SUBMISSION TO THE INFORMATION COMMISSIONER

REQUEST FOR AN INVESTIGATION INTO CARRIBEX LTD T/A PIMEYES

UNLAWFUL PROCESSING OF BIOMETRIC DATA

A. Background and summary

I. Background

1. This submission is provided to the Commissioner on behalf of Big Brother Watch as a basis upon which the Commissioner should commence an investigation, using his applicable regulatory powers, into the processing of personal data by PimEyes. Big Brother Watch is not a data subject; it cannot make a complaint under section 165 of the Data Protection Act 2018. Nonetheless, the Commissioner has the general task of monitoring and enforcing the UK General Data Protection Regulation ('**UK GDPR**') in Article 57(1)(a), and of conducting investigations on the application of the UK GDPR in the absence of a data subject complaint in Article 57(1)(h). This submission formally invites the Commissioner to exercise his discretion to commence such an investigation.

2. PimEyes is a trading name of Carribex LTD, New Horizon Building, Ground Floor, 3 1/2 Miles Philip S.W. Goldson Hwy, Belize, and the name of a service hosted at https://pimeyes.com/ which describes itself as a follows:

> *"PimEyes is a facial recognition search engine. It works similarly to other search engines by displaying a list of websites that are related to a query. In PimEyes however, the search is performed based on an uploaded photo. Using PimEyes you can check which websites from the open web have published photos containing a given face."*

3. PimEyes appears to have been operating since at least July 2020[1].

II. Summary of complaint

4. PimEyes processes the personal data of data subjects in the UK, including their biometric data engaging Article 9 UK GDPR, by creating biometric representations from facial images scraped from across the internet, and enabling users to search against that database by uploading a facial image.

5. Anyone can use the PimEyes service. PimEyes does not take any steps whatsoever to restrict the service such that users can only search the database for images of themselves.

6. PimEyes is in breach of the UK GDPR:

[1] https://netzpolitik.org/2020/pimeyes-face-search-company-is-abolishing-our-anonymity/

i. Its processing lacks a valid legal basis, as its interests are outweighed by those of the data subjects whose personal data it processes (Article 6 UK GDPR).

ii. It processes special category biometric data without a valid exemption under Article 9 UK GDPR.

iii. Its processing is not fair, because it is not within the reasonable expectations of data subjects (Article 5(1)(a) UK GDPR).

iv. Its processing is not transparent (Article 5(1)(a) UK GDPR).

v. Its processing likely involves international transfers in breach of Article 44 UK GDPR.

vi. It does not appear to have carried out a data protection impact assessment, in breach of Article 35 UK GDPR.

vii. It has failed to appoint a representative in the UK, in breach of Article 27 UK GDPR.

7. This unlawful processing is intrusive and poses extremely serious risks to the rights and freedoms of UK data subjects.

8. The Information Commissioner is requested to:

i. Fully investigate 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. Require PIMEYES to stop unlawful processing of personal data.

iii. Require PIMEYES to delete all personal data that has been collected or created unlawfully.

B. <u>The processing and its potential consequences</u>

9. The operation of the PimEyes service involves two principal acts of processing: (i) database creation, and (ii) user search.

I. <u>Database creation</u>

10. Per the PimEyes privacy policy (the '**Privacy Policy**')[2]

[2] https://pimeyes.com/en/privacy-policy

"using PimEyes' index. „Fingerprints" of faces found on the Internet are indexed […] for the purpose of further searches […] PimEyes processes the indexed data for the purposes of creating of an index based on publicly available sources, in order to provide the service in the future."

11. That is PimEyes uses automated web crawling to systematically browse the internet[3] and identify facial images. Those facial images are biometrically processed to create mathematical representations of their features ('**feature vectors**', referred to as 'fingerprints' in the Privacy Policy), which are stored on a database (the '**PimEyes Database'**), alongside the source image and the URL where it was originally found. There is no evidence that PimEyes limits its web crawling on any geographic or jurisdictional basis. That is, it biometrically processes *every facial image on the open web* in order to create its database. The PimEyes Database therefore contains feature vectors and associated images and URLs of an unknown, but very large, number of UK data subjects.

