Prohibit all Remote Biometric Identification (RBI) in publicly accessible spaces

What is Remote Biometric Identification (RBI)?

Nota bene: *biometric identification is the technical process of identifying one person among many, on the basis of their biometric data (as defined in GDPR article 4.14). This is different from biometric verification, which uses someone's biometric data to confirm that they match specific biometric data which have been stored locally, under their control. An example of biometric verification would be unlocking your mobile phone by comparing your fingerprint to the fingerprint template you created when you set up your device. Another would be going through an ePassport gate by comparing your face to the face template contained within the chip of your biometric passport. Both such examples would be excluded from the scope of this recommendation, because they do not constitute biometric identification.*

Remote biometric identification means **the use of an AI system to identify a person using their uniquely-identifiable biometric data, at a distance that is far enough that (i) there is the possibility that they may not know it is happening and that (ii) there is a possibility that others in the space may also have their biometric data captured.**

RBI works by making a comparison between a person in a surveillance feed (via a biometric template) against a reference database/watch-list, to see if there is a match.

Examples of RBI include the use of facial recognition cameras in supermarkets or the application of facial recognition algorithms to CCTV footage of a public space by police. The first example is "real-time" RBI because the analysis happens live (while people are walking around the supermarket). The latter example is "post" RBI because the analysis happens retrospectively, at any point later. This distinction is largely technical, as **both real-time and post modes of RBI can unduly infringe on people's fundamental rights in equally profound ways.** Instead, it is the remoteness (as per the above definition) that exacerbates the fundamental rights risks of such uses. As a recent European Parliamentary Research Service report confirms, the "pervasive tracking of individuals in public spaces" remains "a major interference" with people's rights regardless of whether it is real-time or post. In fact, the extra time entailed by "post" processing uses, which is often claimed to mitigate the risks, has in fact been shown to exacerbate them.

Whilst facial recognition is probably the most common type of RBI, RBI can also be performed using other types of biometric data. This is because other biometric features also have the potential to uniquely identify people, such as the way they walk (their gait), the way they type (their keystroke pattern), their ear shape and more.

This paper was co-drafted by **European Digital Rights (EDRi)**, **Access Now**, **ARTICLE19**, **Bits of Freedom**, the **Chaos Computer Club (CCC)**, **Digitale Gesellschaft CH** and the **IT-Political Association of Denmark (IT-Pol)**.
It is supported by **AlgorithmWatch**, the **European Center for Not-For-Profit Law (ECNL)**, **Fair Trials** and the **Panoptykon Foundation**. It follows the Joint Civil Society Statement 'An EU Artificial Intelligence Act for Fundamental Rights', November 2021, signed by 123 organisations.

What do we define as RBI in publicly accessible spaces?

The use of **RBI in publicly accessible spaces refers to the location in which people being surveilled may or will have their biometric data captured or processed**. For example, if cameras or sensors are installed in a street or park, the location of surveillance would clearly be a publicly accessible space. Any person in that space would have their biometric features scanned, as the use of RBI fundamentally precludes warranted, targeted use against specific individuals only. As called for by the European Data Protection Board (EDPB) and Supervisor (EDPS), the same principle must also apply in online [publicly accessible] spaces.

The notion of 'publicly accessible space' in the AI Act should include any place which any person can in theory access, even if they have to pay to do so. This includes online equivalents, privatised spaces such as airports and train stations, sports arenas and healthcare facilities, as well as spaces that are essential for access to public services. **This wide definition must be preserved**.

Will banning 'RBI in publicly accessible spaces' stop biometric mass surveillance?

People across the EU have called to "ban biometric mass surveillance". The use of RBI in publicly accessible spaces (whether real-time or post) is one of a number of ways that the use of biometric data by governments and companies has led to mass surveillance, due to the inherently disproportionate nature of this generalised surveillance.

Other uses of biometric and related data can also lead to mass surveillance and severe violations of rights and freedoms. See our related papers on **emotion recognition**, **biometric categorisation**, and how to **strictly regulate high-risk uses of biometrics in AI systems** for a comprehensive approach. EU lawmakers must also resist the expansion of underlying biometric surveillance infrastructures, for example through the proposed expansion of the Prüm (II) framework, the EURODAC Regulation, and the broader EU interoperability database infrastructure.

Why we need a prohibition on all RBI in publicly accessible spaces

Over 200 civil society groups across Europe and globally, the EDPS and EDPB, the European Parliament and the UN High Commissioner for Human Rights have all highlighted the unacceptable threat that the use of RBI in publicly accessible spaces, including online, poses to fundamental **rights to privacy, data protection, equality, non-discrimination, freedom of expression and information, peaceful assembly and association, liberty, dignity, and the presumption of innocence, as well as to basic principles of democracy, media freedom and the rule of law**.

