Policy Brief

February 2021

Transparency and Accountability Mechanisms for Facial Recognition

Els J. Kindt

This brief is one of two presenting strategies for addressing challenges associated with facial recognition. These briefs provide policymakers concrete options for setting guardrails and aim to stimulate debate on possible paths forward.

The other brief, *Facial Recognition in the Public Sector: The Policy Landscape* by Rashida Richardson reviews the use of facial recognition technology in the public sector around the world and surveys proposed and pending laws and regulations to mitigate human and civil rights concerns associated with government use of facial recognition.

This brief explores in greater depth three existing regulatory mechanisms of general application that may have specific relevance to facial-recognition technology: data protection impact assessments, technical standards, and certification mechanisms.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

The widespread use of facial-recognition technology presents a range of civil and human rights challenges. Many citizens, civil society groups, and leaders in the United States and Europe have identified the need to address these challenges. Yet policymakers are often understandably hesitant to explicitly regulate specific technologies in order not to hamper innovation, distort competition, or stifle the development of a market, instead preferring technology-neutral regulation. This brief reviews existing legal and regulatory mechanisms and tools that may be useful in addressing civil and human rights challenges arising from facial-recognition technology.

Data Protection Impact Assessments

The European Union's General Data Protection Regulation 2016/679 (GDPR), which applies from 2018, seeks to address challenges related to the protection of personal information. Because biometric data (such as the data used in facial-recognition systems) is usually based upon unique, universal, and persistent human characteristics that allow the identification or recognition of individuals, and these characteristics cannot be revoked and are often fit for capture on the move, EU legislation has deemed such data as deserving particular attention. The GDPR defines the concept of biometric data,[1] and lays out a predefined set of permitted uses as an exemption to a general prohibition to use "sensitive" data. This provides a first step in addressing the technology.

In addition, the GDPR charges data controllers processing biometric data with carrying out a Data Protection Impact Assessment (DPIA). This is mandatory when using new technologies and the data processing is "likely to result in a high risk to the rights and freedoms of natural persons."[2] Facial-recognition technology is likely to fit this description, while it is not addressed specifically in the GDPR. A DPIA is also required if there is "sensitive" data processing, including of biometric data for identification purposes, on a large scale.[3]

In conducting a DPIA, data controllers must assess the "necessity and proportionality" of the data processing and the risks to the rights and freedoms of the individuals concerned. Further, they must set "safeguards, security measures and mechanisms" to mitigate these risks. A similar DPIA mechanism was also included in the Law Enforcement (LEA) Directive 2016/680 that was adopted at the same time as the GDPR to govern the use of personal data by competent authorities in law enforcement and judicial matters.[4]

The idea for data controllers to perform a risk assessment was inspired by similar obligations in other domains, such as requirements for potential polluters to undertake environmental impact assessments. Placing an obligation and responsibility on entities to assess their own data protection activities is intended to make them accountable for these. In addition, a DPIA avoids placing this complex burden on governmental supervisory authorities, which often lack sufficient resources, staff, and expertise to carrying one out. The inclusion of DPIAs as a tool in the GDPR also reflected a growing preference for "risk-based approaches" that focus attention on processing activities that pose more risks for individuals.

National data protection authorities have sought to provide guidance on how to carry out a DPIA. For example, the French authority has given specific advice with regard to biometric technologies. Data controllers must discuss the assessment with the supervisory authorities anytime the safeguards identified may not

[1] Biometric data is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [fingerprint] data." European Commission, General Data Protection Regulation, 2016. Art. 4 (14), and European Union, Law Enforcement Directive, 2016. Art.3(13).

[2] European Commission, General Data Protection Regulation, 2016. Art. 35.1.

[3] European Commission, General Data Protection Regulation, 2016. Art. 35.3.c.

[4] European Union, Law Enforcement Directive, 2016. Art. 27.

mitigate the high risks and obtain written advice of the supervisory authorities. EU member states may also require that data controllers receive prior authorization from supervisory authorities for processing for a task carried out in the public interest. This includes processing for social protection and for public health.[5] Where facial-recognition technology is deployed by governments, such applications are considered often "public interest" ones.

