewatch User Guide Version 1.1[10] indicates that geographic radius is the sole criteria in creating individual client location watchlists:

> *"The Facewatch national watch list of subjects of interest (SOIs) is used to generate alerts proportionately with Facewatch subscribers. When an SOI is reported, Facewatch automatically shares that data proportionately based on the geographic location of the property."*

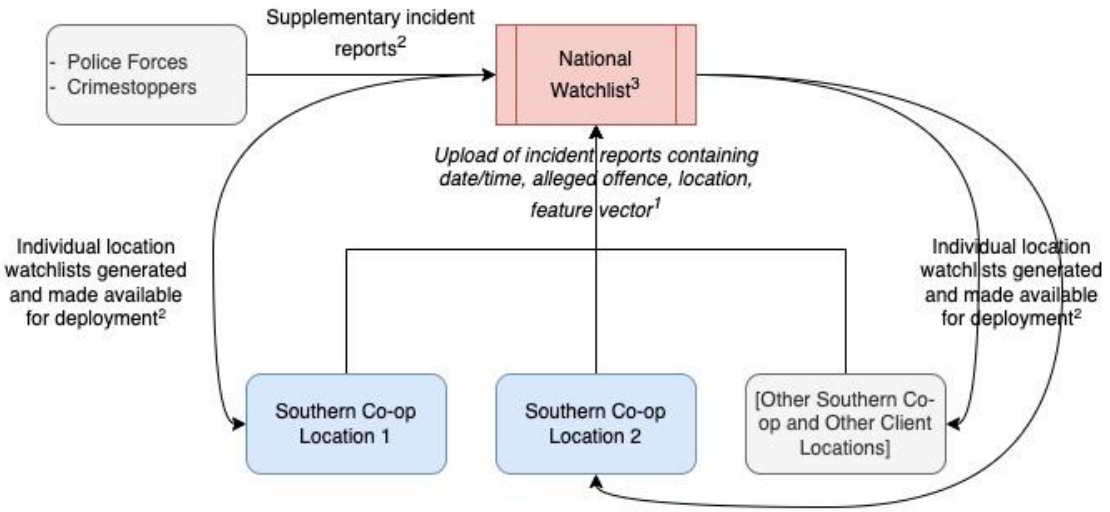
22. For Facewatch client locations in London, the radius is 8 miles. That is, the individual watchlist for a particular location is comprised of every incident report (each of which concerns an individual alleged to have been involved in 'crime or disorder', whose biometric data has been retained) whose location is within an

[8]See also *R (Bridges) v South Wales Police [2020] EWCA Civ 1058 ('Bridges')*
[9]*SOI Notice* p2
[10]See Bundle Section B

8-mile radius of that location. For other location types, the radius is greater, increasing to 46 miles for 'very rural' locations.

23. Figure 1 represents the complainant's understanding of the processing involved in the creation of the National Watchlist and location-specific watchlists, summarising the information in paras 5 to 7.

Figure 1: Creation of national and location-specific watchlists



Acts of Processing
1: Collection and creation of personal data engaging Articles 9 and 10 GDPR
2: Sharing of personal data engaging Articles 9 and 10 GDPR
3: Ongoing storage and other processing (e.g. database maintenance) of personal data engaging Articles 9 and 10 GDPR

III. Facial recognition deployment

24. Facewatch and Southern Co-op deploy live automated facial recognition (LFR) technology at stores across the south of England.[11] The Southern Co-op has had installed CCTV cameras (which the complainant understands to have been provided by Facewatch[12], hereafter 'Facewatch Cameras') at these stores for the purposes of deploying Facewatch's LFR. Facewatch Cameras are positioned so as to capture a facial image of every individual entering the relevant store. From each image of each individual who passes through the store, a feature vector is

[11]As of 2 December 2021, Big Brother Watch discovered that Southern Co-op had deployed Facewatch's facial recognition cameras across 35 Co-op stores in Portsmouth, Bournemouth, Bristol, Brighton and Hove, Chichester, Southampton, West London and West Ewell (https://bigbrotherwatch.org.uk/2021/12/co-op-doubles-orwellian-facial-recognition-cameras-in-supermarkets/)
[12]The User Guide at Bundle Section B indicates at p4 that cameras are installed by Facewatch 'accredited partners', suggesting Facewatch provides the cameras to its clients.

generated.[13] Each feature vector is compared against the feature vector linked with every entry on the location-specific watchlist.[14]

25. A 'match' occurs when Facewatch's system assesses the feature vector of an individual entering a Facewatch client location (person A) to be sufficiently similar to a feature vector for an individual on at least one watchlist entry (person B) as to indicate that person A and person B are the same.

Consequences of no match to the watchlist

26. The Facewatch Privacy Notice states "*If there is no match the data [i.e. the feature vector of an individual entering a Southern Co-op store] is instantly deleted*[15]." It also states that Facewatch retains a copy of the facial images of every individual entering the store at which the Facewatch Camera is installed for potential further biometric processing:

> *"for 72 hours so that images of individuals reasonably suspected of crime or disorder can be uploaded after the event to the Facewatch system."*

27. The situation is different where there is no match – and no alert is sent – but where a feature vector of an individual visiting a Southern Co-op store matches a feature vector on the watchlist to a degree. Per the Facewatch Privacy Notice:

> *"In order to maintain and improve the accuracy of the Facewatch System we retain alerts that are just below our accuracy standard for 48 hours for review."*

Consequences of a match to the watchlist

28. In the case of a match, an alert is sent to employee(s) of Southern Co-op at the relevant store. According to Facewatch's Privacy Notice:

> *"The output of the application is a recommendation in the form of an alert that an image may match that of a subject of interest. Other information provided is the percentage of certainty that the images are a match and a gallery of images held of the subject of interest."*

29. The SOI Notice states that an alert also contains "*a tag for their [i.e. the SOI on the watchlist to whom an individual has been matched] crime types*."

[13]https://www.facewatch.co.uk/privacy/
[14]SOI notice, p2
[15]The SOI Notice states: "No facial recognition data or images are held for more than 10 seconds on our systems unless there is a match", suggesting that feature vectors that do not match a watchlist entry are deleted quickly, rather than 'instantly'.

30. The Facewatch Privacy Notice states that the alert is meant "*to assist a human review by the person receiving the alert who will have sight of the relevant person and be in a position to decide if they consider the match to be accurate*". The SOI Notice states:

> *"The user [i.e. a Southern Co-op employee] receiving the alert can either:*
>
> - *Confirm the alert is correct and take action depending on their company policy (Eg to communicate with or observe the SOI)*
> - *Click an option to say the suggested match is wrong (it is then deleted instantly) or*
> - *if no verification is entered within 1 hour the alert is deleted."*

31. When an alert is received by a Southern Co-op member of staff, it is up to staff within the store as to what action to take. The Facewatch Privacy Notice states:

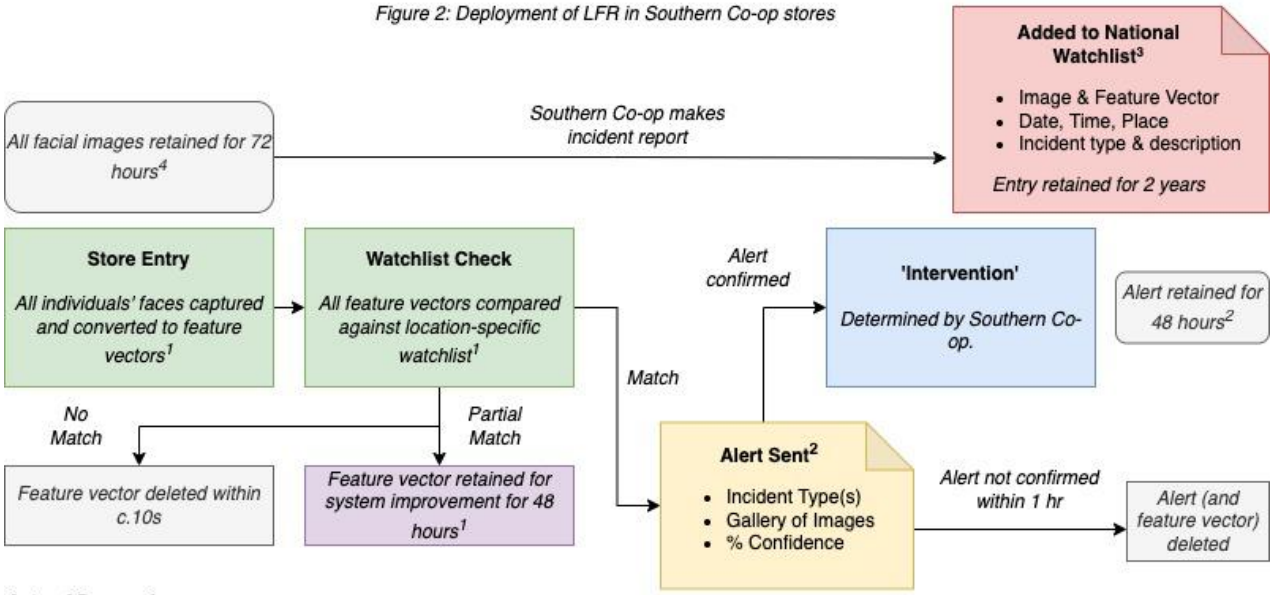
> *"If the person receiving alert considers the alert image matches the person subject of the alert, they will implement their organisational procedure for responding to a matched alert. This action can range from no action to an intervention."*

32. It appears that, at least in some instances, the images and feature vectors collected by Facewatch Cameras may be shared with police or Government agencies. Ostensibly this information is shared via separate, secure, police-owned services for matching against dedicated, police-owned watchlists.[16] However, the nature and extent of this processing cannot be determined from information publicly provided by Facewatch.

[16]Facewatch Information Sharing Agreement V9 170220; Version Specific Information Sharing Agreement V19 04/03/19. See Bundle Section B

33. Figure 2 represents the complainant's understanding of the processing involved in the deployment of Facewatch's LFR in Southern Co-op stores, summarising the information set out in paras 9 to 10.

Figure 2: Deployment of LFR in Southern Co-op stores



Acts of Processing
1: Processing of data engaging Article 9 GDPR
2: Sharing/storing of data engaging Articles 9 and 10 GDPR
3: Collection and creation of personal data engaging Articles 9 and 10 GDPR
4: Storage of personal data

34. It follows that the deployment of Facewatch's LFR technology in Southern Co-op stores involves the processing of personal data under UK GDPR. It also involves the processing of data covered by Articles 9 and 10 UK GDPR:

    i. Every individual entering a Southern Co-op store at which a Facewatch Camera is installed has their biometric data processed when a feature vector is created from their facial image and compared against the location-specific watchlist (Articles 4(14) and 9 UK GDPR). This is the case even if feature vectors are deleted quickly if they are not matched to a watchlist (see *Bridges*).

    ii. Some individuals entering the relevant store who do not match an entry on the watchlist have their biometric data processed for a period of 48 hours in order that Facewatch can review that data to improve its system.

    iii. Existing SOIs entering the relevant store and being matched to the location-specific watchlist have their biometric data and data "relating to [alleged] criminal convictions and offences or related security measures"

(Article 10 UK GDPR and s.11(2)(a) DPA) processed for the generation and sharing of an alert from by Facewatch to Southern Co-op. They also have their data processed in this way when a different individual enters the store, generates a match, but that match is incorrect (i.e. a 'false positive').

iv. Some individuals have their biometric data and data relating to alleged criminal convictions and offences processed when Southern Co-op staff decide to submit an incident report about them to Facewatch's National Watchlist (see para 7 above).

IV. Processing of the complainant's personal data

35. On 31 March 2022, the complainant entered a branch of Southern Co-op on Western Road, Brighton. During that visit:

i. An image including her face was captured by a camera provided by Facewatch and installed by Southern Co-op in that store;

ii. From that image a feature vector was generated.

iii. The feature vector was transmitted by Southern Co-op to Facewatch and compared against the location-specific watchlist for that store. The feature vector did not match any entries on the watchlist.

36. In the 72 hours following that visit, it was open to Southern Co-op staff to upload an incident report relating to the complainant containing allegations of 'crime or disorder', which would have caused a feature vector to be re-generated from her facial image and stored alongside other data (including the allegation of crime or disorder) for a period of two years in the National Watchlist.

37. Facewatch and Southern Co-op have confirmed that the complainant's personal data was processed in this way (see correspondence in Bundle Section C).

V. Controllership

38. Article 26 UK GDPR provides that "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers."

The concept should be interpreted broadly in such a way as to ensure the effective and complete protection of data subjects[17].

39. The complainant is aware of a range of acts of processing, described at paras 5 to 12. Broadly, the acts of processing can be grouped into (i) the **creation of watchlists**, in particular through the creation and upload of incident reports by Southern Co-op (as well as other of Facewatch's clients), and (ii) the **deployment of LFR** in Southern Co-op stores, scanning individuals entering those stores to detect matches to a store's watchlist, and taking action in response to matches.

40. Facewatch and Southern Co-op jointly determine the purposes and means of the processing involved in both the creation of watchlists and the deployment of LFR in Southern Co-op stores:

    i. Facewatch has created and set the broad operating parameters of its LFR system (aspects of the purposes of the processing). It provides and maintains the required software and sets out important aspects of the means of processing in how Southern Co-op uses the system (e.g. by allowing certain data fields to be uploaded in incident reports, and by requiring Co-op staff to make declarations when doing so, see User Guide at Bundle Section B). But within Facewatch's parameters, Co-op has significant latitude in the processing involved in adding incident reports to the National Watchlist. It decides which individuals to upload to the National Watchlist as SOIs, and in what circumstances. It decides what specific information to upload when incident reports are made (e.g. choosing the category of incident and the level of detail with which to describe it)[18]. These matters are also central to the purpose and means of the processing.

    ii. Facewatch provides and maintains the required hardware (Facewatch Cameras) and sets their operating parameters (aspects of the means of processing). But Southern Co-op decides how the hardware will be used,

[17]Case C- 131/12, Google Spain, para. 34.
[18]Facewatch's own terms of use indicate that its clients are joint controllers in respect of the incident reports they make: https://www.facewatch.co.uk/wp-content/uploads/2018/05/Facewatch-User-Terms-of-Use-21-04-18.pdf at 3.2.1

for example where cameras will be installed, and which members of Southern Co-op staff will be permitted to use the Facewatch system (other important aspects of the means of processing).

iii. At deployment, Facewatch, as well as maintaining the National and location-specific watchlists, decides on the circumstances in which match alerts will be sent to Southern Co-op. It also decides what information is provided to Co-op with those alerts, effectively setting an envelope of possible purposes for the processing. But Southern Co-op decides what action is actually taken (if any) in response to alerts, determining the purpose of processing in respect of each data subject affected.

41. The mutual involvement of Facewatch and Southern Co-op in the processing involved in creating watchlists and deploying LFR in stores cannot be disentangled. They jointly determine the purposes and essential means of the processing, and therefore each of Facewatch and Southern Co-op must therefore comply with the responsibilities of controllers set out in the UK GDPR and DPA in respect of both the watchlist and the deployment processing. This complaint sets out the ways in which they fail to do so.

C. Correspondence with the data controllers

42. The complainant submitted subject access requests to each of Facewatch and Southern Co-op on 31 March 2022.

43. Facewatch responded on 1 April 2022, confirming that the complainant's personal data had been processed and providing generic information about the Facewatch system. The complainant asked supplementary questions on 20 April 2022 and received a limited response on 6 May 2022. On 13 May 2022 Facewatch refused to provide copies of key documents referred to and relied upon in its responses to the complainant.

44. Southern Co-op responded on 7 and 14 April 2022 and incorrectly stated that it had not processed the complainant's personal data:

> *"This means unless you have been an offender in the mentioned stores within the last 12 months, our facial recognition technology **will not have processed your data**. We have checked our records and can confirm that you are not*

held in the system as an offender. Therefore, ***none of your personal data has been stored.****" (emphasis added)*

45. Southern Co-op responded to the complainant's supplementary questions on 6 June 2022, contradicting its earlier email and confirming that "[the complainant's] understanding of the processing of [her] personal data is correct", but declined to provide any further information.

46. The result of the complainant's correspondence with the controllers is that she has not been able to satisfy herself that the processing of her data that took place on 31 March 2022 was lawful, fair, or transparent. The correspondence has also failed to allay the complainant's concerns about Facewatch and Southern Co-op's processing of the personal data of large numbers of other data subjects, which she wishes to bring to the Commissioner's attention.

