Center for AI and
Digital Policy

1 August 2022

Dr. Andrea Jelinek
Chair of the European Data Protection Board
Rue Montoyer 30, B-1000 Brussels

Public consultation reference: **05/2022**

The Center for AI and Digital Policy (CAIDP) welcomes the opportunity to comment on the European Data Protection Board's (EDPB) proposed guidelines on the use of Facial Recognition Technology in the Area of Law Enforcement (EDPB Guidelines 05/2022).[1] We acknowledge that our comments are submitted after the deadline. However, we are now able to call attention to the recent decision of the Court of Justice of the European Union concerning AI and machine learning.[2] The CJEU has reaffirmed the primacy of a human-centered approach to AI in the *Ligue des droits humains* judgement. Protection of fundamental rights constitutes an effective limit to the use of facial recognition technology, which should be assessed accordingly. We discuss this topic in more detail at the end of our comments.

CAIDP is an independent non-profit organization that advises national governments and international organizations, including the OECD, the Global Partnership on AI, the Council of Europe, the European Union, the G7/G20, on artificial intelligence (AI) and digital policy. CAIDP aims to ensure that artificial intelligence and digital policies promote a better society, fairer, more just, and more accountable – a world where technology promotes broad social inclusion based on fundamental rights, democratic institutions, and the rule of law.

We work with more than 200 AI policy experts in almost 50 countries and recently published the report *Artificial Intelligence and Democratic Values* which surveys and assesses the AI policies and practices of 50 countries around the world.[3] We have provided

[1] The European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* (May 12, 2022), https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

[2] CJEU - C-817/19 - Ligue des droits humains v. Conseil des Ministres, Judgement, 21 June 2022, https://curia.europa.eu/juris/document/document.jsf?text=&docid=261282&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=335316

[3] CAIDP, *Artificial Intelligence and Democratic Values 2021* (2022) ("*CAIDP AI and Democratic Values report*") https://www.caidp.org/app/download/8376927963/AIDV-Index-2021.pdf?

recommendations to the G20 nations - in our Statement to G-20 Digital Economy Task Force (DETF), we urged the G20 to focus on fairness, accountability, transparency for all AI systems, and to endorse "red lines" for certain AI deployments that violate fundamental freedom.[4] One of CAIDP's core goals is to promote public participation in the AI policy process. We have established the "Public Voice" page to encourage public participation in the policy process.[5] This initiative supports government efforts to engage the public in AI decision-making and helps to produce better informed and more legitimate AI policies.

We support the EDPB Guidelines 05/2022 on the Use of Facial Recognition for Law Enforcement and appreciate the opportunity to provide comments. Our comments focus on:

1. *Limitations on Photographs made Public*
2. *Data Protection Impact Assessments*
3. *Human intervention and oversight*
4. *Exchanges of personal data between national LEAs*
5. *Annex III – the deployment scenarios*

We commend the EDPB for your report last year with the European Data Protection Supervisor (EDPS) calling for a ban on the use of AI techniques for facial recognition in public spaces.[6] In our report *Artificial Intelligence and Democratic Values*, we called for a prohibition on facial recognition for mass surveillance.[7] We have since determined that the ability to prohibit the use of facial surveillance may, at this time, be one of the best indicators of democratic limits on AI technology.[8] We noted the report and resolution of the European Parliament following the EDPB-EDPS report.[9] We hope that the EU AI Act will incorporate the recommendations you have provided.

[4] CAIDP, *Statement for the Digital Economy Task Force* (Mar. 17, 2021), https://www.caidp.org/app/download/8303562963/CAIDP-DETF-03172021.pdf

[5] CAIDP, *The Public Voice,* https://www.caidp.org/public-voice/

[6] EDPB, *EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination (*Jun. 21, 2021), https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-

[7] CAIDP, *Artificial Intelligence and Democratic Values 2021* (2022) ("*CAIDP AI and Democratic Values report*") https://www.caidp.org/app/download/8376927963/AIDV-Index-2021.pdf?

