Access Now submission to the consultation on the European Data Protection Board's guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement

27 JUNE 2022

I. INTRODUCTION

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

Access Now has worked extensively on data protection and related topics in the European Union, and has engaged throughout the EU's discussions on artificial intelligence (AI). Access Now's Europe Advocacy Director, Fanny Hidvegi, was a member of the European Commission's High Level Expert Group on Artificial Intelligence.[1]

With the increasing investment in and proliferation of automation-based technologies, the EU must enforce and develop the highest human rights standards for artificial intelligence systems that are designed, developed, or deployed in the European Union.

In the context of the European Commission's *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence* (hereafter AI Act), Access Now has co-led a coalition of civil society organisations to advocate for increased protections for fundamental rights in the AI Act, notably publishing a joint statement, *An EU Artificial Intelligence Act for Fundamental Rights*, which was signed by over 120 civil society organisations. We have also co-led on the drafting of four 'issue papers' on biometric technologies in the AI Act: on prohibiting remote biometric identification (RBI) in publicly accessible spaces, on prohibiting emotion recognition, on prohibiting biometric categorisation in publicly accessible spaces as well as inherently discriminatory forms of biometric categorisation, as well as a paper on other biometric technologies in the AI Act. We

[1] https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

have also co-drafted a paper on the use of AI technologies in the migration context, which also tackles the use of biometric technologies.

Access Now welcomes the strong stance of the EDPB on the issue of facial recognition technologies, and biometrics in general, which has given strong support to the positions advocated for by our civil society coalition. Particularly in the *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)* (hereafter, the Joint Opinion) of the EDPB and the European Data Protection Supervisor, and here again in the *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* (hereafter, the Guidelines).

With our response to the consultation, we wish primarily to show our support for the strong stance taken in defence of fundamental rights in the context of biometric recognition systems, as well as to make a number of suggestions for how the Guidelines could be strengthened and to clarify a number of technical and terminological issues.

II. POSITIVE NOTES ON THE GUIDELINES

In this first section of our response, we will highlight the huge amount of important and positive statements made in the Guidelines. Overall, the strong stance taken in the Guidelines is hugely important to raise awareness of the profoundly negative impact that the use of facial recognition (FRT) and other biometric technologies can have on fundamental rights.

Foremost among the positive points in this regard is paragraph 104's reiteration of the call for prohibitions from the Joint Statement. Paragraph 104 calls for bans on four uses of AI:

1. "remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into individuals' private lives and does not have a place in a democratic society as by their nature it entails mass surveillance."
    - Access Now, EDRi, and other civil society organisations have called for such a ban in the following issue paper: https://edri.org/wp-content/uploads/2022/05/Prohibit-RBI-in-publicly-accessible-spaces-Civil-Society-Amendments-AI-Act-FINAL.pdf
2. "AI-supported facial recognition systems categorising individuals based on their biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation as not compatible with the Charter."
    - Access Now, EDRi, and other civil society organisations have called for such a ban in the following issue paper: https://www.accessnow.org/AIAct-biometric-categorisation
    - In this issue paper, we have further called for a ban on all forms of biometric categorisation in publicly accessible spaces, due to the extreme potential for discrimination.
3. "the use of facial recognition or similar technologies, to infer emotions of a natural person is highly undesirable and should be prohibited, possibly with few duly justified exceptions."

- Access Now, EDRi, and other civil society organisations have called for such a ban in the following issue paper: https://www.accessnow.org/AIAct-emotion-recognition
- Regarding the issue of exceptions, we have laid out criteria that any such exception would have to fulfil, but based on our research, we have found no proposed use of emotion recognition that would justify an exception, and therefore call for a full ban.