D. Complaint

I. Legal basis for processing under Article 6

47. Processing of personal data must be based on one of the bases in Article 6 UK GDPR (Articles 5(1)(a) and 6 UK GDPR). Facewatch and Southern Co-op state that they rely on Article 6(1)(f), i.e. that their processing is 'necessary for the purposes of the legitimate interests pursued by [them]'[19]. The legitimate interests said to be pursued are:

"to protect our business against criminal activity and to protect the safety of our colleagues, members and customers" (Southern Co-op)

"to provide a service to protect our customers, their customers, staff and business assets from unlawful acts" (Facewatch)

48. The ICO LFR Guidance (at page 32) sets out how the validity of reliance on Article 6(1)(f) for processing can be assessed. Three questions must be addressed[20]:

    i. Is there a legitimate interest behind the processing?

[19]See Facewatch Privacy Notice: "The lawful basis for processing SOI personal data is that it is in our legitimate interest and that of our subscribers to do so." See also p8 of the Southern Co-Op Privacy Notice: https://www.thesouthernco-operative.co.uk/wp-content/uploads/SC-Website-Privacy-Notice.pdf and Bundle Section B

[20]See also *Rigas* C-13/16, 4 May 2017

ii. Is the processing necessary for that purpose?

iii. Is the legitimate interest overridden by the individual's interests, rights, or freedoms?

49. Facewatch's legitimate interests assessment is published as part of the Facewatch Privacy Notice. Southern Co-op has not published any assessment of its legitimate interests. In response to the complainant's requests for information, Southern Co-op stated, without providing further details:

> *"We have undertaken a legitimate interest assessment the result of which was that we can rely on this as our lawful purpose. We do not consider our legitimate interests are overridden by the interests of other data subjects such as your client and the processing is necessary and proportionate in accordance with Article 6 UK GDPR."*[21]

The LFR processing is not necessary

50. The ICO LFR Guidance provides variously:

> *"[LFR] processing will not be necessary if the controller's legitimate purpose could reasonably be achieved by a less restrictive or intrusive approach."*
>
> *"Controllers should not use LFR simply because it is available, it improves efficiency or saves money […] if the deployment of LFR is only likely to be slightly more effective than less privacy-intrusive measures (such as non-biometric measures, e.g. alternative types of surveillance) then it may be unnecessary.*

51. Facewatch and Southern Co-op's LFR processing is not necessary for the interests pursued, taking this guidance into account. Facewatch's legitimate interests assessment assumes that SOIs *must* be apprehended as they enter stores in order to reduce crime:

> *"Without processing information in this way we would be unlikely to effectively identify such persons as they enter subscriber premises"*

52. But apprehending individuals in this way is not the only way to prevent petty crime. The assessment ignores other, less privacy-intrusive approaches to reducing in-store crime, such as increasing the presence of security staff, better training for staff, the wider use of security tags etc. It may be (though it is not

[21] See Bundle Section C

accepted) that Facewatch and Southern Co-op's use of LFR allows them to reduce in-store crime with less investment, but this does not make such intrusive processing necessary.

53. The ICO LFR Guidance underlines this:

> *"Watchlists of individuals suspected of minor offences are less likely to satisfy the key legal tests of necessity and proportionality."*

The LFR processing is not proportionate

54. To assess proportionality, the ICO LFR Guidance requires controllers to consider:

> *"Whether their objective is sufficiently important to justify the processing of biometric data and interference with individuals' privacy"* [22]

55. Placed in the context of the various uses for which LFR has hitherto been deployed in public spaces, Facewatch and Southern Co-op's interests are of, at best, medium importance. They aim at displacing petty crime away from particular stores where Facewatch Cameras are installed, increasing Southern Co-op's profit margins by reducing stock loss. This compares to interests of weightier importance, as indicated in the ICO LFR Guidance:

> *"Controllers' objectives may vary significantly in their importance, from achieving small cost efficiencies or tackling petty crime, to preventing major threats to public safety." (emphasis added)*

56. Where the courts have considered the proportionality of LFR deployments previously, the watchlists used have included, for example individuals already known to the police and whom the police have an operational need to detain[23], underlining the lower relative importance of the interests pursued by the two controllers through a watchlist comprised of individuals suspected by them (but not necessarily by the police) of petty crime.

57. As to the extent of interference with data subjects' rights, the ICO LFR Guidance states that:

[22] See also *Bank Mellat v Her Majesty's Treasury* (No 2) [2013] UKSC 39 [2014] AC 700
[23] See *Bridges,* although other individuals were also included on the police watchlist as part of that deployment.

"where LFR systems are used to collect and analyse biometric data on an automatic and indiscriminate basis, potentially on a mass scale, this could represent a significant privacy intrusion."

58. This is precisely what Facewatch and Southern Co-op's processing does, scanning every visitor to every store at which a Facewatch Camera is installed. The processing is continuous and permanent. Once installed in a store, it will capture every visitor to that store at any time of day permanently. This is significantly more intrusive when compared to the limited-time, targeted deployments of LFR considered in *Bridges.*

59. Thus the processing is privacy-intrusive at significant scale for all store visitors, and highly privacy-intrusive for individuals on watchlists. But in support of an interest of low to medium importance. The intrusion on data subjects' privacy is disproportionate.

Data subjects' interests outweigh those of the controllers

60. The disproportionality of the processing is underlined by its serious impact on data subjects' rights and freedoms. The ICO LFR Guidance requires controllers to consider:

"Whether a fair balance has been struck between the interest of the controller, the rights of the individual and the interests of the community."

61. As well as the risk that non-SOIs will feel distress at having their biometric data indiscriminately processed, SOIs may be denied entry to stores, may be subject to intrusive interventions, or may be brought into dangerous confrontations with security staff. All of these things may happen even when an SOI has never committed an offence (see para 36). Any of these things could have serious consequences for SOIs' lives and personal and social relationships, given that interventions happen in public.

62. Facewatch's legitimate interests assessment considers none of these risks. It does not address the possibility of error, malicious or discriminatory uploads (see paras 25 to 27), or any other misuse of the system by Southern Co-op or any other client. Indeed, without knowing how Southern Co-op (or other clients) will intervene in the case of an alert, it cannot possibly address how its processing might impact data subjects' rights and freedoms. Facewatch effectively washes

its hands of the processing and its consequences once an alert is sent to a client, and therefore it is incapable of balancing data subjects' interests against its own.

63. The impacts on data subjects' rights and freedoms inherent in Facewatch and Southern Co-op's processing are significant and operate at scale. For data subjects on watchlists, they may be very serious. By contrast the interests pursued by Facewatch are purely commercial, reducing loss margins in retail locations. Facewatch and Southern Co-op's legitimate interests are overridden by those of data subjects.

64. The processing does not meet the tests of necessity and proportionality, and Facewatch and Southern Co-op's interests are overridden by those of data subjects. Their reliance on Article 6(1)(f) for their processing is misconceived and they have no legal basis for their processing. Their processing of the complainant's personal data on 31 March 2022 was (and their broader processing of personal data is) unlawful.

II. Exemptions to Articles 9 and 10 UK GDPR

65. The UK GDPR provides:

> *"Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,* ***biometric data*** *for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited [unless one of the conditions in subsection 2 applies]" (emphasis added)*
>
> *"Article 10: Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects."*

66. Facewatch and Southern Co-op must be able to rely on an exemption in Article 9(2) UK GDPR for all of their processing. That is, the exemption must apply in respect of the biometric scanning of every visitor to a store with a Facewatch Camera (not only to the scanning of individuals already on a watchlist). It is irrelevant that such biometric data is only processed briefly where there is no match to a watchlist. They further require an authorisation under Article 10 and

the DPA for the creation of incident reports, maintenance of watchlists, and generation and sharing of alerts.

Reliance on the condition in para 10 Schedule 1 DPA

67. Facewatch states that it relies on the exemption contained in Article 9(2)(g) UK GDPR for its processing of biometric data, i.e. that its processing is:

> *"necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."*

68. Article 9(2)(g) is implemented in England and Wales by s.10(2) DPA, which provides for a number of conditions (listed in Schedule 1 DPA) which, if met, will mean that processing can rely on the exemption. Facewatch relies on the condition in Schedule 1, para 10 DPA (the 'para 10 condition'):

> *"This condition is met if the processing—*
>
> *a) is necessary for the purposes of the prevention or detection of an unlawful act,*
>
> *b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and*
>
> *c) is necessary for reasons of substantial public interest."*

69. Schedule 1, para 5 DPA further provides that, to rely on the para 10 condition, a controller must have an appropriate policy document in place in respect of the processing (as defined in para 39 of that Schedule)[24].

70. Schedule 1 para 36 provides that the para 10 condition can be relied upon to authorise processing engaging Article 10 UK GDPR in member state law, save that such processing need not be necessary for reasons of substantial public

[24]Facewatch have indicated (see Bundle Section C) that they have an appropriate policy document in place, but this has not been made available to the complainant. Southern Co-op has indicated in correspondence that it does not consider Articles 9 or 10 UK GDPR to be relevant to its processing. It is not accepted that either controller has or had a compliant appropriate policy document in place, and the complainant reserves the right to make further submissions on this point.

interest. Facewatch indicates that it relies on Schedule 1 para 36 and the para 10 condition in respect of its processing of data engaging Article 10 UK GDPR[25].

71. Southern Co-op does not state publicly which exemptions it relies upon for its processing engaging Articles 9 and 10 UK GDPR. In correspondence, Southern Co-op stated:

> *"We do not process biometric data and so we consider that our compliance with Articles 9 and 10 GDPR is not relevant."*

72. This is plainly misconceived for two reasons:

    i. Southern Co-op is a joint controller for the processing of the biometric data of every individual visiting one of its stores with a Facewatch Camera installed (as well as of individuals on, and matched to, its location-specific watchlists) for the reasons set out at paras 13 to 14.

    ii. Article 10 UK GDPR relates to the processing of personal data relating to [alleged] criminal offences, not biometric processing. Even were Southern Co-op not a controller in respect of *biometric* processing (which is not accepted), it would still require an exemption from the prohibition in Article 10 UK GDPR because of its controllership of the processing involved in creating and uploading incident reports, and in receiving and acting upon alerts (see paras 6 to 11).

73. The purposes of its processing listed in the Southern Co-op privacy notice closely match those listed in the Facewatch Privacy Notice. To the extent therefore that Southern Co-op (later) purport to rely on the same exemptions as Facewatch, this is addressed in paras 21 to 25.

Processing not necessary for the prevention or detection of unlawful acts

74. Facewatch and Southern Co-op's processing engaging Articles 9 and 10 UK GDPR is not carried out only for the purposes of the prevention and detection of unlawful acts.

75. National Watchlist entries relate to incidents of 'crime or disorder'. The complainant has asked both controllers for a full list of the types of incidents which may lead to an SOI being added to the watchlist. This has been refused.

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

The phrase ‘crime **or** disorder’ however, indicates that the National Watchlist contains at least some entries in respect of conduct which is not unlawful.

76. Marketing material on Facewatch’s site indicates that incident reports can be made in respect of incidents including ‘urban explorer’ and ‘other’[26], as well as ‘verbal abuse’ (Page 13 of the User Guide, Bundle Section B), none of which necessarily constitute unlawful acts, further indicating that some watchlist entries relate to conduct which is not unlawful, merely inconvenient for Southern Co-op and other Facewatch clients.

77. Southern Co-op have stated[27]:

> *“The system alerts our store teams immediately when someone enters their store who has a past record of theft or anti-social behaviour […]* ***including those who have been banned/excluded****” (emphasis added).*

78. This indicates that Southern Co-op and Facewatch carry out processing engaging Articles 9 and 10 as a means of more general access control to stores, not exclusively to prevent or detect unlawful acts.

79. Facewatch also states in its Privacy Notice that it retains feature vectors in order to improve its own service. In such cases it is carrying out biometric processing for a purpose other than the prevention and detection of unlawful acts. No exemption under Articles 9 or 10 applies to such processing and it is unlawful.

80. For the same reasons set out at paras 16 and 16, the processing is not ‘necessary’ because other, less intrusive means of preventing or detecting the unlawful acts are available.

81. In reality, Facewatch and Southern Co-op’s processing is carried out for a range of purposes including general access control to retail sites and improving their own systems. They could also use less intrusive means to achieve their aims. It is not ‘necessary for the purposes of the prevention or detection of unlawful acts’.

Processing not necessary for reasons of substantial public interest

82. Facewatch state[28]:

[26]https://www.facewatch.co.uk/2022/03/24/budgens-buckingham-park-continues-to-praise-facewatch/ at 1:40
[27]https://www.wired.co.uk/article/coop-facial-recognition
[28]https://www.facewatch.co.uk/privacy/facewatch-and-gdpr/

"because Facewatch is processing data on a national level and is demonstrated to reduce/prevent crime in subscriber properties with the further potential to prevent and detect crime it is in the Substantial Public Interest.".

83. That is, Facewatch argue that their pooling of watchlist entries from clients across the UK, and making that pool available between clients transforms a private interest – reducing store crime and loss margins for an individual business – into a substantial public one. This is misconceived.

84. The ICO LFR Guidance indicates the types of processing which are and are not likely to meet the 'substantial public interest test:

85. *"Controllers should not use LFR simply because it is available, it improves efficiency or saves money."*

86. *"Controllers' objectives may vary significantly in their importance, from achieving small cost efficiencies or tackling petty crime, to preventing major threats to public safety."*

87. Separately, the ICO has stated[29]:

"The public interest covers a wide range of values and principles relating to the public good, or what is in the best interests of society. ***Commercial or private interests are not the same as a public interest*** *[…]*

Substantial public interest means the public interest needs to be real and of substance. Given the inherent risks of special category data, ***it is not enough to make a vague or generic public interest argument*** *– you should be able to make* ***specific arguments about the concrete wider benefits of your processing****. For example, you may wish to consider how your processing benefits the public in terms of both depth (ie the amount of benefit experienced from the processing, even if by a small number of people) and breadth (the volume of people benefiting from the processing)." (emphasis added)*

88. Facewatch has published no evidence (and refused to provide any to the complainant) of the national crime-reducing impact of its processing. It states only that its system has the 'further potential to prevent and detect crime'. The complainant can only infer that it is unable to make 'specific arguments' about the 'concrete wider benefits' of its processing.

[29]https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions/#substantial3

89. The characterisation of Facewatch and Southern Co-op's processing as reducing crime in a way that benefits the public interest is misleading. The deployment of Facewatch's LFR technology in certain stores does not reduce crime at a national level. It does not bring serious criminals to justice or prevent serious crime (e.g. terrorism) from taking place. It does not protect the public from harm in any meaningful way. At best, it displaces crime, empowering individual businesses to keep 'undesirables' out of their stores and move them elsewhere, protecting Facewatch's clients' profit margins. This is the very definition of a private, not a public interest, let alone a 'substantial public interest'.

90. Southern Co-op as a joint controller of processing engaging Article 9 must also meet the substantial public interest test in order to rely on the para 10 condition. Facewatch relies on the (unsubstantiated) argument that it is reducing crime at a national level, thus meeting the 'substantial public interest' element of the para 10 condition. Southern Co-op is even less able to satisfy this part of the condition, as it is only carrying out this processing in order to protect its own business. Facewatch themselves state[30]:

> *"In order for this processing to be in the substantial public interest there must be a much wider benefit derived from that processing beyond an individual business, site or premises."*

Processing could be carried out with consent of data subjects

91. Processing will only satisfy the para 10 condition if it 'must be carried out without the consent of the data subject so as not to prejudice [the purposes of preventing and detecting unlawful acts]'. The deployment phase of Facewatch and Southern Co-op's processing could be carried out with data subjects' consent without prejudicing their crime prevention purposes. If each person entering a Southern Co-op store were asked for their consent to biometric processing, they could either:

    i. Consent and enter the store; Facewatch's system would then work in the usual way; or

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

ii. Refuse consent and enter the store, in which case Southern Co-op would be free to treat the individual as if they were an SOI, providing the same level of protection for Southern Co-op against 'crime or disorder'.

92. In either case, obtaining consent would not prejudice the purposes of preventing or detecting unlawful acts.

93. None of the three limbs of the para 10 condition are met by Facewatch and Southern Co-op's processing. Their reliance on the exemption in Articles 9(2)(g) and 10 UK GDPR, as implemented in Schedule 1, paras 10 and 36 DPA is misconceived[31] and they have no valid exemption to the general prohibition in Articles 9, or authorisation under Article 10 UK GDPR. Their processing of the complainant's personal biometric data on 31 March 2022 was (and their broader processing of biometric data and alleged offence data is) unlawful.