[8] CAIDP, *Statement in support of European Citizen Initiative to Ban Biometric Mass Surveillance* (Mar. 3, 2021), https://www.caidp.org/app/download/8299428763/CAIDP-ECI-03032021.pdf

[9] The European Parliament Research Service, *Regulating facial recognition in the EU* (Sep. 2021),

We agree also with other recommendations contained in the EDPB-EDPS Joint Opinion on the draft EU AI Act, including a ban on AI systems using biometrics to categorize individuals by ethnicity, gender, political or sexual orientation, as well as the use of AI to infer emotions, except for very narrow cases (and for the benefit of individuals).[10] We also support your recommendation to prohibit any type of social scoring. The UNESCO's Recommendation on the Ethics of Artificial Intelligence states that "*AI systems should not be used for social scoring or mass surveillance purposes.*"[11] The UNESCO AI Recommendation also found that "*greater transparency contributes to more peaceful, just, democratic and inclusive societies.*"[12] The UN High Commissioner for Human Rights has called for a prohibition on AI practices that violate international human rights law and a moratorium on the use of facial recognition for mass surveillance.[13]

We also support the recent call of EDPB for Experts to "cooperate with Supervisory Authorities around the European Economic Area (EEA), on different stages of their investigation and enforcement activities in the field of data protection law."[14] One of the key tasks of Supervisory Authorities, as set out in the GDPR, is to "monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices."[15] In addition to assisting Supervisory Authorities enforce the safeguarding of personal data, the Pool of Experts

https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf; European Parliament*, Resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (Oct. 6, 2021), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.pdf

[10] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (18 June 2021) <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf>.

[11] *UNESCO Recommendations on the Ethics of AI* at 7 (2021) (Recommendation #26), https://unesdoc.unesco.org/ark:/48223/pf0000380455; CAIDP, *UNESCO Finalizes Recommendation on AI Ethics,* CAIDP Update 2.25 (Jul. 2, 2021), https://www.caidp.org/app/download/8330514463/CAIDP-Update-2.26.pdf;

[12] *UNESCO Recommendations on the Ethics of AI* at 9 (2021) (Recommendation #38), https://unesdoc.unesco.org/ark:/48223/pf0000380455;

[13] United Nation Human Rights Office of the High Commissioner, *Artificial intelligence risks to privacy demand urgent action – Bachelet* (Sep.15, 2021), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E

[14] EDPB*, Call for Experts, the new EDPB Support Pool of Experts* (Feb. 21, 2022), https://edpb.europa.eu/news/news/2022/call-experts-new-edpb-support-pool-experts_en

[15] GDPR, Article 57(1)(i), https://gdpr-info.eu/art-57-gdpr/

could also provide advice concerning new technologies and new business practices that implicate data protection. The Working Party 29, the predecessor of the EPDB, issued many such reports on these topics.[16]

Necessity and proportionality test

The Guidelines make clear that one shall assess necessity and proportionality in all proposed applications of Facial Recognition. Also, the Guidelines highlights the need to differentiate and target those persons covered by it in the light of the objective, and clearly states that systemic processing of personal data without the knowledge of the data subjects, is likely to generate a general conception of constant surveillance.

The Center strongly supports banning mass surveillance.[17] In our report we noticed that facial recognition for mass surveillance was the most controversial application of AI. Countries around the globe still need to act against mass surveillance. The Center has issued two key recommendations concerning mass surveillance: "Countries must halt the use of facial recognition for mass surveillance" and "Countries must commit to these principles in the development, procurement, and implementation of AI systems for public services"[18].

