Dear Members of the Office of Science and Technology Policy,

Thank you for the opportunity to submit input on public and private sector uses of biometric technologies.

ARTICLE 19 is an international human rights organization that seeks to protect and promote freedom of expression. It is headquartered in London and has offices in the United States, Bangladesh, Brazil, Kenya, Mexico, Myanmar, Netherlands, Senegal, and Tunisia. We are submitting this input based on our significant empirical and legal work around the world.

Our work on biometrics over the last decade has included analysis of the human rights implications of these systems and evidence of how their design, development, and deployment in a growing number of domains. These include specific consideration of how these technologies are used for identity verification, identification, surveillance, and inference of attributes, including emotional states and those protected by law. This submission provides crucial findings from our work, information about how stakeholders are affected, and principles that should govern the use of biometric technologies, particularly in light of the fact that biometric technologies rely on increasingly sophisticated and complex artificial intelligence and machine learning systems. Data exploitation; identification and tracking; inference and prediction of information; profiling to sort, score, categorize, assess, and rank individuals; and how these relate to decision making, rights, resource allocation, are among the issues addressed.

With respect to emotion recognition technology, there are no ethical uses for its use and despite claims that this technology can improve with time, given the pseudoscientific and racist foundations of emotion recognition on one hand, and fundamental incompatibility with human rights on the other, the design, development, deployment, sale, and transfer of these technologies should be prohibited and banned. This type of technology is built around three discredited and erroneous scientific assumptions: that facial expressions are universal; that emotional states can be unearthed from them; and that such inferences are reliable enough to be used to make decisions.

There is a need to examine how existing discourses, such as human rights law, data protection, sectoral privacy regulation, and research ethics, relate to different applications and methods of biometric technologies. Overriding challenges to the deployment of biometric technologies include informational asymmetry, the opacity and secrecy of biometric profiling and surveillance; discrimination, unfairness, inaccuracies, and bias; re-identification and de-anonymization; and lack of legal regulatory frameworks as well as technical expertise in policymaking. This submission also addresses the deployment of biometric technologies in China specifically, which lacks human rights safeguards and is a major exporter of such technology around the world.

In this submission, we wish to provide you with resources and highlight some crucial findings from our work that we hope will inform this consultation and any broader efforts, such as efforts to develop an AI Bill of Rights.

1. In January 2021, we released a report, "Emotional Entanglement", on the emotion recognition market in China and its implications for human rights. Here, we critically analyse claims made by 27 Chinese companies that sell this technology for three use cases: public security, education, and driving safety. Some of our main findings are as follows:
    a. **The design, development, sale, and use of emotion recognition technologies are inconsistent with international human rights standards.** While emotion recognition is fundamentally problematic, given its discriminatory and discredited scientific foundations, concerns are further exacerbated by how it is used to surveil, monitor, control access to opportunities, and impose power, making the use of emotion recognition technologies untenable under international human rights law (pp. 36–44).
    b. **Emotion recognition technologies' flawed and long- discredited scientific assumptions do not hinder their market growth in China.** Three erroneous assumptions underlie justifications for the use and sale of emotion recognition technologies: that facial expressions are universal, that emotional states can be unearthed from them, and that such inferences are reliable enough to be used to make decisions. Scientists across the world have discredited all three assumptions for decades, but this does not seem to hinder the experimentation and sale of emotion recognition technologies (pp. 18–35).