DPIAs must take into account the wide range of interests involved in the deployment of new technology, including input from an organization's data protection officer. At the same time, they are sometimes criticized as "check the box" exercises that are treated by data controllers as a formality.

One particular challenge associated with the use of facial-recognition technology is that individuals can be identified in private and public places. This poses risks for rights of privacy, free movement, and free speech. A DPIA for deployment of facial-recognition technology in public places hence requires an evaluation of the impact of the deployment on at least these fundamental rights and freedoms. A study by the EU Agency for Fundamental Rights on the use of facial recognition by law-enforcement bodies has identified other risks to fundamental rights as well, including the right to non-discrimination.[6] More research and study of these risks would be useful for evaluating other applications of facial recognition and informing future DPIAs.

Importantly, a DPIA must assess the necessity and proportionality of the use of facial recognition in relation with the purposes of its use. This requires specific expertise and potentially independent review. The assessment places a significant responsibility on the shoulders of data controllers, and only limited guidance has been provided by data protection authorities to date. A lack of proper assessment was also one of the key findings in one of the first court cases in appeal addressing the use of the technology by the police in the United Kingdom. Further guidance on how to identify and assess the risks of various applications when facial recognition is used by law-enforcement bodies, in public places, or in private applications, would be very beneficial. The idea of categorization of various types and uses of facial-recognition technology is still emerging, especially in the United States.[7] Certain applications may warrant requirements for approval for commercialization and specific use cases, with adequate oversight.

Standards

Another approach to regulating facial recognition through existing tools and mechanisms would be the use of technical standards. Standards have always played an important role in the European Union and in the United States when it comes to regulating technology. They can be agreed and adopted on the national, regional, or international level. Standards are usually not obligatory, but largely voluntary and driven by industry. They are only mandatory when they are explicitly addressed and imposed by legislation.

Standards are in principle not developed by legislators but by private associations and organizations, with the help of experts, at the international and national levels. Standards are also in most cases addressed to the developers of the technology, and only subsequently to the data controllers and users to the extent that they may be required to use technology meeting particular standards.

Standards can be a very important regulatory mechanism to the extent that technology like facial recognition can be technically improved through requirements to meet certain standards, such as those requiring greater accuracy and avoidance of bias.

[5] European Union, General Data Protection Regulation, 2016. Art. 36.5.

[6] European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 27 November 2019.

[7] Erik Learned-Miller, Vicente Ordonez, Jamie Morganstern, and Joy Buolamwini, Facial Recognition Technologies in the Wild: A Call for a Federal Office, Algorithimic Justice League, May 29, 2020.

ISO and IEC standards

Some of the most relevant international standards for facial-recognition technology have been developed over the last twenty years by the subcommittees 27 (SC 27) and 37 (SC 37) of the Joint Technical Committee 1 of the International Standardization Organization (ISO), a federation of national standards bodies, and by the International Electrotechnical Commission (IEC), with main offices in Switzerland.

One of the standards adopted by SC 37 establishes a "harmonized vocabulary," which is very useful for a common understanding in addressing and discussing biometric technology. This standard—ISO/IEC 2382-37:2020—was issued for the first time in 2012, renewed in 2017, and is being updated again. A set of common terms is indispensable in any policy discussion concerning technology. Terms like identification and verification, which are crucial in debates on facial recognition, are defined and clarified in this standard. Other standards published under the direct responsibility of SC 37 include ones about data formats, data quality, performance testing and reporting as well as cross-jurisdictional and societal aspects of the technology. Twenty-eight countries are participating in the development of the standards, while there are about twenty more observing. These countries ratify the work done and vote on the standards.