4. "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, e.g. by "scraping" photographs and facial pictures accessible online, in particular those made available via social networks, would, as such, not meet the strict necessity requirement provided for by Union law."
    - Access Now, EDRi, and other civil society organisations have called for such a ban in the following issue paper: https://edri.org/wp-content/uploads/2022/05/Prohibit-RBI-in-publicly-accessible-spaces-Civil-Society-Amendments-AI-Act-FINAL.pdf

Beyond the call for bans, it is of key importance that the Guidelines highlight not only how the use of FRT by law enforcement authorities (LEAs) can affect our rights, both individually and collectively, but how it can negatively impact the essence of our democracies. In paragraph 3, the Guidelines note how the use of FRT "will also have considerable effects on the way we live together and on our social and democratic political stability, valuing the high significance of pluralism and political opposition." In January 2021, we joined over 60 civil society organisations in calling for red lines on uses of AI that are incompatible with a democratic society, including the use of remote biometric identification technologies in publicly accessible spaces. For technologies that threaten the essence of our rights, or which are incompatible with the foundations of democratic society, a prohibition is the only option. We therefore welcome the Guidelines' strong stance in support of this.

As noted in the Ban Biometric Surveillance (#banBS) letter, which was signed by over 190 civil society organisations from over 60 different countries, the existence of facial recognition and other remote biometric recognition tools in the hands of LEAs and other actors "will always create incentives for function creep and increased surveillance of public spaces, placing a chilling effect on free expression." It is therefore encouraging to see the emphasis on the chilling effect these technologies can cause throughout the Guidelines, including in paragraph 36, which states that:

> *it is also not inconceivable that the collection, analysis and further processing of the biometric (facial) data in question might have an effect on the way that people feel free to act even if the act would be fully within the remits of a free and open society*

This paragraph importantly stresses that the presence, and possible operation of these technologies in our public spaces, may undermine people's willingness and freedom to act in entirely legitimate ways in public spaces, for fear of being tracked, profiled and surveilled.

Moreover, because these technologies can process people's biometric data without their knowledge, they pose a particular threat and are even more prone to causing a chilling effect, as noted in paragraph 59:

Furthermore, it has to be considered as a matter of severity, that if the data is systematically processed without the knowledge of the data subjects, it is likely to generate a general conception of constant surveillance. This may lead to chilling effects in regard of some or all of the fundamental rights concerned

In this regard, the practical example made in Scenario 5 in Annex I importantly raises the many fundamental rights implications of remote biometric identification in public spaces. As the example outlines, 'the bar for necessity and proportionality becomes higher the deeper the interference', and the use of this system does not meet such threshold:

- "*The aforementioned scenarios concerning remote processing of biometric data in public spaces for identification purposes fail to strike a fair balance between the competing private and public interests, thus constituting a disproportionate interference with the data subject's rights under Articles 7 and 8 of the Charter.*"

This is especially salient today, given the roll back of rights in certain countries, even within the EU, where rights to access abortion services, and even the basic rights of LGBTQ+ people, are under attack. FRT, and particularly so-called 'post' or 'retroactive' FRT, gives LEAs and other actors the capability to search for people retroactively in CCTV or other video footage to track their movements. This can be used to persecute people who are discovered to have accessed abortion services, to track the movements of LGBTQ+ people, or even to uncover a journalist's sources following the publication of an investigation. It is thus important to stress that the chilling effect of the use of FRT is not just associated with 'live' or 'real time' FRT, but also, if not even more so, with 'post' or 'retrospective' FRT.

The following paragraphs are therefore especially welcome for highlighting the dangers of post/retrospective FRT:

- Paragraph 15 importantly stresses the danger of integrating FRT capabilities in existing infrastructure:
    - "*Unlike video capture and processing systems, for example, which require the installation of physical devices, facial recognition is a software functionality which can be implemented within existing systems (cameras, image databases, etc.). Such functionality can therefore be connected or interfaced with a multitude of systems, and combined with other functionalities. Such integration into an already existing infrastructure requires specific attention because it comes with inherent risks due to the fact that the facial recognition technology could be frictionless and easily hidden*."
- Paragraph 22 importantly highlights how post/retrospective FRT could be used to track the movements of people, such as journalists, LGBTQ+ people, or those who have accessed abortion services:
    - "*reconstructing a person's journey and their subsequent interactions with other persons, through a delayed comparison of the same elements in a bid to identify their contacts for example*"
- Paragraph 25 importantly notes that "ex post use of facial recognition technology is not per se safer and that this use also poses specific risks which have to be assessed on a case-by-case basis"