Therefore, we oppose the use of FRT for mass surveillance, since constant monitoring violates fundamental rights. LEAs are not always following AI principles, for instance mass surveillance in Netherlands conducted by police[19]. Using facial recognition technology by police for mass surveillance purposes is appalling and violates human rights in several different ways[20]. The Guidelines state, "*With regard to data subjects for whom there is no evidence capable of*

[16] See, for example, Article 29 Data Protection Working Party, *Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6* (May 30, 2002), https://ec.europa.eu/justice/article- 29/documentation/opinion-recommendation/files/2002/wp58_en.pdf

[17] CAIDP, *Statement in support of European Citizen Initiative to Ban Biometric Mass Surveillance* (Mar. 3, 2021), https://www.caidp.org/app/download/8299428763/CAIDP-ECI-03032021.pdf

[18] CAIDP, *Artificial Intelligence and Democratic Values* (2020), (Recommendations), https://www.caidp.org/reports/aidv-2020/

[19] The Amnesty International, *Netherlands: End dangerous mass surveillance policing experiments* (Sep. 29, 2020), https://www.amnesty.org/en/latest/news/2020/09/netherlands-end-mass-surveillance-predictive-policing-2/

[20] The Amnesty International, *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance* (Jun. 11 2020), https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/

suggesting that their conduct might have a link, even an indirect or remote one, with the legitimate aim according to the LED, there is most likely no justification of an interference". Words "most likely" might be read to suggest that even in case of no evidence, interference can still be justifiable, which could serve as a loophole for mass surveillance. Considering the present wordings, as well as the abuse of FRT by LEA makes clear the need for a prohibition. Therefore, we recommend that the Guidelines make clear that Facial Recognition Technology for mass surveillance is not permissible.

Further, we recommend clarifying the particular cases where LEAs are entitled to use FRTs. We express our concerns that the requirement might be interpreted in a broader way, since LEAs might argue based on an ambiguous legitimate aim. The aim should be to narrow the scope of permissible surveillance. Also, the Guidelines need to make clear which cases are "not applicable" or what is "not possible".

Photographs made public

The Guidelines establish that biometric data retrieved from a photograph that is publicly accessible cannot be considered images manifestly made public. This will help to prevent the activities of companies such as Clearview AI whose face images database is mainly nurtured by images taken from websites where images may be public available but they are often posted without the knowledge or consent of the person concerned, or the image is posted in the context of a particular network or organization for use related to the network or organization.[21] And even images that are widely available, such as advertising images associated with celebrities, may have use restrictions imposed by licensing arrangements and legal rules.

The EDPB Guidelines establish that only when the data subject intentionally makes public their biometric template, without restriction on subsequent use, can this be considered personal data manifestly made public. However, state of the art FRT does not require biometric templates to provide identification or verification anymore due to the improvement in deep learning techniques. Therefore, such a provision should be amended to reflect state of the art AI techniques employed by FRT that can produce a match just by comparing facial images without the use of biometric templates.

Data Protection Impact Assessment

[21] See also EDPB, *EDPB response to MEPs Sophie in 't Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI* (2020) https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en)

The EDPB’s recommendation to make DPIAs’ results public is welcome since it will help harmonize DPAs’ activities and criteria. However, the Guidelines do not specify what exactly they mean by making it public. This should be clearly stated as then the recommendation can be easily adopted and enforced if necessary.

Human intervention and oversight

The Guidelines cite recital 38 of LED and indicate that should decision-making be done solely based on FRT, then the data subjects need to be informed about the features of automated decision making. Later in the recommendations section the Guidelines highlight the importance of human intervention and indicate the following: “never take any measure concerning an individual solely based on the outcome of FRT. Also ensure that LEA users avoid automation bias, by investigating contradictory information and critically challenging the results of the technology”. We strongly support the Guidelines emphasis on human oversight. We believe that AI profiling technologies in general and FRT in particular should be carefully monitored by human agents. The risk of succumbing to automation bias within the use of FRT by LEAs has already led to wrongful arrests and incarceration within the U.S.[22]

The Guidelines also encourage LEAs to record, measure and assess to which extent human oversight changes the FRT original decision. We consider that it will beneficial if the Guidelines set certain requirements for deviations and also provide some guidance on how LEAs shall treat particular FRT decision of which often changes by humans.