III. Fairness

94. Processing of personal data must be fair (Article 5(1)(a) UK GDPR). Fairness in the processing of personal data is a broad concept. The ICO has stated that it includes a requirement that controllers:

> *"only handle people's data in ways they would reasonably expect, or can justify any unexpected processing; and have considered how the processing may affect the individuals and can justify any adverse impact."*[32]

95. The ICO LFR Guidance identifies ways in which the use of LFR may breach the requirement for fair processing:

> *"If an LFR system is not sufficiently technically effective and statistically accurate, it may lead to adverse impacts and unfair outcomes. LFR systems may also work less effectively for people from different demographic groups. This could potentially lead to unfairness in the form of discrimination and bias."*

96. A number of these issues are evident in relation to Facewatch and Southern Co-op's processing.

[31]Whilst the failure to meet the substantial public interest limb of the para 10 condition applies only to the controllers' processing of biometric data, the other reasons why the para 10 condition is not met apply equally to their processing of data on alleged offences.
[32]https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

Unfair bias in watchlist creation

97. The National Watchlist is composed of voluntary uploads by members of staff of Southern Co-op and other Facewatch clients. An incident report requires that a Southern Co-op staff member (i) becomes aware of the relevant incident, and (ii) decides that an individual ought to be added as an SOI. This reliance on individual judgment of relatively untrained store staff creates a significant risk that uploads will be biased on the basis of stereotyping – whether or not conscious – against groups with protected characteristics[33] such as age or ethnicity. For example:

    i. Store staff may be more alert in the presence of individuals from certain groups, and therefore more likely to become aware of an incident capable of leading to an incident report.

    ii. Store staff may stereotype individuals with protected characteristics as being more likely to commit theft, interpreting evidence (e.g. CCTV) that would be inconclusive for one person, as conclusive 'proof' of theft for another.

    iii. Store staff may additionally or alternatively perceive conduct by individuals with certain protected characteristic as more 'threatening' or 'abusive'. This risk is greatly increased given that the criteria for inclusion on a watchlist include reasonable suspicion of "disorder", an undefined and subjective term. [34].

98. Without safeguards, such as (i) training of Southern Co-op staff, and (ii) monitoring of additions to the watchlist for protected characteristics bias, such bias could lead to individuals with protected characteristics being overly represented in the National Watchlist and disproportionately likely to be matched by Facewatch's system and subject to interventions. This may be compounded where store staff are more likely to intervene – or intervene more aggressively –

[33]Within the meaning of the Equality Act 2010

[34]As to sub-paragraphs (ii) and (iii) see e.g. https://www.theguardian.com/uk-news/2018/dec/02/revealed-the-stark-evidence-of-everyday-racial-bias-in-britain in which 38% of black people reported being treated as a shoplifter without cause, compared to 14% of white people. See also https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/stop-and-search/latest showing that black people are stopped and searched at a rate 5 times that of white people. See also https://www.apa.org/news/press/releases/2017/03/black-men-threatening

in response to matches involving individuals from those same groups. This would be inherently unfair.

99. Neither controller addresses these risks publicly. The complainant has asked both controllers about the composition of the National Watchlist and the training in place for Southern Co-op staff. Facewatch has not responded, and Southern Co-op stated in correspondence, without further explanation:

> *"We do not consider there is unfair bias. Individuals are treated fairly in line with Article 5(1)."*

Unfair bias in the level of feature vector matching accuracy

100. There are widely documented issues with differential rates of accuracy in feature matching between groups with protected characteristics (see the extensive evidence compiled by the Commissioner at page 21 of the ICO LFR Guidance). There is a significant risk that non-SOIs with certain protected characteristics will be the subject(s) of a disproportionate number of 'false positive' matches, alerts, and interventions. This would be inherently unfair.

101. The complainant has requested information from Facewatch on any differential accuracy rates between groups with protected characteristics, but it declined to respond. It is notable, however, that Facewatch does not address these issues in its legitimate interests assessment or anywhere else publicly. The complainant can only speculate as to whether:

    i. Facewatch has no access to the underlying data used to train the LFR technology it uses; or

    ii. Facewatch is not in a position to audit false positives and false negatives on its LFR system for bias.

102. Facewatch have refused to answer the complainant's questions about the risk of bias in their processing. Southern Co-op appear have stated in correspondence, without further explanation:

> *"We have satisfied ourselves that there are no risks as to the accuracy and security through our governance processes."*

103. Without evidence of how the demonstrated risks of unfair bias in watchlist creation and LFR deployment are mitigated, there are good reasons to believe

Facewatch and Southern Co-op's processing is biased, unfair and therefore unlawful.

General accuracy of feature vector matching

104. The lack of evidence of the general accuracy of Facewatch's feature vector matching (as opposed to differential accuracy between groups), and why this is sufficient in the circumstances – see paras 39 to 40, also suggests that Facewatch and Southern Co-op's processing is not fair[35].

Processing is not within data subjects' reasonable expectations

105. Fairness requires that controllers 'only handle people's data in ways they would reasonably expect'. Facewatch and Southern Co-op's processing is very novel and unlikely to be within the reasonable expectations of the large number of data subjects it affects.

106. Southern Co-op have stated in correspondence:

> *"We have adequate signage and so people would therefore reasonably expect their facial image to be processed in accordance with the facial recognition system in the way that it is. There is nothing unusual about it."*

107. Aside from the fact that it is plainly wrong that there is 'nothing unusual' about this novel use of new technology in retail stores, this misunderstands the principle of fairness which requires that *all* of the processing and its potential consequences should be within data subjects' reasonable expectations. Merely making data subjects aware that the technology is used in some way cannot make it fair; the connection of that use with the creation of watchlists, and the possibilities for interventions in the case of an alert, must also be within data subjects' reasonable expectations.

108. Even with the limited information provided in-store and online (see section 29 on transparency below), a data subject being scanned on entry to a Southern Co-op store is highly unlikely to expect that, at the option of a member of Southern Co-op staff, they might be immediately added to a watchlist containing allegations of criminal conduct, which may result in them being refused entry or confronted by security staff in an unknown number of retail locations (whether or

[35]See ICO LFR Guidance, Section 4.6

not belonging to Southern Co-op) within a radius of up to 43 miles. Much less that this could continue for two years from the date of their visit. Even a motivated and privacy-conscious data subject would struggle to reach this understanding using the information on Facewatch and Southern Co-op's websites.

109. Other aspects of the processing fall outside of data subjects' reasonable expectations, including that in near-match cases, Facewatch uses biometric processing to improve its own system. Data subjects might (although it is not accepted) expect biometric processing to be used in stores to identify proven criminals. They are unlikely to reasonably expect that their biometric data will be used by Facewatch to progressively increase the accuracy of its facial recognition system, improve its profits, and extend the power that it and its clients wield over members of the public.

110. Facewatch and Southern Co-op's processing is not within data subjects' reasonable expectations. It was not within the complainant's reasonable expectations, and the processing of her personal data on 31 March 2022 was therefore unfair and unlawful.

IV. Transparency

111. Processing of personal data must be transparent (Article 5(1)(a) UK GDPR). The ICO LFR Guidance states that this means:

> *"Controllers must provide clear information to data subjects about when, where and why they are using LFR."*

112. Facewatch and Southern Co-op have transparency obligations to all individuals entering Southern Co-op stores who have their data processed to detect possible matches. They also have an obligation to be transparent to SOIs about the fact of their data being processed through the National Watchlist and alerts sent to Facewatch clients.

113. The Information Commissioner has stated[36] that transparency is "fundamentally linked to fairness", which is about being "clear, open and honest with people from the start about who you are, and how and why you use their personal data."

[36]https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

114. What transparency requires is context specific. It depends on the risk of harm to data subjects from the processing, the sensitivity of the personal data, and the intrusiveness of the processing. Facewatch and Southern Co-op's processing is highly intrusive, involves sensitive data, and creates real risks for data subjects. It requires a high degree of transparency.

