EDPS Opinion on the possibility to use Clearview AI and similar services at Europol (Case 2020-0372)

1. INTRODUCTION

This Opinion relates to the use that can be made of Clearview AI and similar services at Europol.

Clearview AI is an American private company offering a browser-based[1] product through which users can upload facial images for analysis and cross-checking against a database of images scraped by Clearview from a variety of sources, including social media.[2]

The EDPS has prepared this Opinion following news that Clearview had been demonstrated at Europol. As the EDPS got reassurance that Europol had not used Clearview AI in any structural capacity, the EDPS elects at this point to provide guidance and recommendations, which can then also be taken into account for similar services in the future.

The EDPS issues this Opinion in accordance with Article 43(2)(d) of Regulation (EU) 2016/794[3] ('the Europol Regulation', or 'ER' abbreviated), which includes the possibility for the EDPS to provide advice to Europol, on his own initiative, on all matters concerning the processing of personal data.

2. BACKGROUND AND FACTUAL DESCRIPTION

On 18 January 2020, the New York Times published an article alleging that Clearview AI was being used by over 600 law enforcement agencies worldwide.[4] The publication of this article prompted many data protection authorities around the globe to look into the use being made of Clearview AI within their respective jurisdictions.[5]

On 11 February 2020, the EDPS relayed this information to the Europol Data Protection Function ('DPF') and asked, via email, whether Europol uses Clearview AI or if Europol activities are in any way linked to the use of this application. On 20 February, the DPF answered that Europol was not using any related Clearview AI product.

---

1 EDOC#1115855v1, page 1.

2 Scraped images and corresponding URLs are kept by Clearview even after the original URL to the online image or corresponding webpage has been taken down. 'De-indexing' requests can in these scenarios be sent to Clearview AI via the following form: https://clearview.ai/privacy/deindex.

3 Regulation 2016/794 of the European Parliament and the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ, L 135, 24.05.2016, pp. 53-114.

4 Available at https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

5 For example: (SE) https://www.datainspektionen.se/nyheter/datainspektionen-inleder-tillsyn-med- anledning-av-clearview-ai/, (CA) https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/, (AU, UK) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

In the course of March 2020, several newspapers[6] reported that the application Clearview AI had been demonstrated during a meeting held at Europol's headquarters in autumn 2019.

Following these information, the EDPS sent several requests[7] to the DPF via email to obtain further information and clarification regarding the involvement of Europol in the use of Clearview AI:

- The first request inquired into Europol's past and future activities which might be in any way linked to the use of this application. In its response, Europol confirmed that one of the external participants at the 7th Victim Identification Taskforce ('VIDTF 7'), had demonstrated the tool to the participants to illustrate its usefulness in identifying victims. The VIDTF series is a recurring event hosted by Europol in the fight against child sexual abuse. Europol confirmed that the tool: '[...] *was not used at any stage by AP Twins staff. The demonstration was part of the regular work of VIDTF, exchange of information, tools and investigative methods and its use was not endorsed by Europol.*'

- The EDPS' second request sought to collect further information regarding the organisation of these VIDTF meetings. The EDPS' questions inquired into the kinds of personal data that are used for these meetings and the way they are being processed. From Europol's responses, the EDPS learned that the '*primary focus of the Victim Identification Task Force (VIDTF) is the identification of child victims of sexual abuse through the examination of visual and audio information from digital pictures and video-audio recordings seized throughout investigations related to online child sexual exploitation and contributed by Member States and Third Parties.*' Secondly, the participants to the taskforce meeting '*support one another by sharing their different experiences and knowledge in relation to Victim Identification including the tools and techniques that they use.*' The one-off demonstration of Clearview AI took place in the context of this second goal of the VIDTF series.

- With its third request, the EDPS sought to clarify various aspects related to the demonstration of new technologies during the VIDTF meetings. The EDPS learned that the demonstration of Clearview AI was made by [redacted] at Europol's premises, using one or more photos provided by Europol [redacted]

The EDPS learned that, aside from the IVAS, the VIDTF relies on a number of Europol datasets and resources [redacted]. On the external side, these resources are complemented by:

A. specialist law enforcement databases such as the Interpol International Child Sexual Exploitation ('ICSE') database; and
B. open-source intelligence ('OSINT') resources.[11]

---

6 For example: https://www.svt.se/nyheter/inrikes/polisen-utsatt-barn-identifierades-med-hjalp-av-clearview-ai.

7 On 13 March 2020, 23 March 2020 and 28 May 2020.

8 [redacted]

9 [redacted]

10 [redacted]

During operator processing, internal and external databases and resources are queried while defining or adding e.g. victim/offender data, circumstance data or metadata to the series, in order to identify the victim or the relevant country.[12] In response to the EDPS' questions of 28 May 2020, **Europol stated that it would categorise potential future use of Clearview AI as performing OSINT searches**.[13] It is therefore necessary to consider whether use of Clearview AI in the context of VIDTFs could legally qualify as performing OSINT searches, namely whether it is compatible with Article 17(2) ER.

3. LEGAL ANALYSIS AND RECOMMENDATIONS

3.1. Regarding the qualification of Clearview AI as OSINT

Under Article 17(2) ER, Europol may directly retrieve and process information, including personal data, from publicly available sources, such as the internet and public data.

