European Data Protection Board

Ms Sophie in 't Veld,
Mr Moritz Körner,
Mr Michal Šimečka,
Ms Fabiene Keller,
Mr Jan-Christoph Oetjen,
Ms Anna Donáth,
Ms Maite Pagazaurtundúa,
Mr Olivier Chastel,
Members of the European Parliament

10 June 2020

By email only

Ref: OUT2020-0052

Dear Members of the European Parliament,

Thank you for your letter concerning the facial recognition app developed by Clearview AI and for your continued vigilance in protecting the personal data of individuals in the Union. The EDPB naturally shares your commitment and is, beyond this case, particularly concerned by certain developments in the European Union and around the world regarding facial recognition technologies, which raise unprecedented issues from the point of view of data protection.

Facial recognition technology may undermine the right to respect for private life and the protection of personal data, but also other fundamental rights and freedoms (in particular freedom of expression and information, freedom of assembly and association, and freedom of thought, conscience and religion). It may also affect individuals' reasonable expectation of anonymity in public spaces. Such technology also raises wider issues from an ethical and societal point of view.

Regarding the service offered by Clearview AI, the EDPB is aware of media reports indicating that the company has been in contact with national law enforcement agencies, government bodies, and police forces in several EU Member States. The EDPB furthermore has taken note of the public acknowledgement of limited use by police forces in one of the Member States. The EDPB also notes that since Clearview AI's database is allegedly set up by "scraping" photographs and facial pictures accessible online, in particular those made available via social networks, the possible use of this service by law enforcement authorities (comparing photos through facial recognition analysis against the database) is likely to entail the processing of biometric data of persons in the European Union.

Based on the information at its disposal to date, the EDPB is in a position to share some preliminary answers to the questions you raised. This preliminary assessment focuses on the compliance and lawfulness of processing resulting from the possible use by EU law enforcement authorities of a service such as offered by Clearview AI. For your information, several EDPB members have already started to further inquire about the use of such facial recognition technologies in their respective jurisdictions. Please note that for the investigation and enforcement of individual cases the competency lies with each individual member of the EDPB.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

On the possible use of the Clearview AI application by law enforcement authorities in the EU

The EDPB notes that under the Law Enforcement Directive (EU) 2016/680, law enforcement authorities in the Union may process biometric data for the purpose of uniquely identifying a natural person only in accordance with the strict conditions of Articles 8 and 10 of the Directive. According to Article 8, such processing can only take place to the extent necessary for the performance of a task for purposes to which the Directive applies and that is based on Union or Member State law, which must comply with the EU Charter of Fundamental Rights as well as the European Convention on Human Rights. In addition, Art. 10 requires such processing, inter alia, to be strictly necessary and subject to appropriate safeguards for the rights and freedoms of data subjects.[1] In line with these strict conditions, EU law enforcement authorities may under certain circumstances process certain biometric data, including biometric templates from photos and check these against biometric templates in databases that are under the control of the official authorities and that have been established under Union or Member State law.

The possible use of a service such as offered by Clearview AI by law enforcement authorities would, however, be fundamentally different, in that it would imply, as part of a police or criminal investigation, the sharing of personal data with a private party outside the Union and the biometric matching of such data against the latter's mass and arbitrarily populated database of photographs and facial pictures accessible online.

The EDPB has doubts as to whether any Union or Member State law provides a legal basis for using a service such as offered by Clearview AI. Therefore, as it stands and without prejudice to any future or pending investigation, the lawfulness of such use by EU law enforcement authorities cannot be ascertained.

In addition, the EDPB considers that processing of personal data in a law enforcement context that would rely on a database populated by collection of personal data on a mass-scale and in an indiscriminate way without any limitation, or any precise connection between the data collected and the objective pursued would, as such, likely not meet the strict necessity requirement provided for by the Directive. As regards observance of this principle of proportionality, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court of Justice of the European Union, that derogations from and limitations to the protection of personal data should apply only in so far as it is strictly necessary.[2]

[1] The need for safeguards is all the greater where personal data is subject to automated processing. Those considerations apply particularly where the protection of the particular category of personal data that is sensitive data is at stake (see, to that effect, judgments of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55, and of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 109 and 117; see, to that effect, ECtHR, 4 December 2008, S. and Marper v. the United Kingdom, CE:ECHR:2008:1204JUD003056204, § 103).

[2] (judgments of 16 December 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU:C:2008:727, paragraph 56; of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 51 and 52; of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 92; and of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 96 and 103).

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Finally, the EDPB notes that the possible use by EU law enforcement authorities of an application made available by a data controller with established operations outside the Union such as Clearview AI would constitute a transfer of personal data from the Union to the United States of America, where the company is established (e.g. the transfer of personal data of those whose identity is sought through the use of the facial recognition service). The EDPB notes in particular that the transfer of personal data would not be subject to the provisions of the EU-US Privacy Shield adequacy decision, nor to the EU-US Umbrella Agreement. To be lawful, such a transfer would have to be compliant with the strict conditions and requirements set in Article 39 of the Law Enforcement Directive that governs specifically transfers from EU law enforcement authorities to private operators in third countries.

Without prejudice to further analysis on the basis of additional elements provided, the EDPB is therefore of the opinion that the use of a service such as Clearview AI by law enforcement authorities in the European Union would, as it stands, likely not be consistent with the EU data protection regime.

On the possible use of the Clearview AI application by intelligence services in the EU

In view of its competence, the EDPB this letter focuses primarily on the possible use of an application such as the Clearview AI by law enforcement authorities.

While questions relating to processing in the area of national security fall only partly within the scope of EU law and therefore the competence of the EDPB, it should be recalled that at any rate, processing of this data by intelligence services should, always, be carried out under conditions complying with the provisions of the European Convention on Human Rights, as interpreted by the European Court of Human Rights, and Convention 108.

On the EDPB initiatives related to facial recognition technologies

This preliminary assessment by the EDPB is without prejudice to any initiative or formal decisions that national supervisory authorities may wish to take in respect of both the processing carried out by Clearview AI on its own behalf under the GDPR and the possible use of such service by law enforcement agencies, as well as intelligence authorities when falling within the scope of their competence, in the EU.

The EDPB is committed to continuing its work on analysing the use of facial recognition in its various forms. The EDPB guidelines adopted in January 2020 on processing of personal data through video devices already address this technology and several supervisory authorities have also taken positions or adopted decisions on specific cases involving facial recognition. This work will be continued by the EDPB, in particular with a view to inform future legislative work at European and national level, also with regard to the use of facial recognition technology by law enforcement authorities.

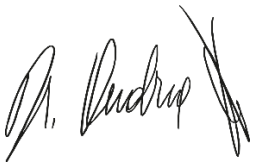
The EDPB considers that, beyond the need for compliance with the EU data protection *acquis*, facial recognition - for which different usages raise different issues - calls for political choices to be made:

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

as to the role a democratic society is ready to give this technology and how it affects the fundamental rights and freedoms of individuals. The EDPB is willing to contribute, within the limits of its competence, to the necessary political decision-making on this matter. In this context, the EDPB considers that the recent White Paper of the European Commission on artificial intelligence provides an opportunity for such debate which should lead to the determination of cases in which facial recognition is acceptable and necessary in a democratic society and cases in which it is not.

Yours sincerely,



Andrea Jelinek

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels