EDRi submission – EDPB Public Consultation on Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement – 27 June 2022

1.0 Background

European Digital Rights (EDRi) is a dynamic and resilient collective of 57+ NGOs, as well as experts, advocates and academics working to defend and advance digital rights across the continent. For almost two decades, EDRi has served as the backbone of the digital rights movement in Europe.

In 2020, EDRi published the position paper 'Ban Biometric Mass Surveillance' where we called for, *inter alia*, law enforcement uses of "untargeted biometric processing systems" to be fully prohibited in EU law. This was based on our fundamental rights assessment, which found that such use "unjustifiably infringes on fundamental rights including privacy, data protection, equality, freedom of expression and information, freedom of assembly and association, due process and more" and that such practices are intrinsically unnecessary and disproportionate.

Since then, our position has evolved. In terms of application to the EU's Artificial Intelligence Act 2021/0106(COD), our call to Ban Biometric Mass Surveillance means that we urge the following additional rules to address the particular effects that arise in the context of the use of AI:

- A full prohibition – without exceptions – on Remote Biometric Identification (RBI) in publicly-accessible spaces, by all actors, regardless of whether it is conducted in an ex post (retrospective) or real-time (live) manner;
- A prohibition on biometric categorisation where it may lead to discrimination, for example on the basis of gender, ethnicity, age, sexual orientation, other protected characteristics, and their proxies;
- A prohibition on biometric categorisation where it may lead to manipulation, for example for the function of profiling people in public spaces for targeting advertisements;
- A prohibition on emotion recognition;
- Adjustments to Annex III of the AI Act to fully capture the wide range of uses and practices that cause a high risk of harm to fundamental rights, and to better align to EU data protection acquis.

This does not mean that uses of biometric systems outside of what we list above are de facto permissible or acceptable. Particularly in the context of law enforcement, we reassert the risks of any biometric processing are severe. We thus call for the continued adherence to the Data Protection Law Enforcement Directive (LED) as well as additional EU and member state guidance and case law to further clarify impermissible uses of biometric systems, and for citizen and resident mobilisation, strategic litigation, continued policy work, and other actions for the protection of fundamental rights.

In particular, we have been disappointed in EU Member States that have – sometimes repeatedly – deployed biometric systems in contradiction to the LED, its national interpretations, and the EU Charter of Fundamental Rights ("the Charter"), for example France and Italy. We reiterate that the LED remains the key instrument, for protecting people's biometric data from rights violations by law enforcement.

2.0 Our assessment of the Guidelines

2.1 EDRi welcomes these Guidelines:

EDRi welcomes the EDPB's draft Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, and we are grateful for the opportunity to provide feedback to help further strengthen these guidelines. Members of the EDRi network have worked on issues relating to the use of biometric data for decades, and in 2020, we called for additional EU-level guidance for member states about uses of biometric systems in our 'Ban Biometric Mass Surveillance' paper. We therefore find these Guidelines to be a necessary and positive development.

2.2 Fundamental rights approach:

In particular, we are very supportive of the EDPB's explicit recognition that "**FRT is prone to interfere with fundamental rights – also beyond the right to protection of personal data – and is able to affect our social and democratic political stability**" (p.3) as well as that "**The processing of biometric data under all circumstances constitutes a serious interference in itself**" (para 37, p.12). We further support the detailed elaboration of the risks in Section 1 (Introduction) paragraphs 2 and 3, as well as throughout Section 3 (General legal framework).

In particular, the analysis of the ability of FRT systems to make intrusive conclusions about people's private lives (para 35, p. 12) and the acknowledgment of the risk of police offers abusing biometric data (para. 36) are very commendable. What's more, the engagement with the fact that turning people's faces into biometric templates can constitute "objectifying the face" and therefore may infringe on the right to dignity, including to "not [be] treated as mere objects" (Section 3.1, para 40, p.13), is something that EDRi thinks is very important. We are very grateful for the EDPB recognising this important but often under-acknowledged risk of potentially all forms of biometric processing.

The EDPB's reassertion that processing "does not depend on the outcome, e.g. a positive matching" and that "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" (para 37, p.12) are also important. This is because several Member State law enforcement agencies have attempted to claim that their use of FRT is not 'generalised' or 'mass' because it only searches for individuals on a watch list, and/or because those found not to be on the list have their biometric data deleted near-instantaneously. For these reasons, we think that it can be helpful to think of uses such as remote biometric identification (RBI) in publicly-accessible spaces as n:n processing (because every person in that space has their features compared to the database) rather than 1:n processing.

The engagement of the Guidelines with the chilling effect of the use of FRT is equally important from a fundamental rights perspective, particularly the following:

> *"If the data is* [sic] *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 such as human dignity under Article 1 of the Charter, freedom of thought, conscience and religion under Article 10 of the Charter, freedom of expression under Article 11 of the Charter as well as freedom of assembly and association under Article 12 of the Charter."* (p.4)

We believe that such reminders are urgently needed in the EU, given the wide-ranging industry and political push towards the use of biometric data in almost every part of our societies, under the sinister guise of ‘convenience’ and ‘efficiency’. We see a powerful role for the EDPB to continue to tackle these and other dangerous myths about the use of biometric systems.

It is also positive that the Guidelines problematise the issue of human intervention (Section 2.3, para 28, p.11) and emphasise its limitations for correcting errors and mitigating risks. This section, however, would benefit from an additional paragraph (i.e. 30A) to further explain that even beyond issues of bias and discrimination in FRT systems, choices around locations of deployment as well as which individuals to search for can also facilitate both indirect and direct discrimination. **In a nutshell, EDRi suggests that technologies which are designed to surveil and punish can never be ‘fair’, as their essential purpose is in upholding existing power relations.**

As will be discussed in Recommendation 1 of this consultation response, paragraph 30 of Section 2.3 (p.11) also provides a good opportunity to add a discussion on how accuracy can only go so far. Questions raised by the ‘base rate fallacy’ could also be a necessary part of the assessment of the reliability of a system. So too should a recognition that accuracy under lab conditions is usually vastly lower than accuracy ‘in the wild’.

We welcome additionally the inclusion of the analysis of automated decision-making and profiling as salient fundamental rights concerns in the context of FRT.

Lastly on the question of fundamental rights, we welcome the implication that generalised (i.e. public) surveillance will never be justifiable, even in the search for particular suspects:

> "*It can further be inferred that with regard to data subjects for whom there is no evidence capable of 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*" (Section 3.2.3, para 79, p.20).

This is further complemented by some of the scenarios in Annex III, for example scenario 5, which explains that “Remote biometric identification is so prone to mass surveillance that there are no reliable means of restriction” (p.47). We also welcome the fact that scenarios 3 and 6 confirm, respectively, that post FRT can pose a disproportionate interference with fundamental rights and that databases scraped from the internet cannot be lawfully used.

2.3 Supporting the Law Enforcement Directive:

We are also very supportive of the nature of these guidelines in reinforcing the LED, as well as reiterating the necessity of engaging the EU Charter of Fundamental Rights when interpreting the LED. On strict necessity, we are glad to see these Guidelines help with the application of this criteria, particularly the assertion that:

> "*Processing of special categories of data, such as biometric data can only be regarded as "strictly necessary" (Art. 10 LED) if the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary, i.e. indispensable, and excluding any processing of a general or systematic nature.*" (p.4)

Generally, the Guidelines are very strong in asserting the high level of responsibility and the many obligations that Member States face should they wish to use FRT. It is thus very good that the Guidelines emphasise, for example, that under the LED, a sufficiently clear legal basis is needed, and that “A legislative measure cannot be invoked as a law authorising the processing of biometric data by means of FRT for law enforcement purposes if it is a mere transposition of the general clause in Article 10 LED. (para 71, p.18). As we have seen systemically across Europe, law enforcement agencies have frequently used FRT without a sufficient legal basis, and in many cases have duly been admonished by their respective data protection authorities. (e.g. the example of the unlawful use of FRT by police at Belgium's Zaventem airport.)

2.4 The 'manifestly public' question:

The assertion that the making public of a photograph is not the same as the making public of a biometric template in Section 3.2.1.3 is a relatively novel, and very welcome, assertion. The clarification provided in paragraphs 75 and 76 (p.19) are very useful and important for protecting the rights of data subjects in an increasingly digitalised environment. In light of several data protection authorities' decisions against Clearview AI, such rules are important in preventing the mass scraping of online sources by police or by companies on their behalf / to provide them with services.

2.5 Necessity, proportionality and safeguards:

We are strongly supportive of the assertion that "An objective of general interest – however fundamental it may be – does not, in itself, justify a limitation to a fundamental right" (p.15). The additional clarification of *strict* necessity meaning absolute necessity is further welcomed (para 51, p.15 and para 57, p.16) and so too is the reinforcement that national authorising laws need to establish "substantive and procedural conditions and objective criteria" for any processing (para 55, p.16).