Exchange information between national LEAs

Recently, the EU has adopted two proposals that will modify the way LEAs interact with one another and exchange data, in particular: the Proposal for a Directive on information exchange between law enforcement authorities[23] and the Proposal for a Regulation on automated data exchange for police cooperation (“Prüm II”)[24]. Article 21 of the Prum II Proposal clearly

[22] Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives* (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/

[23] EU, *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA* (Dec.8, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A782%3AFIN&qid=1639141440697

[24] EU, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation (“Prüm II”), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and*

indicates that LEAs might exchange facial images with one another, also Article 22 enables such authorities to conduct automated searching.

Therefore, we consider that Annex I should add a section questioning and your recommendations about the interoperability of the databases used and the data exchanges between different LEAs (if any).

Annex III – the deployment scenarios

The deployment scenarios proposed in Annex III will be of great use to LEAs. Further, we acknowledge the EDPB's recourse that any change in circumstances regarding the situations described might entail a change in whether FRT's use is necessary and proportional. We consider these scenarios might confuse LEAs to think that such situations or similar ones, might automatically allow for FRT use. However, as the doctrine of proportionality argues, when less restrictive means are available to achieve the same purpose, they should be used. This might be the case in most of these scenarios when LE agents can perform such activities. Even when this could entail more effort from an economic or logistical perspective, the impact that biometric data processing by FRT entails for the data subjects should not be overlooked. Therefore, we believe that stronger warnings should be placed at the beginning of Annex III discouraging the use of FRT when less restrictive means are available. As an example, the use of Clearview AI FRT software by LE authorities have been widely banned and economically sanctioned by DPAs all over the EU.[25]

The *Ligue des droits humains* Judgement and Artificial Intelligence

Finally, the Court of Justice of the European Union has recently ruled, in a case concerning the Passenger Name Records Directive, that machine learning techniques may be incompatible with the protection of fundamental rights.[26] The Court observed that the opacity of artificial intelligence might make it impossible to understand the reason why a given program

2019/818 of the European Parliament and of the Council (Dec.8, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0784&from=EN

[25] A big success for Homo Digitalis: The Hellenic DPA fines CLEARVIEW AI with €20 million (Jul. 13, 2022) https://www.homodigitalis.gr/en/posts/12155; To Ban Biometric Mass Surveillance European Citizen Initiative Statement of The Center for AI and Digital Policy (CAIDP) (Mar. 3, 2021) https://www.caidp.org/statements/

[26] CJEU - C-817/19 - Ligue des droits humains v. Conseil des Ministres, Judgement, 21 June 2022, https://curia.europa.eu/juris/document/document.jsf?text=&docid=261282&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=335316

arrived at a positive match'.[27] As the Advocate General had earlier observed, 'algorithms 'must function transparently and that the result of their application must be traceable'.[28] The Court added in *Ligue des droits humains* that the use of pre-determined criteria also precludes the use of systems that modify 'the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria.'[29]

These holdings could have far-reaching significance for the use of Artificial Intelligence (AI) techniques by law enforcement agencies, and the EU AI Act now under consideration.[30] We hope you will take the *Ligue des droits humains* judgement into account as you consider the use of new technologies by law enforcement agencies and make recommendations regarding AI techniques.

Conclusion

Thank you for your consideration of our views. We would welcome the opportunity to discuss these recommendations with you.

Sincerely yours,

Marc Rotenberg
CAIDP President

Merve Hickok
CAIDP Chair

Tamar Kankava
CAIDP Research Fellow

Natalia Menendez
CAIDP Research Fellow

[27] CJEU - C-817/19 - Ligue des droits humains v. Conseil des Ministres, Opinion, 21 June 2022, par. 194,

[28] Judgement, par. 228.

[29] Judgement, par. 194.

[30] Marc Rotenberg, *CJEU PNR Decision Unplugs the "Black Box",* European Date Protection Law Review (forthcoming)