Lack of transparency during deployment

115. The ICO LFR Guidance indicates how controllers should use signage to comply with the principle of transparency during deployments of LFR:

> *"Controllers should consider more extensive and effective measures to ensure that the public understands how their data is being processed. This should include prominent signage [at deployment sites], clearly visible and accessible to members of the public, explaining:*
>
> - *that LFR is in use and for what purposes;*
> - *that biometric data is being processed; and*
> - *how people can access more information and exercise their data protection rights.*

116. There is signage at the store that the complainant visited (see Bundle Section B). In correspondence with the complainant, Southern Co-op relies on the existence of this signage:

> *"We consider we have appropriate signage in place […] your client was made aware of our use of facial recognition technology by the notices in the store she visited on 31."*

117. As the ICO LFR Guidance makes clear, the mere use of signage alone will not make LFR processing compliant with the principle of transparency. It is not enough for data subjects to be 'made aware of [the] use of facial recognition technology'. The signage must meet a range of criteria. Southern Co-op's signage fails to meet these criteria. It does not cover important matters, including:

    i. That biometric processing (explicitly stated) is taking place;

    ii. How feature vectors are compared to a watchlist, or indeed that a watchlist is in use at all;

iii. The purpose of the processing: i.e. that it is intended to enable Southern Co-op to take action against individuals if they are matched to a watchlist;

iv. What action might be taken by Southern Co-op (or, following Southern-Co-op adding an individual to a watchlist, by the owner of any other store within the relevant radius) in the case of a match; or

v. That an individual's biometric profile (and information on alleged offences) might be added to a watchlist during or in the 72 hours after their visit.

118. Some (but not all) of this information is available via the link included in the signage. No further useful information is available in Southern Co-op's Privacy Notice. In correspondence, Southern Co-op stated that an alert leads to "*positive customer services towards the individual and/or aisle presence".* Such vague language only compounds the lack of transparency about key aspects of the potential consequences of the controllers' processing.

119. In any event it is not reasonable to expect data subjects to consult this information given the everyday context of the technology's deployment. Provision of information on these crucial matters in this way does not comply with the principle of transparency, not least because data subjects are not provided with information on the purposes of the processing as required by Article 13(1)(c) UK GDPR.

120. Other basic transparency information – such as the exemption relied upon by Southern Co-op for the processing of personal data engaging Articles 9 and 10 UK GDPR, is not available to data subjects anywhere, despite information on the legal basis for the processing being required by Article 13(1)(c) UK GDPR.

121. The ICO LFR Guidance also states:

Controllers should consider supplementing this signage by:

- *using leaflets, digital techniques (eg QR codes) and other local media, in advance where possible;*
- *making trained staff available to provide advice and answer questions […]"*

122. Neither Facewatch nor Southern Co-op do this. The complainant sought further information about the processing of her personal data during her visit on 31

March 2022 from in-store staff, but it was not forthcoming. Staff appeared to lack training in explaining the LFR system or basic privacy concepts. In correspondence, Southern Co-op claim that

> *"[S]tore colleagues are instructed to put customers in touch with our Customer Services Team who with the support of our Data Protection Team are better placed to answer any queries."*

123. The complainant can only observe that this training, if it does take place, is ineffective since – as is accepted by Southern Co-op – this process was not followed during her visit.

124. The result is that during deployment, a combination of ineffective signage, online information, and poorly trained staff constitute a failure to provide the information required by Article 13 UK GDPR to data subjects, and a breach of the principle of transparency in Article 5(1)(a) UK GDPR.

No information on the consequences of processing

125. Transparency means that data subjects should meaningfully understand how their data is being processed. This processing involves potentially very serious consequences for data subjects; transparency required that the possible consequences of the controllers' processing of the complainant's personal data were explained at the time they collected it. But no such information was provided to the complainant. Indeed, meaningful information on the consequences of the processing that Facewatch and Southern Co-op carry out is not available to any data subject, because they cannot know:

    i. In what circumstances they might be added to the National Watchlist. The Southern Co-op Privacy Notice states only that crime information may be processed 'in certain circumstances'. The Facewatch Privacy Notice uses the vague language of 'crime or disorder'.

    ii. If they are added to the National Watchlist, where else they might be identified by Facewatch's system, as there is no comprehensive list of locations of Facewatch Cameras available to data subjects.

    iii. The consequences of being matched and the subject of an alert, as neither Facewatch nor Southern Co-op explain what action is taken against SOIs who are matched by Facewatch's LFR system.

126. The lack of information provided to data subjects when Facewatch and Southern Co-op collect and process their personal data makes it impossible for them to anticipate the very serious potential consequences of that processing, preventing them from making informed decisions. This is contrary to the principle of transparency and Article 13 UK GDPR.

Retrospective incident reports

127. Facewatch permits its clients to make incident reports (which must include the creation of feature vectors) that relate to incidents taking place up to two years prior to the date of upload[37]. Since the feed of facial images from Facewatch Cameras is only retained for 72 hours, it can be inferred that this must be possible by creating feature vectors from existing images or CCTV that a Facewatch client has retained. This would include footage or images captured prior to the installation of Facewatch Cameras and any signage. On signing up to Facewatch, its clients therefore avail themselves of the opportunity to process biometric data and alleged offence data about any visitor to their store in the previous two years. Such visitors will not have been provided with even the limited transparency information afforded by the deficient Facewatch signage, which would not have been in place during their visit, constituting an even more serious breach of the principle of transparency in Article 5(1)(a) UK GDPR.

Lack of transparency for Subjects of Interest

128. Facewatch's description of its service (see User Guide, Bundle Section B) indicates that SOIs are not informed at the point they are added to the National Watchlist (for example in that SOIs are envisaged as being added after their visit to the relevant location). They are therefore not provided with the information to which they are entitled under Article 13 UK GDPR – in respect of the watchlist processing specifically – despite the fact that the relevant personal data has been collected from them[38]. The complainant has asked Southern Co-op if they inform SOIs when they are added to the watchlist (or at any later point) but no response was provided. Practically speaking, it would seem to be impossible for Southern

[37]Facewatch User Guide, Bundle Section B
[38]The European Data Protection Board has confirmed that persona data collected through observation (e.g. using cameras) is collected from data subjects' within the meaning of Article 13: https://ec.europa.eu/newsroom/article29/redirection/document/51025 p14

Co-op to notify individuals at the point of their entry onto the watchlist, as it is difficult to imagine this taking place whilst the individual is still in the store, and it is not clear how store staff would reach an individual at a later point.

129. In the *SOI Notice*, Facewatch invites SOIs to contact them if it comes to their notice that they may be on the National Watchlist.

> *"If you feel that you are on our system and you shouldn't be, please do not hesitate to contact us."*

130. This makes SOIs personally responsible for finding out crucial information about hidden processing by Facewatch and Southern Co-op that may be having a major detrimental effect on their daily lives. Attempting to put the onus on individual data subjects to take such steps in the context of this processing is to reverse the obligations imposed on controllers by the UK GDPR.

131. Any exemption to the obligation to provide this information to SOIs can only be relied upon by Facewatch and Southern Co-op to the extent that complying with transparency obligations would be 'likely to prejudice' the prevention or detection of crime (Schedule 2 Para 2(1)(a) DPA[39]). Providing transparency to SOIs would not prejudice the prevention or detection of crime, because there is no way for individuals to modify their behaviour in response to the transparency in a way that undermines Facewatch's system. The most an SOI might practically do in response to being made aware of the full extent of Facewatch and Southern Co-op's processing is refuse to enter a store where a Facewatch Camera is installed; their crime prevention and detection objectives would be unaffected by this[40]. Neither Facewatch[41] nor Southern Co-op indicate that they rely on any exemptions to transparency obligations under the UK GDPR.

132. It follows that the processing of the complainant's personal data on 31 March 2022 was not transparent. Information required to be provided to her under the UK GDPR was not provided or available, and the envisaged consequences of the profiling to which she was subject were (and remain) unclear. Facewatch and

[39]The other elements of Schedule 2 Para 2(1) are not relevant, as Facewatch's system does not assist in the apprehension or prosecution of offenders, or the assessment or collection of taxes.
[40]Note that Facewatch's system is said to be effective even when an individual is wearing a face mask: https://www.facewatch.co.uk/2021/02/15/standing-up-for-retail-workers/
[41]https://www.facewatch.co.uk/privacy/facewatch-and-gdpr/

Southern Co-op did not comply with the ICO's guidance on LFR transparency. The processing of the complainant's personal data was therefore unlawful.