II. User search

12. PimEyes allows users to perform a search of the PimEyes Database 'based on an uploaded photo'. The uploaded facial image is itself converted to a feature vector, and that feature vector is compared against all entries in the PimEyes database. For each feature vector in the database matching the uploaded feature vector sufficiently-well, the associated image and URL in the PIMEYES Database is returned as a search result.

13. The effect is to allow the user to *'check which websites from the open web have published photos containing a given face'*, that is search for any facial images on the internet[4] of an individual for whom a user already has at least one facial image. Annex 2 contains screenshots showing the steps in the search process.

14. Any person can carry out a search of the PimEyes database using a facial image of any other person.

[3] PimEyes indicates - https://pimeyes.com/en/contact - that its crawling is limited to internet sites that permit the use of web crawling.
[4] With the minor limitation that PIMEYES claim that only facial images hosted on sites that permit web crawling will be included in the PIMEYES Database, which we are unable to confirm.

III. Biometric processing and controllership

15. Both the creation of the PimEyes Database and each search of it involve the processing of 'biometric data for the purpose of uniquely identifying a natural person' (Article 9 UK GDPR). Every feature vector in the PimEyes Database is:

> *"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images"* (Article 4 UK GDPR)

16. The creation of the PimEyes database involves the creation and storing of biometric data (alongside other personal data, including the facial image itself). Each search of the PimEyes Database involves (i) the creation of biometric data from the uploaded facial image, and (ii) the interrogation and sharing of biometric data (and other personal data) from the PimEyes Database.

17. PimEyes is the data controller for the processing involved in both the database creation and in every search of the PimEyes Database.

IV. Potential Consequences of processing

18. Search allows users to find images of any individual (the **'searched individual'**) from across the internet. Results could include media articles, facial images uploaded by the searched individual's employer, photographs in which the searched individual only appears in the background, business promotional material (e.g. wedding photographers), to name just some examples. The returned facial images are provided alongside the URLs where they are hosted, allowing the user (if they have paid for a subscription account) to navigate to the image(s) and access highly revealing contextual information about the searched individual. This contextual information could include the searched individual's name, details about their place of work, or indications of the area in which they live, for example. Given the indiscriminate nature of the search and the results provided, there are few practical limits on the type or extent of the contextual information that might be returned in response to a search.

19. The uploaded image used for the search can come from anywhere. It could be obtained from another person, purchased, taken from an image of a larger group of people (e.g. a family member in the background of a photograph of a

prominent individual), taken from social media, or even taken surreptitiously in a public place. PimEyes places no limits on the type of images that may be used for search, save (presumably) that they be of sufficient quality and resolution.

20. It can be seen that the PimEyes service allows users to search for individuals who they know, as well as individuals who they do not:

    i. A user could use a PimEyes search to find out a range of personal information about a searched individual whom the user already knows (however well) – a colleague or distant connection on social media, for example.

    ii. Conversely, a user could use a PimEyes search to determine the identity (and other information) of a searched individual whom the user does not know, but has obtained a facial image of.

21. Being the subject of a search is deeply privacy-intrusive. It returns web results about a searched individual that they very likely are not even aware of themselves. A search can (in most cases, likely does) take place without the searched individual being informed. An unknown individual is empowered to obtain an unknown (but likely extensive) amount of information about the searched individual, all without the searched individual's knowledge and as the result of hidden biometric processing of the searched individual.

22. The nature of the PimEyes service means that it is not possible to speculate on all of the different ways in which it might be used, or in which a search might harm data subjects' rights and freedoms. Some specific risks however, are obvious, many of which are likely to be particularly acute for women and girls:

    i. PimEyes could be used to locate an individual as a preliminary to contacting them against their will or harassing them (including where an the searched individual has fled a domestic abuse situation);

    ii. PimEyes could be used in an attempt to uncover 'revenge porn' posted online featuring a searched individual already known to the user[5].

[5] See e.g. https://www.dailymail.co.uk/news/article-11134081/How-intimate-photos-stolen-scorned-partners-shared-social-media-platform-Reddit.html for coverage of the growing extent of such images being posted online without the featured individuals' knowledge.

iii. Conversely, PimEyes could be used in an attempt to discover the identity of an unknown searched individual featured in revenge porn or child sexual abuse material already in the user's possession.