- Paragraph 84 also notes that it is particularly difficult in the case of post/retrospective FRT for the LEA to notify the data subject at the time of collection of their data:
    - "*It is particularly challenging if a LEA is analysing through FRT video material that derives from or is provided by a third party since there is little possibility, and most of the time none, for the LEA to notify the data subject at the time of collection (e.g. via a sign on-site).*"
- And Scenario 3 (Annex I) importantly showcases how the use of post/retrospective FRT lacks an appropriate legal framework and does not meet the necessity and proportionality requirements:
    - "*even if there was a sufficient legal base, the necessity and proportionality requirements would not be met, thus resulting in a disproportionate interference with the data subject's rights to respect for private life and the protection of personal data under the Charter.*"

A further point which Access Now welcomes is the confirmation that the processing of biometric data in the context of FRT usage represents **a serious interference with a person's rights even when the match is negative**. Again and again we hear the argument from those developing and deploying FRT that no interference occurs with a person's rights if there is a negative match, because their data is not retained in such cases. This is a gross misunderstanding or intentional misrepresentation both of the technical processes and of the rights we have in relation to our sensitive biometric data. As paragraph 37 notes:

> *The processing of biometric data under all circumstances constitutes a serious interference in itself. This does not depend on the outcome, e.g. a positive matching. The processing constitutes an interference even if the biometric template is immediately deleted after the matching against a police database results in a no-hit.*

When FRT is used in publicly accessible spaces, the rights of every single person who passes through that space are seriously infringed as their biometric data is collected and processed for the purpose of identification, even when the final result is a negative match. This infringement is in no way mitigated by the data being deleted after the negative match.

In the same vein, we also welcome the statement in paragraph 28 that human confirmation is not sufficient guarantee for the protection of people's rights:

> *human intervention, in assessing the results of facial recognition technology may not necessarily provide for a sufficient guarantee in respecting individuals' rights and in particular the right to the protection of personal data, considering the possible bias and error that can result from the processing itself.*

The mass surveillance of public spaces represents such a serious interference with so many of the rights of all the people who pass through those spaces, and those who avoid them due to the chilling effect, that neither human intervention nor any other legal safeguards can sufficiently mitigate that violation.

In connection with this impossibility of mitigation, it is important to highlight paragraph 63's statement regarding the necessity of foreseeability:

> *The ECHR also sets standards with regard to the way limitations [of rights] can be undertaken. One basic requirement, besides the rule of law, is foreseeability. In order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures. This requirement is acknowledged by the CJEU and EU data protection law (cf. section 3.2.1.1).*

If the use of FRT, and remote biometric identification in general, is not fully prohibited in publicly accessible spaces, it will be impossible to fulfil this requirement of foreseeability. This is because **any exceptions to the prohibition will require the infrastructure to exist so that the technology can be used in those exceptional circumstances.** A data subject will therefore always be forced to assume that the system could be turned on, in the case of live or real-time FRT, or that it could be used retroactively on CCTV or other footage, in the case of post/retrospective FRT.

Access Now also appreciates that the Guidelines emphasise that the use of FRT by LEAs must not only be necessary, but **strictly necessary**, as noted in paragraph 73:

> *The addition of the term "strictly" means that the legislator intended the processing of special categories of data to only take place under conditions even stricter than the conditions for necessity (see above, item 3.1.3.4). This requirement should be interpreted as being indispensable. It restricts the margin of appreciation permitted to the law enforcement authority in the necessity test to an absolute minimum.*

Given the proliferation of companies which have amassed extensive databases of people's biometric data by indiscriminately scraping the web, we welcome the clarification in paragraphs 74, 75, and 76 regarding the meaning of 'manifestly made public':

- Paragraph 74 importantly highlights that even if a photograph has been manifestly made public, this does not imply that the biometric data which can be extracted from that photograph has been manifestly made public: "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."
- Paragraph 76 also makes the important point that simply neglecting to activate certain privacy features on the part of the data subject is also not sufficient grounds to consider that their data has been manifestly made public: "the fact that the data subject did not trigger or set specific privacy features is not sufficient to consider that this data subject has manifestly made public its personal data and that this data (e.g. photographs) can be processed into biometric templates and used for identification purposes without the data subject's consent."