133. For the same reasons, and in addition because transparency information is not provided to SOIs, Facewatch and Southern Co-op's broader processing of other individuals' personal data is insufficiently transparent and therefore unlawful.

V. Accuracy and security of processing

134. Articles 5(1)(d) and (f) UK GDPR states that personal data shall be:

> *"accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."*
>
> *[and]*
>
> *''processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing […] using appropriate technical or organisational measures"*

135. Facewatch and Southern Co-op's use of LFR and maintenance of watchlists entails a range of risks to accuracy and security of processing that do not appear to be appropriately managed.

Risk of inaccuracy in uploads to the National Watchlist

136. The consequences of being on the National Watchlist are potentially extremely serious. Even if (which is not accepted) the use of the Watchlist is legitimate, it must be held to the highest standard of accuracy. 'Every reasonable step' within the meaning of 5(1)(d) will be a very high bar, 'having regard to the purposes' of this processing, which is to maintain a privately held biometric register of alleged criminals. In relation to LFR watchlists, the ICO LFR Guidance states:

> *"The Commissioner expects controllers to […] include only images that are lawfully acquired and accurate, ensuring that they understand their provenance." (emphasis added)*

137. For Facewatch and Southern Co-op's watchlists, 'accurate' would imply either:

i. That any individual on the watchlist has indeed committed the offence of which the watchlist entry accuses them[42]; or, at the very least

ii. Extensive safeguards to keep inaccurate accusations on watchlists to an absolute minimum.

138. But Facewatch's National Watchlist operates on the basis of 'reasonable suspicion' and voluntary uploads by members of staff of Southern Co-op and other clients. What Facewatch describe as a database of 'habitual offenders'[43] is, in reality, a database of allegations and suspicions of its clients' staff, many of which will be unfounded and unproven. This creates multiple potential points of failure which may introduce inaccuracy into the National Watchlist:

i. Inadequate training of Southern Co-op staff, leaving them unclear on the evidential thresholds that must be met to justify an incident report (or the type of incident that can be reported).

ii. Mistaken uploads, or incident reports for which there is insufficient evidence – even if the member of Southern Co-op staff has what they feel is a 'reasonable suspicion'.

iii. Malicious and discriminatory (see paras 25 to 27) uploads.

Lack of safeguards from the controllers to ensure watchlist accuracy

139. According to the Facewatch Privacy Notice:

> *"Subscribers upload information about an SOI only when that individual is reasonably suspected of crime or disorder – this is strictly controlled and anyone who uploads any data which is not compliant could be subject to fines or censure by the ICO."*

140. In fact, uploads to the watchlist appear far from 'strictly controlled'. The fact that the ICO might take regulatory action in the case of an inaccurate or malicious incident report is not a safeguard of accurate and lawful processing. A real safeguard is something built into the system which obviates the need for the ICO to take regulatory action.

[42]Though it is not accepted that the commission of an offence, even if proven, does justify the processing of an individual's personal data by Facewatch and Southern Co-op in the way described in this Complaint.
[43]https://www.facewatch.co.uk/2021/02/15/standing-up-for-retail-workers/

141. The high standard of accuracy to which the National Watchlist must be held, would appear to require Facewatch to implement technical and organisational measures such as:

    i. Auditing its clients' policies, training, and practices;

    ii. Only allowing incident reports onto the National Watchlist once they have been checked by a trained, senior member of staff (either at Facewatch or its client);

    iii. Spot-checking incident reports to detect and manage mistaken and malicious uploads; and/or

    iv. Proactively availing itself of information which might indicate that an SOI is not in fact guilty of an offence.

142. The complainant has asked for details of any such steps taken by Facewatch, but none have been forthcoming (see Bundle Section C). The Facewatch Privacy Notice states:

    "Findings of no crime, not guilty or cessation of proceedings will lead to removal of that incident record against the SOI."

143. However, in their email dated 13 May, Facewatch stated "We do not monitor or hold information pertaining to police reporting." Thus Facewatch appears to take no proactive steps to find out if an SOI falls into any of the following categories, each of which should, according to their own privacy notice, result in removal from the watchlist:

    i. Individuals against whom the police decide to take no further action;

    ii. Individuals who are charged but whose prosecution is dropped; and/or

    iii. Individuals who are charged, tried, and acquitted.

144. Facewatch appears to rely on its clients to make these investigations. Its Model Purpose Specific Information Sharing Agreement (see Bundle Section B) states:

    "Business Subscribers may also report SOI's to the Police and they should monitor their progress through the judicial system […]"

145. The complainant asked Southern Co-op if it takes these steps, but no response was provided. Indeed, there is an air of unreality to the idea that Southern Co-op

or any other Facewatch subscriber could make these investigations, as there is no comprehensive database of individuals who have been acquitted, much less one comprising individuals against whom no further action is taken by police. The Complainant can only assume that no meaningful steps are taken by Southern Co-op to 'monitor [SOIs'] progress through the judicial system'.

146. Even if, for a subset of SOIs, there is the (albeit theoretical at best) prospect of being removed from the Watchlist based on the outcome (or lack of an outcome) of a police investigation, there will presumably be many SOIs whose incidents are never reported to the police by Southern Co-op[44]. For these SOIs, allegations of criminal conduct will remain associated with their biometric image on Facewatch's National Watchlist for two years on the basis of nothing more than the suspicion of a member of Southern Co-op staff.

147. The complainant asked Southern Co-op what training or guidance they provide, or what quality control mechanisms they have in place to prevent inaccurate uploads, but no details were provided.

Unauthorised disclosure of sensitive personal data during deployment

148. There are a number of ways in which an unauthorised disclosure of an SOI's status on the National Watchlist might be made during deployment by Southern Co-op, given that alerts and interventions take place in public areas with large numbers of members of the public present:

    i. Depending on how devices are used in store, a member of the public (or an unauthorised Southern Co-op staff member) could inadvertently see an alert about an SOI and its details.

    ii. During an intervention, a Southern Co-op staff member might reveal or indicate that they are taking action because the SOI is on the National Watchlist.

    iii. A member of Southern Co-op staff might maliciously reveal that an individual (someone known to them, for example) is on the National Watchlist.

[44]The complainant asked Southern Co-op if they always report the addition of an SOI to the watchlist to the police, but they declined to answer.

149. Members of the public or unauthorised members of Southern Co-op staff will not know how the Facewatch system works. They may well infer from such unauthorised disclosure that the SOI is on a police-maintained watchlist; perhaps that they are wanted by the police for serious criminal offences. The risks to data subjects of such unauthorised disclosure cannot be overstated. Despite being asked, Southern Co-op have provided no information on the training, policies, or procedures they have in place to prevent this type of security breach.

No justification of the rate of accuracy in feature vector matching

150. The ICO LFR Guidance elaborates how the UK GDPR requirement for processing to be accurate applies to the accuracy of feature vector matching:

> *"Controllers should make sure the [LFR] system is sufficiently statistically accurate for their purposes. An incorrect match may have an adverse impact on the individual.* ***The greater potential detriment an inaccurate result could have on individuals, the more important it is that controllers' systems are statistically accurate****." (emphasis added)*

151. Facewatch and Southern Co-op's processing is a clear example in which there is great 'potential detriment' in the case of inaccurate results. The ICO LFR Guidance lists some, which are directly relevant to this complaint:

> *"[Inaccurate feature vector matching] could lead to interventions such as additional surveillance, removal from the premises, or even being referred to and potentially detained by law enforcement authorities."*

152. Thus, even if (which is not accepted) the use by Facewatch and Southern Co-op of LFR is legitimate, the level of accuracy in feature vector matching must be (i) very high, and (ii) clearly justified by reference to the specific risks inherent in the processing.

153. Facewatch make a number of vague statements about the technical accuracy of their feature vector matching:

> *"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." (SOI Notice)*

> *"We do not send alerts to subscribers that do not meet our high accuracy standards." (Facewatch Privacy notice)*

"We use NIST tested top performing software for accuracy to ensure accurate operation of the system." (Facewatch Email, Bundle Section C)

154. Despite these claims, Facewatch offer no information publicly on how accuracy in feature vector matching is assessed or improved. The complainant has sought from Facewatch and Southern Co-op, but has not been provided with, specific information on the accuracy (i.e. rates of false positives and false negatives) of feature vector matching[45], nor any justification from Facewatch or Southern Co-op as to why the processing is sufficiently accurate in light of the very serious risks it entails.