c. **Chinese local governments' budding interest in emotion recognition applications confer advantages to both startups and established tech firms.** Law enforcement institutions' willingness to share their data with companies for algorithm-performance improvement (p. 22), along with local government policy incentives (pp. 18, 20, 22, 24, 25, 33), enable the rapid development and implementation of emotion recognition technologies.
d. **The emotion recognition market is championed by not only technology companies but also partnerships linking academia, tech firms, and the state**. Assertions about emotion recognition methods and applications travel from academic research papers to companies' marketing materials(pp. 22, 25-26) and to the tech companies' and state's public justifications for use (pp. 20, 22-33). These interactions work in tandem to legitimize uses of emotion recognition that have the potential to violate human rights.
e. **Chinese law enforcement and public security bureaus are attracted to using emotion recognition software as an interrogative and investigatory tool.** Some companies seek procurement order contracts for state surveillance projects (pp. 18-22) and train police to use their products (p. 22). Other companies appeal to law enforcement by insinuating that their technology helps circumvent legal protections concerning self-incrimination for suspected criminals (pp. 42-43).
f. **While some emotion recognition companies allege they can detect sensitive attributes, such as mental health conditions and race, none have addressed the potentially discriminatory consequences of collecting this information in conjunction with emotion data.** Some companies' application programming interfaces (APIs) include questionable racial categories for undisclosed reasons (p. 41). Firms that purportedly identify neurological diseases and psychological disorders from facial emotions (pp. 41-42) fail to account for how their commercial emotion recognition applications might factor in these considerations when assessing people's emotions in non-medical settings, like classrooms.
g. **Chinese emotion recognition companies' stances on the relationship between cultural background and expressions of emotion influence their products**. This can lead to problematic claims about emotions being

presented in the same way across different cultures (p. 40) – or, conversely, to calls for models trained on 'Chinese faces' (p. 41). The belief that cultural differences do not matter could result in inaccurate judgements about people from cultural backgrounds that are underrepresented in the training data of these technologies – a particularly worrying outcome for ethnic minorities.

h. **None of the Chinese companies researched here appears to have immediate plans to export their products.** Current interest in export seems low, (p. 40) although companies that already have major markets abroad, such as Hikvision and Huawei, are working on emotion recognition applications (pp. 23, 27, 29-33, 40).

2. Building on this, in April 2021, ARTICLE 19 also published its biometrics policy which warns against the use of biometric technologies, especially on national security and counterterrorism grounds, without a sufficient legislative framework to protect human rights. We consider that a human rights-based approach ought to be embedded at the start of the design and development of any technology. A summary of our recommendations is as follows:
    a. States should ban biometric mass surveillance
    b. States should ban the design, development and use of emotion recognition technologies
    c. Public and private actors who design, develop and use biometric technologies should respect the principles of legitimacy, proportionality and necessity
    d. States should set an adequate legislative framework for the design, development and use of biometric technologies
    e. Government authorities must ensure that the design, development and use of biometric technologies are subject to transparency and open and public debate
    f. Transparency requirements for the sector should be imposed and thoroughly implemented by both public and private sectors
    g. States should guarantee accountability and access to remedies for human rights violations arising from biometric technologies
    h. The private sector should design, develop and deploy biometric systems in accordance with human rights standards.

3. More generally on AI, in April 2019, we published a report "Governance with Teeth", which documents how "ethical" approaches to AI are toothless when treated as an end in and of themselves, how they obscure responsibility and buy time for private companies to experiment with AI technologies, including biometrics, while causing real harm to people. We highlighted the importance of a human-rights based approach in regulating AI.

4. Finally, in our April 2018 published in conjunction with Privacy International, "Privacy and Freedom of Expression in the Age of Artificial Intelligence" we identified the human rights implications of these systems in detail. Each of the novel interferences with privacy are significant and have an impact on the a range of other human rights and societal norms. Many of the issues raised in this report are relevant to consider with respect to the concerns about the use of biometric surveillance:
    a. to identify people who wish to remain anonymous;
    b. to infer and generate sensitive information about people;
    c. to profile people based upon population-scale data;
    d. to make consequential decisions using this data, some of which profoundly affect people's lives or the ability of groups to freely associate and express themselves

We would be happy to discuss any aspect of these reports with you and provide evidence as may be necessary. We look forward to additional opportunities to provide input to this consultation.

Best,

Dr. Courtney C. Radsch
U.S. and Tech Policy Advisor
ARTICLE 19
www.article19.org