We also welcome the practical example made in Scenario 6 of Annex I, where it is clarified that there is no applicable legal framework that would allow a private entity to provide law enforcement authorities with a database storing personal data collected in an unlimited and mass-scale way :

- *"The lack of clear, precise and foreseeable rules that meet the requirements in Article 4 and 10 of the [LED] Directive, and the lack of evidence that this processing is strictly necessary in order to achieve the intended objectives, leads to the conclusion that the use of this application would not meet the necessity and proportionality requirements and would mean a disproportionate interference of data subjects' rights to respect for private life and the protection of personal data under the Charter*."

Finally, we wish to express our strong support for the clarification in paragraph 96 that before any use of FRT, a Data Protection Impact Assessment is required and that it should be made publicly available:

> *A data protection impact assessment (DPIA) before the use of FRT is a mandatory requirement since the 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 EDPB recommends making public the results of such assessments, or at least the main findings and conclusions of the DPIA, as a trust and transparency enhancing measure.*

Access Now believes that any such use of an inherently high risk technology like this which processes personal data should not only require a DPIA to be carried out, but that the full DPIA should be made publicly available, particularly when the technology is being used by a public authority.

III. DEFINITIONAL AND OTHER ISSUES IN THE GUIDELINES

While Access Now overwhelmingly supports the recommendation made in the Guidelines, we do wish to highlight a definitional issue in paragraphs 10 to 15, which we believe can lead to serious confusion and problems in assessing the impact of uses of FRT. Paragraph 10 states that FRT can fulfil two distinct functions, on the one hand, authentication, on the one hand, identification. It is also stated that authentication is the same as verification. Unfortunately, this is not an accurate use of terminology.

Rather, an FRT system can do two things: verify a person's identity, or identify someone. Both of these can then be used for the purpose of authentication. So, rather than authentication and verification being the same thing, in reality both verification and identification can be used for the purpose of authentication.

For example, the following example of FRT for identification given in paragraph 22 is actually an example of **identification used for authentication:**

> *access to services, with some cash dispensers recognising their customers, by comparing a face captured by a camera with the database of facial images held by the bank*

In the above example, the person's face is compared against a database of images, so we have a 1-many identification process, but this identification process is **done for the purpose of authenticating that person's identity**. However, unlike a 1-1 form of verification for the purpose of authentication, if performed remotely, this use case involves all the risks associated with remote biometric identification as it will necessarily scan the faces, and process the biometric data, of all

people who present themselves at the terminal. Moreover, such an application also necessitates the centralised storage of a reference database, which again increases the level of risk, as such a database would be at risk of hacking, misuse, or other forms of illegitimate access.

Verification, authentication and identification[2]

In most cases, the Guidelines use the terms "authenticate"/"authentication" and "identify"/"identification" to differentiate between the two main forms of biometric processing (e.g. Section 2.1, para 10, p.7; Section 2.1, para 12, p.8; and many other places throughout the document). In para 10 of section 2.1, authentication is described as a synonym for verification, and at various other points, the terms "verification" and "authentication" are used interchangeably.

Whilst there is still discussion within the technical community about the most correct use of these terms, there is generally a view that authentication is not the same as verification. Biometric authentication is a function of a person claiming an identity the basis of their biometric feature(s). It is usually done via verification, and the purpose of verification is to authenticate one's self.