This paper was co-drafted by **European Digital Rights (EDRi)**, **Access Now**, **ARTICLE19**, **Bits of Freedom**, the **Chaos Computer Club (CCC)**, **Digitale Gesellschaft CH** and the **IT-Political Association of Denmark (IT-Pol)**.
It is supported by **AlgorithmWatch**, the **European Center for Not-For-Profit Law (ECNL)**, **Fair Trials** and the **Panoptykon Foundation**. It follows the Joint Civil Society Statement 'An EU Artificial Intelligence Act for Fundamental Rights', November 2021, signed by 123 organisations.

RBI is designed to scan every person who appears in a surveillance feed. If the feed covers an area of publicly-accessible space, this means that every person who passes through will have their biometric data scanned. The Italian DPA has confirmed that this constitutes a form of mass surveillance, even if the data of people who are not on the watch-list are deleted quickly. That's because whether or not you are in the database, the knowledge that you may be scanned has a profound '**chilling effect**' on your rights and freedoms.

These risks and harms can apply equally strongly whether those deploying RBI systems are law enforcement agents, public authorities (such as councils or municipal governments), privatised service providers or commercial actors, and whether the processing is real-time or post. Current rules in the General Data Protection Regulation (GDPR) contain provisions which have been widely abused to conduct biometric mass surveillance, creating a huge burden on data protection authorities to try to stop these uses, and demonstrating the need for a clear prohibition at EU level. Furthermore, rules on the processing of biometric data in the Law Enforcement Directive (LED) have been circumvented at a national level, and the Directive has not yet been effectively enforced across the EU.

According to human rights expert Dr Nóra Ni Loideain, **the weak approach to prohibiting RBI in the proposed AI Act is likely in conflict with EU fundamental rights** and with CJEU case law. The worryingly-limited scope of the proposed ban fails to tackle equally harmful non-law-enforcement uses and "post" uses, threatens to undermine existing data protection rules, and makes exceptions for broad mass surveillance practices. In this way, **Article 5.1 currently provides more of a blueprint for biometric mass surveillance practices than a legal limitation.**

This paper was co-drafted by **European Digital Rights (EDRi)**, **Access Now**, **ARTICLE19**, **Bits of Freedom**, the **Chaos Computer Club (CCC)**, **Digitale Gesellschaft CH** and the **IT-Political Association of Denmark (IT-Pol)**.
It is supported by **AlgorithmWatch**, the **European Center for Not-For-Profit Law (ECNL)**, **Fair Trials** and the **Panoptykon Foundation**. It follows the Joint Civil Society Statement 'An EU Artificial Intelligence Act for Fundamental Rights', November 2021, signed by 123 organisations.

Recommendations

RBI definition

The final clause of the definition of RBI is technically flawed[1] and risks arbitrarily excluding certain forms of RBI that can equally infringe on people's fundamental rights. The term 'at a distance' is also unclear, which risks legal, commercial and technical uncertainty and potential loopholes.

The proposed Act should also keep dual-use RBI applications in its scope (Article 2(3) on military exemptions).

RBI prohibition

Once the definition of RBI has been corrected, the protection of fundamental rights necessitates that the use of RBI systems must be entirely prohibited in publicly accessible spaces. **It is critical for the protection of fundamental rights that this includes real-time and post uses by any actor.** The scope of the prohibition should also expand to the placing on the market / putting into service of products that are intended for use as RBI systems in publicly-accessible spaces, so that, for example, products intended to be used as biometric stalker-ware cannot be sold in the EU.

Additionally, two new paragraphs should be added below paragraph 1. The first will ensure that the AI Act supports the position of the European Parliament on the unlawful use of services like Clearview AI. The second will ensure that the use of biometric databases is consistent with rules on data minimisation and purpose limitation under the GDPR and LED, contrary to many current examples in the EU, and as necessitated by the Clearview AI decision from the Hamburg data protection authority.

For more information on these recommendations, please contact ella.jakubowska@edri.org and daniel.leufer@accessnow.org.

1 The flaws in the definition have been recognised by the Council of the European Union in their compromise position on the AI Act and by the European Parliament's Scientific Foresight Unit in their study.

This paper was co-drafted by **European Digital Rights (EDRi)**, **Access Now**, **ARTICLE19**, **Bits of Freedom**, the **Chaos Computer Club (CCC)**, **Digitale Gesellschaft CH** and the **IT-Political Association of Denmark (IT-Pol)**.
It is supported by **AlgorithmWatch**, the **European Center for Not-For-Profit Law (ECNL)**, **Fair Trials** and the **Panoptykon Foundation**. It follows the Joint Civil Society Statement 'An EU Artificial Intelligence Act for Fundamental Rights', November 2021, signed by 123 organisations.