23. These specific risks are only some examples, but give an indication of the potential power of the PimEyes service and the nature of the risks it poses to the data subjects whose data it processes, which can scarcely be overstated.

C. Breaches of the GDPR

I. Territorial extent of the UK GDPR

24. Regardless of where PimEyes is established, its processing is subject to the UK GDPR. Article 3 UK GDPR states:

> *"1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the United Kingdom, regardless of whether the processing takes place in the United Kingdom or not.*
>
> *2. This Regulation applies to the relevant processing of personal data of data subjects who are in the United Kingdom by a controller or processor not established in the United Kingdom, where the processing activities are related to:*
>
> *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the United Kingdom […]"*

25. PimEyes's processing is related to the offering of a service – the PimEyes service – to data subjects in the UK. Recital 23 UK GDPR provides:

> *"[…] factors such as the use of a language or a currency generally used in [the UK] with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the [UK], may make it apparent that the controller envisages offering goods or services to data subjects in the [UK]."*

26. PimEyes offers its website in English and that website is available when browsing from the UK. It offers subscription packages denominated in GBP[6]. It is offering its service to data subjects in the UK. The Privacy Policy also refers to the GDPR, indicating an acceptance on PimEyes' part that its processing is within the scope

[6] https://pimeyes.com/en/premium See also screenshot 4 at Annex 1, accessed 26 August 2022

of the GDPR (and by extension the UK GDPR). PimEyes's processing is therefore subject to the UK GDPR.

II. No Lawful Basis

27. PimEyes does not specify in the Privacy Policy a lawful basis for the processing of personal data involved in the creation of the PimEyes Database, interrogation of the records in that database, or sharing of those records when they match a searched facial image using feature vectors.

28. PimEyes has indicated elsewhere that it relies on Article 6(1)(f) for this processing, which is said to be in its legitimate interests of *'[creating] a database […] for the purposes of future service provision.'*[7] It has not published a legitimate interests assessment.

29. To the extent that PimEyes purports to rely on its legitimate interests as a lawful basis for the processing involved in the creation of the PimEyes database, this is misconceived. Article 6(1)(f) may not be relied upon where the legitimate interests pursued are overridden by data subjects' rights, interests, and freedoms[8]. Assuming (though it is not accepted) that PimEyes has a legitimate interest in offering its service, that legitimate interest is purely commercial and should be accorded little weight. Conversely, the impact of PimEyes's processing on data subjects is negative and substantial. As set out at paras 21 to 23, not only is PimEyes's processing highly intrusive, it creates very serious risks to the privacy, reputation and physical security of every individual included in the PimEyes Database.

30. ICO guidance[9] states:

> *"You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests."*

31. Individuals do not expect that strangers may be able to identify, locate, and learn private information about them using nothing more than an image of their face

[7] https://mobile.twitter.com/PrivaCat/status/1533173442488451076
[8] CJEU *Rigas* C-13/16, 4 May 2017
[9] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

and a free internet search. This is particularly acute given that images returned by a PimEyes search may well have been both taken and uploaded to the internet before facial recognition technology was invented (the technology is still not widely understood by the general public). The PimEyes service carries a very significant risk of causing data subjects in the PimEyes Database unjustified harm. Those data subjects' interests override any commercial legitimate interests that PimEyes has: it cannot rely on Article 6(1)(f) UK GDPR, lacks a legal basis for its database creation and search processing and that processing is therefore in breach of Article 5(1)(a) UK GDPR and unlawful.

32. The Privacy Policy indicates that PimEyes relies on Article 6(1)(a) (consent) for the creation and comparison of a feature vector from an uploaded image as part of a search:

> *"in order to perform the ordered service, PimEyes processes the User's face images provided by the User - face search is carried out using specific technical processing relating to the physical characteristics of a natural person based on the consent expressed by the User before using the service."*

33. The personal data processed for this aspect of a search is that *of the individual in the uploaded image*. It is that individual who would need to consent for the lawful basis to be relied upon by PimEyes. Put another way, this limited aspect of the search would only have a valid legal basis if the user and searched individual are the same person[10].