However, it is also possible for authentication to be performed via a certain method of identification. That particular method is called 'closed-set' identification (as opposed to 'open-set' identification). Closed-set identification uses a pre-determined database of (usually) pre-enrolled persons and performs its analysis by asking "who in this database are you"? Open-set identification, however, compares a person, often without their knowledge, to a database, and asks "Are you in this database? If so, who are you?"

This distinction is important not just for technical reasons but, as we will discuss, also for fundamental rights reasons. The conflation of authentication and verification is thus problematic, and these Guidelines provide a great opportunity for the EDPB to authoritatively address this issue and ensure common terminology across the EU. This seems to be consistent with the Guidelines' approach to actual use cases, as paragraph 22 (examples of facial recognition identification) include both open- and closed-set examples; and the use cases in paragraphs 19, 20 and 21 accurately describe verification use cases.

How to address this in the Guidelines:

The definition of authentication (first bullet point of paragraph 10, section 2.1, page 7) describes verification, and should be corrected instead to be called "verification". And the definition of identification (second bullet point of paragraph 10, section 2.1, page 7) describes open-set identification specifically, which should be indicated.

It would be helpful, further, to add in an additional definition for closed-set identification, or at least to mention the two methods of identification in the definition. Whilst both open and closed-set methods are forms of identification (meaning largely 1:n, and relying on a database), closed-set identification can be used for authentication functionalities, whereas open-set identification cannot. And whilst authentication is a functionality of closed-set biometric identification, it is not its only functionality.

[2] This and the following section were contributed by Ella Jakubowska, policy officer at European Digital Rights

Furthermore, the term 'authenticate' is sometimes used by industry when trying to avoid explicitly mentioning (closed-set) biometric identification. For example, many biometrics providers describe the process of enrollment in a biometric system (for example by pre-enrolling the biometric features from your passport) as 'verification' and then the subsequent closed-set identifications against a central database as 'authentication' (despite the fact that this is closed-set identification).

We suspect that, because of the general public sentiment that biometric verification is mostly acceptable (e.g. because of the high acceptance of the use of biometric features to unlock one's smart phone) and that identification is more risky, it is thus commercially and reputationally advantageous for companies rolling out closed-set biometric identification systems to use terms like "authentication". Such terms connote verification, and therefore may appear to be safer / less controversial. By conflating authentication and verification, the EDPB Guidelines thus risk inadvertently providing cover to those companies. Conversely, clarifying the difference between authentication and verification will help ensure properly-informed debates on these issues. The term authentication can be used alongside verification to describe its function, but never as a perfect equivalence.

For example, a person identifying themselves via an ePassport gate would be a classic example of biometric verification. However, increasingly we see airlines, train operators and others using closed-set identification for the function of "authenticating" passengers via pre-enrollment so that they can undertake 'paperless', 'touchless' or 'seamless' travel.[3] If this is done via, for example, wall-mounted or ceiling-mounted cameras (instead of individual kiosks) that check all travellers entering a space to see if they have pre-enrolled (e.g. at the 2020 Roland Garros tennis tournament), such a use case would then be *remote* (closed-set) biometric identification.

Many of the issues raised by remote (open-set) biometric identification – like the use of facial recognition against protesters in a public square – are thus present. For example, non-enrolled people could have their biometric data processed without their knowledge; consent might not be properly informed; private companies would hold large amounts of people's sensitive biometric data as a result of the pre-enrollment; serious risks to fundamental rights to privacy, dignity, data protection and a chilling effect could arise, and so forth.

Furthermore, Section 2.1, paragraph 17 (p.9) could also assist this clarification by further explaining the issue, and highlighting the risks that arise when closed-set identification is used in ways that make people think it is verification. Finally, the use of the word "authentication" needs to be corrected to "verification" throughout the Guidelines, particularly in Section 2.2, paragraphs 19 – 21 (p. 9). Paragraph 21, in particular, describes a scenario which is increasingly being performed by (non-remote) closed-set biometric identification (e.g. the Eurostar example) and so it should be clarified that such a use case must always rely on the identity document and not on pre-enrollment.