155. Facewatch and Southern Co-op have refused to answer the complainant's questions about how they ensure accuracy and security of this high-risk processing. **Without evidence about how the demonstrated risks to accuracy and security are managed by Facewatch and Southern Co-op, there are good reasons to believe that their processing is not accurate or secure as required by the UK GDPR, and is therefore unlawful.**

VI. Breach of the principle of data minimisation

156. Article 5(1)(c) UK GDPR provides that personal data shall be:

"limited to what is necessary in relation to the purposes for which they are processed."

157. Facewatch's clients are encouraged to add 'as much information as possible' in incident reports[46]. There is no indication of why this additional information is needed. Indeed it cannot be necessary, since an alert only includes the type of incident, without further details. **The collection and further processing of this additional information, which is not necessary for the purposes of the processing, is in breach of the principle of data minimisation and is unlawful.**

VII. Data Protection Impact Assessments

158. Article 35 UK GDPR requires:

[45]Southern Co-op state simply in correspondence: "We have satisfied ourselves that there are no risks as to the accuracy and security through our governance processes."
[46]Facewatch User Guide, Bundle Section B

"(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

(2) The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

(3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of […] (c) a systematic monitoring of a publicly accessible area on a large scale." (emphasis added)

159. Both Facewatch and Southern Co-op, as joint controllers, should have data protection impact assessments (DPIAs) in place for their LFR deployments. Facewatch indicated in correspondence with the complainant that it has a DPIA in place. Southern Co-op has not confirmed whether or not it has. Per Article 35(7) UK GDPR, each controller's DPIA should contain 'at least':

"(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."

160. This complaint details considerations relevant to proportionality, a number of risks to rights and freedoms of data subjects, and safeguards that would need to be in place for the controllers' processing to manage those risks, were the processing proportionate (which is not accepted).

161. The ICO has stated[47]:

> *"You need to keep your DPIA under review. You may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing."*

162. In the context of Facewatch and Southern Co-op's processing this would include, at a minimum, ongoing or periodic monitoring of the extent to which the risks outlined in paras 25 to 29, and 35 to 35 are materialising, for example by:

    i. Reviewing the composition of watchlists (both location-specific and National) to assess whether individuals from certain groups are over- or under-represented.

    ii. Auditing the incidence of false positive and false negative LFR match outcomes to assess whether there are differential accuracy rates between relevant groups.

    iii. Auditing the number, quality, and results of interventions made following matches, to assess whether individuals from relevant groups are treated fairly.

163. Contrary to ICO Guidance,[48] neither Facewatch nor Southern Co-op have published any DPIAs covering their processing. Neither has provided a DPIA to the complainant. The complainant therefore does not know whether DPIAs (if they are in place), address the clear risks to rights and freedoms identified in this complaint, or whether the controllers take the required steps to keep those risks under periodic review. **If they do not, however, the controllers' processing is likely to be in breach of Article 35 UK GDPR and is unlikely to be lawful under Article 5(1)(a) UK GDPR**, and the complainant reserves the right to make submissions on this point.

E. <u>Requests to the Information Commissioner</u>

164. The Information Commissioner's Draft Regulatory Action Policy[49] ('RAP') sets out a number of aggravating factors to be taken into account when considering

[47]https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how12
[48]*Ibid*: "To aid transparency and accountability, it is good practice to publish your DPIA."
[49]https://ico.org.uk/media/about-the-ico/consultations/4019400/regulatory-action-policy-2021_for-consultation.pdf

whether and how to use the Commissioner's powers. A number of those aggravating factors apply to Facewatch and Southern Co-op's unlawful processing of personal data, underlining the urgency and importance of remedial action by the Commissioner:

i. **"the attitude and conduct of the person or organisation concerned suggests an […] an unlawful business or operating model":** Facewatch is a facial recognition technology company. Its sole service is the processing of biometric and (alleged) offence data; its business model is based on high-risk and – as this complaint highlights – unlawful processing of personal data.

ii. **"the data protection legislation breaches […] affected many people":** the number of individuals on Facewatch's National Watchlist is unknown. But Facewatch and Southern Co-op's unlawful processing does not only affect SOIs. The biometric data of every individual who enters a Southern Co-op store with a Facewatch Camera installed is unlawfully processed. The number of data subjects affected by implementation in Southern Co-op stores (leaving aside other Facewatch clients) is likely to number (conservatively) in the thousands per month.

iii. "the person or organisation did not follow relevant advice, warnings, consultation feedback, conditions or guidance from [the Commissioner]": the Commissioner issued a detailed opinion on the use of LFR in public places by private companies in June 2021. This complaint has set out how Facewatch has not followed the advice in that opinion.

iv. **"the breach concerns novel or invasive technology":** LFR is a novel technology that relies on invasive processing of individuals' biometric data that gives data controllers unprecedented amounts of power to track and influence the lives of data subjects.

v. **"the breach involves special category data or a high level of privacy intrusion":** Facewatch and Southern Co-op's processing is of personal data engaging both Articles 9 and 10 UK GDPR. It is highly intrusive.

165. The RAP includes further factors which the Commissioner may consider, some of which militate in favour of action to stop Facewatch and Southern Co-op's unlawful processing:

    i. **"Whether the person or organisation is representative of a sector or group, raising the possibility of similar issues arising again across that group or sector if they do not address them"**: Facewatch (by its own claims) is one of the leading providers of facial recognition technology to private sector organisations in the UK[50]. Its business model explicitly pools incident reports from all of its clients into one National Watchlist, making it representative of a group of organisations implementing this type of processing across the UK.

    ii. **"the public interest in taking regulatory action (for example, […] to test an issue in dispute)":** LFR is a novel technology. As the ICO LFR Opinion indicates, the extent to which it can be lawfully used in public places by private sector organisations is an issue in dispute. Facewatch and Southern Co-op are at the forefront of deploying a novel technology, with serious risk to the rights of data subjects, where there are serious concerns about that deployment's lawfulness. Enforcement action would set an important and useful precedent. Without enforcement action, data controllers are likely to respond to commercial incentives with a creeping implementation of this technology in more and more of our public spaces, fundamentally and illegitimately shifting the power balance away from individuals and in favour of businesses.

166. The processing described in this complaint affects many data subjects. But those whom it affects the most – those included on the National Watchlist as SOIs – are likely to be the least able to stand up for their own data rights due for example to the pressures of living on low incomes or lack of knowledge about law and regulation. There is also a good chance that they do not know they have been subject to this invasive processing. It is not reasonable to expect them to conduct litigation to challenge Facewatch and Southern Co-op's processing.

[50]See also https://www.randdtax.co.uk/safety-or-surveillance-whos-leading-the-facial-recognition-technology-race-in-the-uk/

167. The Commissioner has a general obligation to monitor and enforce the application of the UK GDPR (Article 57(1)(a)). In Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd* (EU:C:2020:559) at para 108 the Court of Justice of the European Union (CJEU) held that "the supervisory authorities' primary responsibility is to monitor the application of the UK GDPR and to ensure its enforcement." Authorities such as the Commissioner must, for example, handle complaints with "all due diligence": para 109. At para 112, the CJEU emphasised the margin of appreciation to for a supervisory authority is limited:

> *"Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is nevertheless required to execute its responsibility for ensuring that the UK GDPR is fully enforced with all due diligence."*

168. As well as unlawful processing of the complainant's personal data, this complaint sets out serious, well-founded concerns about the processing of the personal data of many other data subjects. The Commissioner is well-placed to use his powers under the UK GDPR and DPA to investigate these concerns and take enforcement action where they are found to be substantiated.

169. The complainant requests that the Commissioner:

    i. Fully investigates the concerns raised in this complaint using all the powers vested in him under Article 58 of the UK GDPR and Part 6 DPA.

    ii. Requires Facewatch and Southern Co-op to stop unlawful processing of personal data, including of visitors to Southern Co-op stores, the creation of incident reports and the maintenance of the National Watchlist.

    iii. Requires Facewatch and Southern Co-op to delete all personal data that has been collected or created unlawfully.

Aidan Wills

Matrix Chambers

Alex Lawrence-Archer

AWO

13 July 2022