Another important standard safeguarding the use of biometric data technologies, especially in the private sector, is the standard developed by SC 27 for biometric information protection. This standard—ISO/IEC 24745:2011—addresses requirements for binding a biometric reference with an identity reference and for the protection of individuals during storage and processing of biometric data. This standard addresses the risks of linkability of identities in contexts where this is not necessary and where risks to fundamental rights exist. Linkability and limits to it also play an important role in limiting "function creep." The standard also allows providers to issue pseudonyms, protecting individuals against inappropriate use and allowing them to revoke and renew their biometric identifier.

U.S. standardization bodies

The U.S. National Institute of Standards and Technology has long been involved in testing vendor performance for various biometric characteristics. A 2019 study on facial-recognition vendors measured demographic differences in the commercial facial-recognition algorithms of almost 100 sellers.[8] When tested on photographs from a global population, the study revealed that false-positive rates were highest for West African, East African, and East Asian people, and lowest for Eastern European ones. However, algorithms developed in China produced low false-positive rates for East Asian people. When tested on photographs collected by U.S. law-enforcement authorities, false-positive rates were highest for American Indian people and also high for African American and Asian people. False positives were also found to be higher for women than men, for the elderly, and for children. The study demonstrated that the algorithms may show bias and thus the potential need for standards that limit the use of biased algorithms.

The EU's role in standardization

The European Commission supports the standardization work of three European organizations: the European Telecommunications Standards Institute (ETSI), the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (Cenelec). The legal framework for the operation and involvement of different stakeholders is set forth in Regulation on European Standardization 1025/2012. This framework specifies that the commission may identify technical specifications in public procurement. This could also apply to specifications for facial-recognition technology.

It remains uncertain whether such standards are sufficient to ensure fair technology and legal compliance. Fairness in AI is under wide discussion around

[8] National Institute of Standards and Technology, NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, December 19, 2019.

the world. It is a broad notion, including various components, such as the need for human oversight.

Even if facial-recognition systems accord to standards and are fair, there remains the issue of legal compliance, such as with principles of data minimization, purpose specification, and transparency. The European Commission has identified possible benefits of standards for its policies and legislation, including in the areas of privacy and data protection. In its 2020 Rolling Plan for ICT Standardization, drafted in close collaboration with the European multi-stakeholder platform on ICT standardization, the commission links standardization with its legislation.[9] One of the key enablers for privacy consists of technical measures for anonymization and pseudonymization. The ISO/IEC 24745:2011 standard on biometric information protection could certainly also be very relevant in this context. Another key enabler is an independent review of the potential of and adherence to standards in the context of certification (see below).

Because legal principles are often difficult to apply and enforce, technical standards can play a role in translating principles into technology. The GDPR mandates "data protection by design and by default," requiring data controllers to implement appropriate technical and organizational measures when designing and operating their technology in order to integrate data protection safeguards. Data protection by design should likewise be taken into account for facial-recognition technology. Such a principle would imply minimizing reference data, limited or decentralized storage of the data, pseudonymization where appropriate, encryption of data during transmission and storage, and use of any other standards that may be beneficial.

Overall, standards, if captured by legislation, are a potentially important building block for facial recognition technology. Standards may be able to aid developers in avoiding certain risks, such as inaccurate results, unnecessary linkage between biometric data and real identities, and biased algorithms.

Certification Mechanisms

While certification has long been discussed in the data protection context, the success of this policy mechanism has been limited. One of the first certification mechanisms set up in the European Union in the domain of data protection concerned the European Privacy Seal.[10] The GDPR includes a provision on certification, suggesting that data controllers or processors could rely on certifications to demonstrate compliance with it.[11]

Certification mechanisms could, in combination with well-chosen standards, play an important role for facial-recognition technology. To the extent that legal and ethical principles can be translated into standards and be reflected in the design of the technology, certification could allow users to evaluate the qualities of a particular tool or technology. At the same time, experience with these mechanisms is very limited in the EU. The European Data Protection Board has issued guidelines on the criteria for such certification schemes. Certification schemes have not yet been set up for facial recognition. Their transparency and accessibility for smaller businesses will be important. The benefits of such mechanisms must also be assessed, recognizing that often mainly technical aspects including adherence to standards could be certified. To the extent that legal principles and obligations can also be translated in standards and in the design of the technology, such certification could further gain in importance.

Oversight

The development and deployment of new technologies such as facial recognition can implicate human rights, raising questions as to the necessity of the technology and proportionality of any regulations.

[9] European Union, Rolling plan for ICT standardization, May 5, 2020.

[10] European Union, European privacy seal, 2017.

[11] European Commission, General Data Protection Regulation, 2016. Art. 42.

To address such risks, independent and strong oversight of the use of the facial-recognition technology in operation is needed. While there are existing bodies for oversight and enforcement of relevant laws, multidisciplinary expertise remains essential in the appropriate governance of new technology. The expertise required includes at least technical knowledge in the domain of biometric systems and facial recognition, alongside expertise on ethical, legal, and societal implications of the technology. This multidisciplinary expertise should also be present within oversight bodies. These bodies could play an important role in reviewing DPIAs, identifying relevant standards, and supervising proper use of certification mechanisms.

Conclusion and Recommendations

Because of the risks posed for fundamental rights, the European Commission launched in early 2020 a debate about legislation for remote biometric identification in its White Paper on Artificial Intelligence.[12] Where biometric technology serves as a specific investigative tool deployed by law-enforcement bodies, an independent review and prior authorization of the use of such technology in cases defined by law could address specific concerns related to the technology while still permitting beneficial uses. The use of facial recognition in public places by government and public authorities presses for a justification within boundaries set out by legislative measures, and the use by private parties should equally be within legal boundaries minimizing the risks.

In the meantime, the mechanisms described above can play a role in ensuring that deployment of facial-recognition technology by law-enforcement bodies, other public entities, or private entities respects human rights and democratic values. DPIAs, standards, and certification align with the new approach of increasing accountability of the controllers of the technology and the risk-based approach.

DPIA requirements as laid out in the GDPR remain abstract and put a high burden on users of the technology. To support the effective use of DPIAs to identify and mitigate risks associated with the use of facial-recognition technology, interdisciplinary teams—bringing together facial-recognition systems experts, biometric and AI experts, and ethical, legal and societal experts, as well as stakeholders (users and citizens)—should be created to identify the common risks from the use of the technology in different scenarios. These teams should develop a catalogue of present and possible future uses of facial-recognition technology and an overview of the current technological limitations for each use. In addition, they should develop guidelines for risk assessment and suggest principles for regulation and specific regulatory approaches. Such teams could also suggest codes of conducts for specific sectors.

Several standards for biometric technologies have been developed already or under construction and should be leveraged. At present, most are voluntary; further research should investigate which ones may warrant reference in legislation. The same interdisciplinary teams described above should collaborate to identify relevant standards that could help mitigate particular risks associated with facial-recognition technology, such as those related to of inaccuracy, bias, impersonation, and function creep.

If and when certain standards are identified that can help provide helpful guidelines for the development of facial-recognition technology, certification mechanisms can be developed to allow technology developers to demonstrate the compliance of their tools and data controllers the use of facial recognition. Governmental authorities should provide for facial-recognition technology to be certified according to standards and other criteria identified by an independent certification body according to well established certification procedures and mechanisms.

[12] EU Commission, White Paper on Artificial Intelligence: a European Approach to Excellence and Trust, February 19, 2020.

February 2021

About the Author(s)

Els Kindt is a legal researcher and lecturer at KU Leuven, Belgium and an associate law professor at the Universiteit Leiden, eLaw, the Netherlands.

About GMF Digital

The German Marshall Fund's Digital Innovation and Democracy Initiative (GMF Digital) works to support democracy in the digital age. GMF Digital leverages a transatlantic network of senior fellows to develop and advance strategic reforms that foster innovation, create opportunity, and advance an equitable society.

The views expressed in GMF publications and commentary are the views of the author(s) alone.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of World War II, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

G | M | F

Ankara • Belgrade • Berlin • Brussels • Bucharest
Paris • Warsaw • Washington, DC

www.gmfus.org