The EDPS understands that personal data may also be retrieved from various publicly available sources by another party on behalf of Europol,[14] as long as this party acts in the capacity of a processor. Considering the variety and volume of resources available online, the fact that a private entity simply gathers personal data from many different resources and provides them in a more structured overview to Europol, does not by itself disqualify Article 17(2) ER as a legal basis. However, this intermediary role should be interpreted strictly. Where an entity goes beyond the tasks of a processor and changes either the purposes or the essential means of the processing, for instance by enriching the personal data with non-publicly available personal data, Europol would no longer be covered by Article 17(2) ER when it retrieves personal data from this entity.

Irrespective of the (unverified) claim made by Clearview AI that it retrieves all images from publicly available sources, it has to be considered that it does not collect these images merely to make them accessible to Europol, but that it uses the images to offer its proprietary facial matching algorithm to law enforcement services worldwide.

In other words, what Clearview does not do is:

- merely providing a set of already publicly available data in aggregated format; or
- selling or licensing a local copy of the software to Europol, which can be used without needing to go through Clearview as an intermediary.

Instead, Clearview sells a facial recognition service completely hosted and operated on its own platform, ostensibly without following any instructions with regards to the purposes and the essential elements of the means of its services.[15] Therefore, the EDPS considers that Clearview would not seem to qualify as a processor acting on behalf of Europol and that Europol would not be covered by Article 17(2) ER when making use of its services. The

---

11 [redacted]

12 [redacted]

13 [redacted]

14 EDPS case 2019-0063.

15 See in this respect the EDPS' guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, available on the EDPS website https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf.

EDPS further reiterates that there is an obligation on controllers to assess whether the data protection guarantees offered by the processor are sufficient. According to the information available, such an assessment has not taken place yet.

While in light of the above, the EDPS would not consider Clearview AI as an intermediary acting [redacted] or the retrieval of OSINT, it should be examined whether Clearview AI itself could be considered a "publicly available source", as referred to in Article 17(2) ER. In that regard, the EDPS takes into consideration that access to Clearview's platform, even if free of charge, is very restrictive. Clearview mentions on its website that it is only available to 'active law enforcement personnel'.[16] In order to verify that a potential user is working in law enforcement, a host of personal data are requested, including 'title or rank' and the 'name of the agency or department'. Registration is only granted once these data have been verified. This indicates that access to Clearview's information is not publicly available.

Clearview's registration requirements also contradict Europol's own internal conditions for OSINT, which can be found in the Europol Anonymous Internet Service ('AIS') policy. [redacted][17]

Some examples of open source searches provided by Europol include:[18]

- Forums and social networks, [...] including personal data such as [...] pictures and links made available to the public;
- Publicly available parts of the Dark Web.

Based on the above, the EDPS concludes that registration to Clearview AI is definitively not available to '*any Internet user*' as required by the AIS policy. The EDPS generally would not consider it sufficient that a source is accessible for 'any law enforcement officer' for Article 17(2) ER to apply. Rather it should be possible for members of the public, in particular journalists and civil society, to access these databases and to scrutinise its contents.

Considering that transferring (via upload) and retrieving personal data from Clearview AI is likely not compliant with the Europol Regulation, the EDPS strongly advises Europol not to engage its services. Equally, the EDPS advises against allowing third parties to check Europol data using Clearview AI at Europol organised events, as this would amount to a circumvention of the specific regime of the Europol Regulation. A similar assessment should be made by Europol for each potential provider of publicly available information, prior to engaging its services.

3.2.Regarding the demonstration of similar solutions at Europol events

The EDPS notes that Clearview AI has not been structurally used by or at Europol in the framework of its operational support. Rather it has been demonstrated in a one-off manner

16 https://clearviewai.typeform.com/to/asZZXY.
17 [redacted]
18 [redacted]

by a partner authority, using personal data provided by Europol. So far, results from OSINT have not been required to be logged as part of the VIDTF workflow. As such Europol has not kept track of the particular image or video file used by the participant [redacted] for the demonstration of Clearview AI.[19]

While the EDPS supports the exploration of novel tools in the fight against crime, the EDPS points to the risks for data subjects where their data are used to demonstrate tools which may not be compliant with the Europol Regulation.

Therefore, a list of proposed tools to be demonstrated by Europol partners should be drawn up prior to each event organised by Europol. Where it is clear that Europol itself would not be able to use of this tool, or where there are significant doubts on the tool's compliance with the Europol Regulation, Europol should ask the partners to perform the demonstration using national data, rather than providing Europol data for this purpose.

Furthermore, where the demonstration of the tool took place using personal data provided by Europol, the demonstration should be logged by Europol. This logging should include a reference to the exact personal data being used and the outcome of the use.

4. CONCLUSION

The EDPS recommends Europol, pursuant to Article 43(3)(d) ER to:

1. not engage the services of Clearview AI, as this would likely infringe the Europol Regulation;
2. not promote the use of Clearview AI at Europol events, or provide Europol data to be processed by third parties using Clearview at these events;
3. perform an assessment of whether similar service providers could be qualified as processors, before engaging them under Article 17(2) ER;
4. draw up a list of novel tools which will be demonstrated at each Europol event, prior to the event taking place;
5. perform an assessment of whether these tools would be likely to comply with the Europol Regulation;
    a. where compliance is unlikely, or where compliance is unclear, Europol should ask participants to use national data for their demonstrations;
    b. where the tool would be considered compliant, Europol may provide personal data, however it should log the demonstration, including at least a reference to the exact personal data being used and the outcome of the use.

Done at Brussels, 29 March 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI

[19] [redacted]