34. Users are asked as part of the process to accept PimEyes' terms and conditions and the Privacy Policy, which states *"PimEyes is not intended for the surveillance of others and is not designed for that purpose".* However, PimEyes takes no steps to enforce this: a user may upload a facial image of any other person for a search.

35. PimEyes is obliged to demonstrate its compliance with the principle of lawful processing (Article 5(2) UK GDPR). Absent any measures to ensure that the user and the searched individual are the same person, PimEyes cannot demonstrate

[10] Even in such a case, the creation and interrogation of the feature vectors of other individuals in the PimEyes Database would still lack a legal basis.

that its processing can rely on Article 6(1)(a). It is therefore in breach of both Article 5(2) and Article 5(1)(a) in respect of this aspect of its processing.

III. Article 9 UK GDPR

36. As set out at paras 15 to 16, PimEyes creates, stores, interrogates and shares feature vectors from facial images scraped from the web and uploaded by users of the search service. Every feature vector it creates, stores, and uses is biometric personal data engaging Article 9 UK GDPR.

PimEyes's argument that its Database does not contain personal data

37. The Privacy Policy states:

> *"PimEyes never looks for a specific person, it only indexes pictures available on the Internet and the information about the websites where they were found. PimEyes does not establish the identity of persons whose photos are indexed."*

38. This appears to be an argument that Article 9 UK GDPR is not engaged because a search of the PimEyes database does not (necessarily) permit the direct identification by name of one or more individuals. This is misconceived. Article 9 UK GDPR – in combination the definitions of personal data in Article 4(1) UK GDPR – does not require that an individual be directly identified by name for them to be 'identified' by the processing[11]. PimEyes's processing – which creates unique biometric representations of individuals' faces, both in building the PimEyes database and in carrying out user searches, plainly permits the identification of those individuals. Indeed that is its very purpose: *"using PimEyes you can check which websites from the open web have published photos containing a given face."*[12]

No valid exemptions to the prohibition in Article 9 UK GDPR

39. Article 9 UK GDPR prohibits the processing of personal data within its scope, unless one of the exemptions listed at Article 9(2) applies. The Privacy Policy

[11] See also *R (Bridges) v CC South Wales & Ors [2020] EWCA Civ 1058* and European Data Protection Board (EDPB) Guidelines 05/2022 which provides that identification can take place '*without necessarily making the link with the person's civil identity*'. In any case, for many searches of the PimEyes database, individuals are directly identifiable by name, as the results returned include context which permits this.

[12] https://pimeyes.com/en/contact

does not indicate which exemption PimEyes purports to rely on for its processing of biometric data.

40. To the extent that PimEyes purports to rely on the exemption in Article 9(2)(a) (explicit consent), this would be misconceived. As set out in paras 34 to 35, to rely on consent, PimEyes would need to ensure that the search user and searched individual were the same person. It does not and cannot. In any event, this exemption could only apply to the creation of a feature vector from the uploaded image; it would not provide an exemption for the biometric processing involved in creating and interrogating the PimEyes database.

41. To the extent that PimEyes purports to rely on the exemption in Article 9(2)(e) UK GDPR (data manifestly made public) this would also be misconceived. EDPB Guidelines 05/2022[13] state at page 4:

> *"The fact that a photograph has been manifestly made public by the data subject does not entail that the related biometric data, which can be retrieved from the photograph by specific technical means, is considered as having been manifestly made public."*

42. The feature vectors that PimEyes creates, stores, and interrogates have not been manifestly made public and therefore this exemption cannot be relied upon for its biometric processing.

43. No other exemption under Article 9(2) UK GDPR can apply to PimEyes's processing, which is therefore in breach of Article 9 UK GDPR and unlawful.

III. Fairness

44. 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."*[14]

[13] https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf
[14] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

45. The PimEyes service is unusual and relies on technology that is not well-understood by the data subjects whose data it processes (every person for whom at least one facial image exists on the open web). As set out at para 31, PimEyes's processing is far from being within data subjects' reasonable expectations, and PimEyes can offer no justification for this unexpected processing. And as set out at paras 21 to 23, the processing involves the risk of the most serious adverse impacts on data subjects, which PimEyes cannot possibly justify. Its processing is unfair, in breach of Article 5(1)(a) UK GDPR and therefore unlawful.