The Guidelines do an excellent job of providing a thorough and detailed assessment of the serious risks of law enforcement use of FRT, as well as the many criteria that must be met in order for a use to be considered lawful and legitimate. It would be even better if the Guidelines gave an authoritative and explicit assessment of the times in which these safeguards, established by a national legal basis, intrinsically cannot protect people from the severe risks. This is already very strongly indicated by the various comments on RBI (e.g. paragraphs 102 and 103).

Annex I of the Guidelines (Template for description of scenarios) would benefit from an additional section containing questions which enable LEAs to particularise the question of 'absolute necessity' in order to justify that they have exhaustively reviewed alternatives to prove that the necessity is absolute. Currently this is missing from the section (p.28) called 'necessity and proportionality analysis' which implies a lower threshold than being indispensable. This correction should also be reflected in Annex II, section 2 (pp.31-32).

2.6 Data Protection Impact Assessments:

The reinforcement of the obligation to conduct a DPIA (Section 3.2.5.1) is positive. It could be complemented with a suggestion for controllers to undertake a full Fundamental Rights Impact Assessment (FRIA) which would also include elements such as environmental impact, as per civil society's recommendations for high-risk AI systems.

This may also be necessitated by the limited engagement with fundamental rights in Annex I (p.27) which would benefit for a more thorough and informed analysis of fundamental rights risks, supported by independent figures with expertise in fundamental rights. The form in Annex I (p.27) would also benefit from an additional category to acknowledge that indirect outcomes can also impact upon fundamental rights.

We would suggest further that the full publishing of the *full* DPIA and FRIA are "strongly recommended" by the EDPB.

2.7 Prior consultation:

The reinforcement of the need for prior consultation with the supervisory authority (i.e. DPA) (Section 3.2.5.2) is positive. As emphasised by Algorithm Watch, it would be even better if such consultations were also recommended with civil society, equality authorities and groups and impacted communities. Such recommendations could be codified in the process outlined in Annex II, ideally as a central part of sections 2, 3 and 4 (pp.30-34).

2.8 External providers:

The engagement with the risks posed by the use of external FRT products / services are positive. There could be an opportunity to expand on the need for a reform of procurement procedures as well as a reiteration that certain providers (e.g. providers of private biometric databases) should never be allowed by law enforcement.

2.9 Reinforcing the call for a ban:

We are very glad to see the EDPB's continued commitment to red lines against unacceptably harmful uses of biometric systems:

> *"There are certain use cases of facial recognition technologies, which pose unacceptably high risks to individuals and society ('red lines'). For these reasons the EDPB and the EDPS have called for their general ban"* (para 103, p.26).

To even further address the risks of technsolutionism, paragraph 102 (p.26) could further clarify that "Moreover, while modern technologies may be part of the solution, they are by no means a "silver bullet" **and in some cases will be ineffective, counterproductive and harmful**" (text in bold is suggested as the addition here).

3.0 Additional recommendations to further strengthen the Guidelines

3.1 Recommendation 1: Refine the terminology used

It is very positive that the EDPB Guidelines immediately state that biometric recognition is a 'probabilistic technology' (Section 2.1, para 6, p.7) and then again that any match is only an "estimated match" (para 11). This could be even further supported by an explicit clarification of the implications of this assertion, namely that it means that FRT and other biometric recognition technologies never provide a conclusive/definitive result. A discussion of the phenomenon of the 'base rate fallacy' would also be especially useful here to demonstrate that even at the highest levels of accuracy, biometric recognition technologies will always suffer from false positives and false negatives.

3.1.1 Clarifying authentication:

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.

3.1.2 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.

Furthermore, our research has indicated that 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.[1] If this is done via, for example, wall-mounted or ceiling-mounted cameras (instead of individual kiosks) that check all travelers 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.

Note: we support the implicit 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 EDRi's 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

3.2 Recommendation 2: encourage the use of alternatives to FRT

Given that biometric data are rightly recognised in the EU data protection framework as very sensitive, we would encourage the guidelines to go further in specifically recommending that law enforcement pursue alternative solutions to effectively fighting crime without disproportionately infringing on fundamental rights.