[3] Whilst it is often said that such use cases are acceptable as long as they are GDPR/LED complaint, the increasing commodification of biometric identity is a serious challenge that has not yet been properly interrogated within EU policymaking. As such, we believe that many existing / pilot uses of closed-set biometric identification, for example for travel authentication, do not comply with the GDPR even though they are not remote (e.g. because they use kiosks). In particular, the example given in the Guidelines of 'tracking of a person's journey'(p.10) is, in our opinion, hard to consider necessary given that it aims to remove all opportunities for meaningful consent.

Note: we support the implict definitions established in Annex I which define data capture as either 'remote' or 'in a booth or controlled environment' (p.27). This seems to complement the understanding of how RBI can be either remotely or non-remotely and – in the case of closed-set identification, impermissible when it is conducted remotely.

Other definitional issues:
Furthermore, paragraph 14 states that facial detection and facial analysis, including emotion recognition, are not types of facial recognition. This goes against the common use of the term facial recognition as an umbrella term for a range of processes, including detection, verification, identification and analysis/categorisation/classification. Arbitrarily excluding detection and analysis from the term facial recognition will only give credence to the problematic line often taken by industry that when they are performing facial analysis, for example, they are "not doing facial recognition."

Finally, we would like to highlight an issue with the practical example outlined in Scenario 1, of Annex I. This first case refers to the use of a FRT verification system in the context of Automated Border Control (ABC) system for the purpose of authenticating the biometric image stored in a travel document and establishing the passenger is the right holder of the document. While the use of biometric verification systems in the context of document controls could be considered proportionate and covered by existing legislation, paragraph 1.1 of Scenario 1 also foresees the possibility to compare the biometric data stored in the travel document against law enforcement databases:

- *"Under specific circumstances, the biometric data can be also used to search for matches in law enforcement databases (in such a case 1-many identification would be performed in this step).*"

If the biometric data of the individual is processed for the purpose of identifying known suspects, the FRT practice totally differs from the verification procedure made for authentication. Therefore, the two cases should be considered separately and a different analysis on the applicable legal framework should take place, as different conclusions would occur.

In fact, the use of a FRT identification system for the processing of biometric data of all travellers raises serious concerns regarding the necessity and proportionality of the mesure. Similar concerns have already been raised in the context of the Passenger Name Directive, which allows the automated processing of alphanumeric data against law enforcement databases. Given the sensitivity of biometric data, the use of FRT identification system risks undermining several fundamental rights, such as the right to free movement, to non-discrimination, to asylum and it undermines the presumption of innocence.

V. ADDITIONAL RECOMMENDATIONS

Access Now welcomes the statement in paragraph 97 that recommends that authorities deploying FRT should consult with the competent supervisory authority prior to deployment. However, we recommend that this be strengthened to an obligation to consult, given the serious infringement of rights, and threat to democratic society, that such technologies pose.

Finally, Access Now recommends that the Guidelines include a section about the impact of spyware technology on the rights to privacy and data protection. While the capabilities of modern spyware go beyond facial recognition and other biometric technologies, their combination further exacerbates potential and existing human rights violations that are unacceptable in a democratic society. Therefore, Access Now calls for a moratorium limiting the sale, transfer, and use of abusive spyware until people's rights are safeguarded under international human rights law. In situations when such safeguards or remedies can not sufficiently mitigate these violations - such as in the case of Pegasus - a ban is necessary. As paragraph 45 points out

> *The limitations of the fundamental rights imminent to each situation still have to provide for the essence of the particular right to be respected. The essence refers to the very core of the relevant fundamental right. Human dignity has to be respected too, even where a right is restricted*

We support the European Data Protection Supervisor's Preliminary Remarks on Modern Spyware and we call on national data protection authorities and the EDPB to take a strong stance against spyware technology to ensure not only the fundamental rights to privacy and data protection but also the basic principles of a democratic society.

For any questions or to connect with us about our work please contact Daniel Leufer, Senior Policy Analyst, daniel.leufer@accessnow.org and Caterina Rodelli, Policy Analyst, caterina@accessnow.org