IV. Transparency

46. Processing of personal data must be transparent (Article 5(1)(a) UK GDPR). PimEyes has transparency obligations to every person from whose face it creates a feature vector for its database (every person who has at least one facial image on the open web).

47. The Information Commissioner has stated[15] 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."

48. 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. PimEyes's processing is highly intrusive, involves sensitive data, and creates extreme risks for data subjects. It requires a high degree of transparency. The minimum required to be provided to data subjects is set out in Article 14(1) UK GDPR. The information in Article 14(2) UK GDPR should also be provided to data subjects given the high degree of transparency required.

49. PimEyes provides none of the information in Articles 14(1) and (2) to data subjects. To the extent PimEyes purports to rely on the exemption in Article 14(5), this would be misconceived. It is not 'impossible' to provide transparency information to the data subjects. It would involve a significant amount of effort, but the intrusiveness of, and risks involved in, PimEyes's processing mean that

[15] *Ibid*

that effort would not be 'disproportionate'. PimEyes is therefore in breach of Article 14 UK GDPR in its entirety.

50. If (which is not accepted) the exemption in Article 14(5) could apply, PimEyes would be required to *'take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available'*. PimEyes does not take any such measures. Among other things, PimEyes fails to make publicly available the information in Articles 14(1)(b), (c) (d), (e), (f) and 14(2)(b), (c) and (e).

V. International transfers

51. PimEyes does not state publicly where it carries out its processing, but given it is headquartered in Belize, there is good reason to believe that personal data of UK data subjects are transferred out of the UK in breach of Article 44 UK GDPR.

VI. Data Protection Impact Assessments

52. Article 35 UK GDPR requires:

> *"(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."* (emphasis added)

53. PimEyes should have a data protection impact assessment ('**DPIA**') in place for its processing. Per Article 35(7) UK GDPR, that 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."

54. This complaint details considerations relevant to proportionality and risks to rights and freedoms of data subjects. Contrary to ICO Guidance[16] PimEyes has not published a DPIA. If one is not in place, its 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.

VII. No representative in the UK

55. Article 27 UK GDPR provides:

> *"Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the United Kingdom"*

56. As set out at paras 24 to 26, Article 3(2) applies. PimEyes has not designated a representative in the United Kingdom, and it is therefore in breach of Article 27 UK GDPR.

D. Requests to the Information Commissioner

57. This complaint discloses a business model based on the systematic unlawful biometric processing of the personal data of every UK data subject for whom there is at least one facial image on the open web – likely to number in the millions if not tens of millions. This unlawful processing creates extreme risks for those data subjects, making regulatory action urgent.

58. The Information Commissioner's Draft Regulatory Action Policy[17] ('RAP') sets out a number of aggravating factors to be taken into account when considering whether and how to use the Commissioner's powers. A number of those aggravating factors apply to PimEyes's processing, underlining the urgency and importance of remedial action by the Commissioner:

[16] 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
[17] https://ico.org.uk/media/about-the-ico/consultations/4019400/regulatory-action-policy-2021_for-consultation.pdf

i. **"the attitude and conduct of the person or organisation concerned suggests an […] an unlawful business or operating model":** PimEyes' sole service is its unlawful search function; its business model is unlawful.

ii. **"the data protection legislation breaches […] affected many people":** PimEyes has unlawfully processed the personal data of every UK data subject with a facial image on the open web; this is likely to run into the 10s of millions.

iii. **"the breach concerns novel or invasive technology":** Facial recognition is a novel technology that relies on invasive processing of individuals' biometric data creating unprecedented risks to data subjects.

iv. **"the breach involves special category data or a high level of privacy intrusion":** PimEyes's processing is of personal data engaging Article 9 UK GDPR and is highly intrusive.

59. PimEyes's processing affects many data subjects. The vast majority will be completely unaware of this processing – even where a search is made using an image of their face. It is not reasonable to expect them to conduct litigation to challenge PimEyes's processing; they are reliant on the Commissioner taking action.