Section 3.1.2.2 (Strict Necessity) could be a good place to specifically explore and encourage the pursuit of feasible alternatives to FRT. This would be based along the lines of "what is absolutely necessary" (para 73, p.19) and could emphasise that alternative policing and social methods should be prioritised over the use of FRT. In particular, it might help law enforcement agencies to better understand what is meant by biometric processing being allowed only if it is "indispensable" (paragraph 73, p.19). This is an incredibly important facet that seems to be frequently misunderstood or ignored by law enforcement agencies. By making clear not only that alternatives can be pursued, but what those alternatives, which would minimise or eliminate the processing of biometric data, could look like, would be a powerful step towards protecting people from FRT in the EU.

It would be great if the Guidelines could also explicitly say that there are clearly some practices which effect the essence of fundamental rights to such a degree that they can never be

[1] 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.

legislated for nationally This is already hinted at strongly by the use of "*if* it can" (e.g. "The controller must carefully consider how to (or if it can) meet the requirements for data subject's rights before any FRT processing is launched " para 83, p.21).

3.3 Recommendation 3: expand beyond faces

It is not clear why the Guidelines have chosen to focus on facial recognition technology only, rather than including recommendations for other type of biometric recognition technology, for example on the basis of gait, which can pose equivalent risks and harms. We therefore encourage the EDPB to broaden the guidelines to apply to all forms of biometric data.

3.4 Recommendation 4: include emotion recognition and other harmful forms of processing even if they do not uniquely identify people

Section 2.1, paragraph 15 (p.8) engages with human feature detection as well as emotion recognition, but does not go far enough to properly interrogate the fundamental rights risks of these practices. The concluding paragraph (para 104, p.26) then points to the need for a general ban on emotion recognition. This would be useful to treat earlier in the Guidelines.

We also support Access Now's recommendation that the Guidelines consider emotion recognition, human feature recognition and other forms of biometric categorisation under the umbrella term of 'facial recognition'.

3.5 Recommendation 5: strengthen the fundamental rights and data protection elements (summary of recommendations from the first section of this paper

As discussed at length in the section of this paper called '**Our assessment of the Guidelines**' (Section 2.0), we believe the already strong Guidelines could benefit from:

- DPIAs being accompanied by FRIAs;
- Prior consultations including civil society and impacted groups;
- Transparency of full (not summary) DPIAs and FRIAs;
- Acknowledgment of discrimination in the deployment of FRT;
- Discussion of the base rate fallacy;
- Specific recommendation against the use of private databases by LEA; and
- Further critique of technosolutionism and the problems that it can create.

Lastly, we briefly discuss some issues that have not been dealt with elsewhere in our response:

- Although the risks of 'traditional' CCTV cameras being 'converted' into FRT has been covered in the Guidelines, we would welcome additional EDPB Guidelines to connect the issues of FRT to wider issues of infrastructures and enablement of harmful practices. In particular, harmonised rules for national police databases could increase the protection of people's sensitive biometric data;
- Ditto issues of export;
- The Guidelines could perhaps also engage with issues of how FRT can pose obstacles for justice; for example, a 2019 case at the court of Zeeland-West-Brabant in the Netherlands fell apart because it was based solely on a facial recognition match;
- We recommend that paragraph 25 (section 2.3, p.25) explicitly recognises that not only does post FRT come with serious risks, but that in some cases, these risks may be even more pronounced than live FRT given the potential of such systems to track people

across time and place. This can be especially dangerous for human rights defenders, political dissidents, journalists, people seeking healthcare, and many more;

- The issue of spoofing in paragraph 26 (pp.10-11) could be specifically noted as a criteriato consider when assessing necessity, both in the Guidelines, and in Annex I. This is because if those that are being sought (i.e. criminals) are those most likely to be able to spoof FRT systems, this concern should be taken into account;
- Paragraph 16 (Section 2.2, p.8) makes an ambigous comment about FRT being used for law enforcement beyond the scope of the Law Enforcement Directive. It is not clear what this refers to, nor how it would be legal'
- Like Access Now, we have strong concerns about scenario 6 of Annex III, as it conflates the mass biometric searches of travelers with automated biometric verification of a person against their identity document. We therefore strongly suggest that these two separate use cases are treated separately, and a new analysis undertaken.

For questions, please contact **Ella Jakubowska, Policy Advisor at EDRi** (ella.jakubowska@edri.org). With many thanks to EDRi members who have been instrumental in developing the policy position on which this submission relies.