60. 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, enforce the UK GDPR 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."*

61. The Commissioner is well-placed to use his powers under the UK GDPR and DPA to investigate the concerns in this complaint and take enforcement action where they are found to be substantiated. There is no practical alternative to the Commissioner carrying out the tasks imposed on him by the UK GDPR in relation to PimEyes. It is not possible to rely on individual data subjects to commence litigation against PimEyes, as its use of scraping means only a tiny percentage of those whose facial images have been processed will be aware of that processing.

62. Big Brother Watch 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 PIMEYES to stop unlawful processing of personal data.

    iii. Requires PIMEYES to delete all personal data that has been collected or created unlawfully.

    iv. Takes such other regulatory action as the Commissioner thinks appropriate.

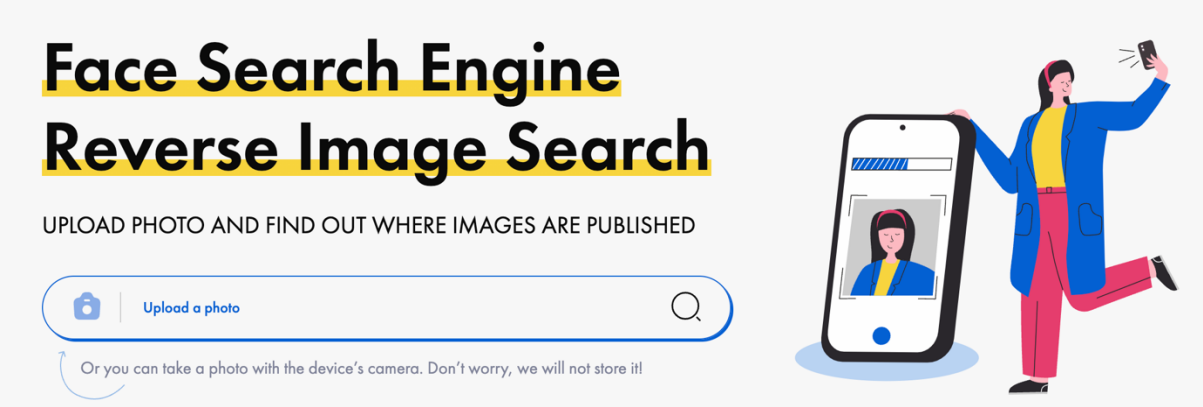
Alex Lawrence-Archer

AWO

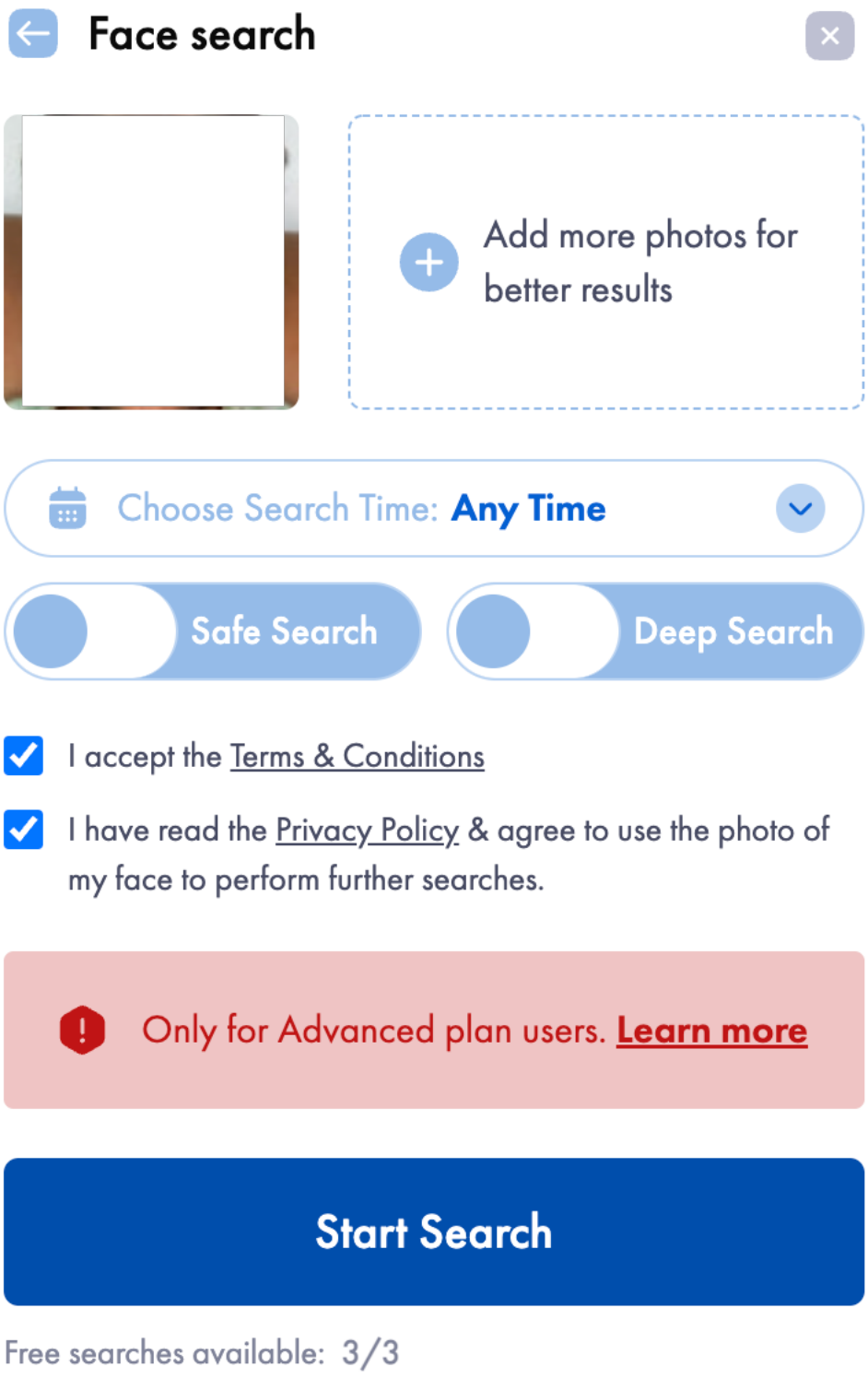
September 2022

E. Annex: Screenshots

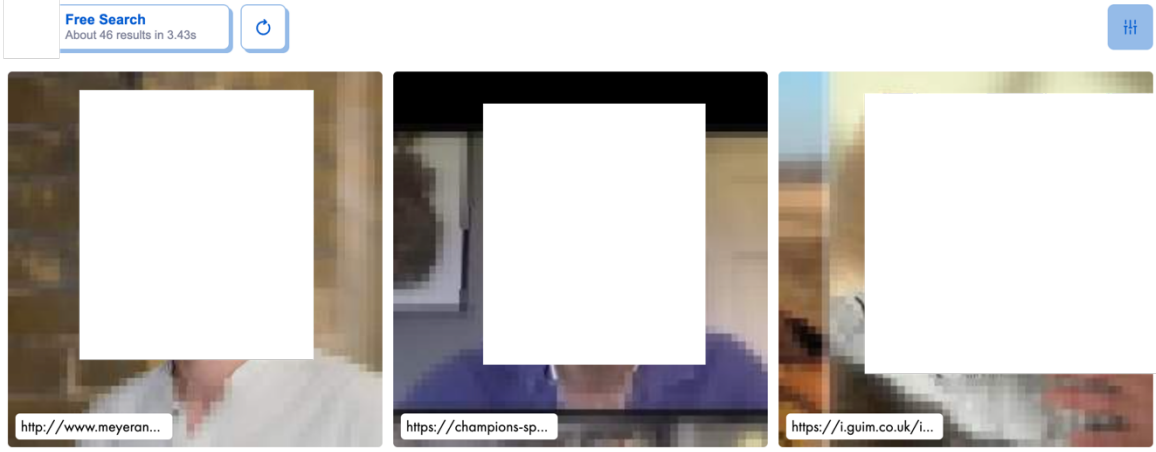
Screenshot 1: upload photo for search



Screenshot 2: confirm search



Screenshot 3: receive images and URLs



Screenshot 4: subscriptions offered in GBP