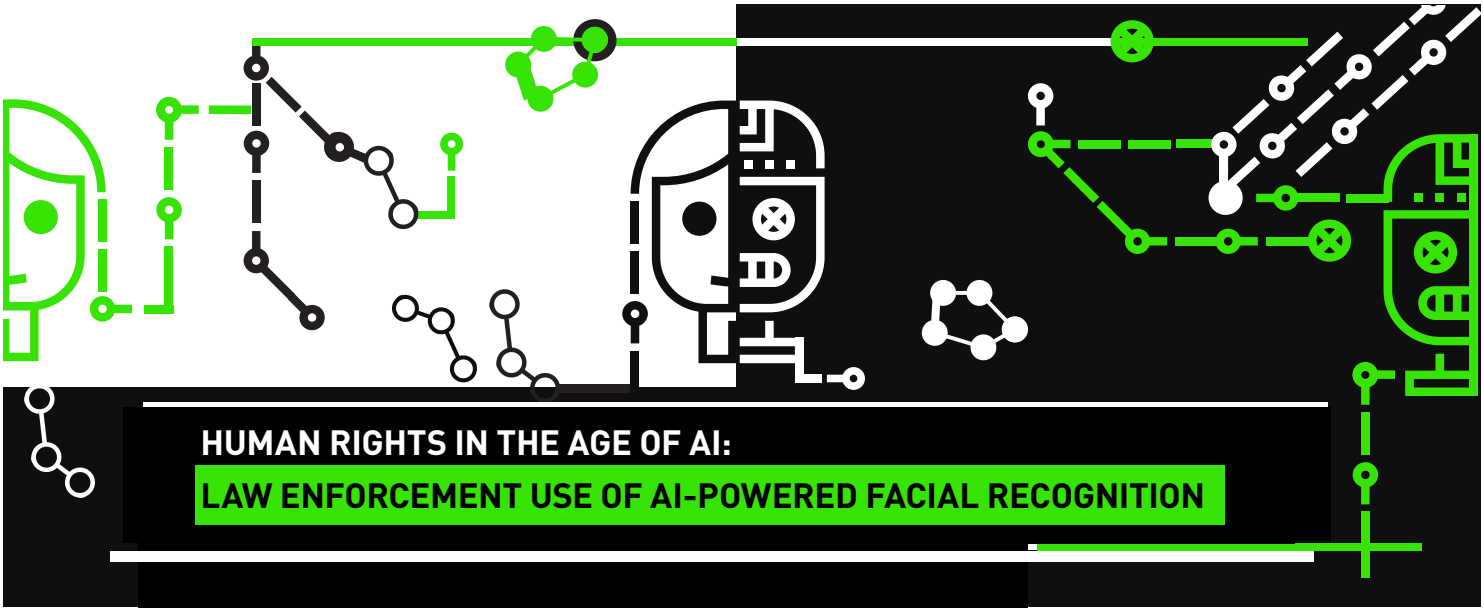

As AI continues to find its way into daily lives, its risk of interfering with human rights gets more severe. Access Now has conducted a review of human rights issues that are being raised today or will be in the near future. The following case study is provided to help understand the parameters of the report.

HUMAN RIGHTS IN THE AGE OF AI: A CASE STUDY EXAMINING LAW ENFORCEMENT USE OF AI-POWERED FACIAL RECOGNITION

One pervasive and dangerous example of uses of AI is in facial recognition software.[1] Although the technology is still imperfect, law enforcement are looking to AI-powered facial recognition technology as a tool to monitor, identify, and locate people, which facilitates profiling.[2]

China has taken the most drastic steps in integrating these capabilities into its domestic surveillance apparatus. Last year, China made international headlines when local police arrested dozens of wanted criminals at a beer festival by identifying them using a network of CCTV cameras and facial recognition software.[3] The government is steadily expanding this surveillance network nationwide; it already has an estimated 200 million cameras.[4]

Outside of China, the U.K. deploys facial recognition technologies at public events.[5] Use of real-time facial recognition in the U.S. is largely in the testing phase. Recently, Amazon was reportedly marketing a facial recognition product called Rekognition to law enforcement agencies for use with police body cameras.[6] In 2018, Australia unveiled a plan to connect its network of CCTV cameras to existing facial recognition and biometric databases.[7]

1. In 2018, Australia unveiled a plan to connect its network of CCTV cameras to existing facial recognition and biometric databases. The proposed measure is pending in Parliament. Ihttps://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf.
2. Recently, Amazon has come under fire for directly marketing a facial recognition product called Rekognition to law enforcement agencies for use in conjunction with police body cameras, which would allow police to identify people in real time. The product was piloted with police departments in Orlando, Florida and Washington County, Oregon. https://www.theguardian.com/technology/2018/may/22/amazon-rekognition-facial-recognition-police
3. https://www.theguardian.com/world/2017/sep/01/facial-recognition-china-beer-festival.
4. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.
5. https://www.theguardian.com/technology/2018/jun/14/police-face-legal-action-over-use-of-facial-recognition-cameras, and https://www.lawfareblog.com/one-nation-under-cctv-uk-tackles-facial-recognition-technology.
6. https://www.theguardian.com/technology/2018/may/22/amazon-rekognition-facial-recognition-police. The product was piloted with police departments in Orlando, Florida, and Washington County, Oregon.
7. https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf. The proposed measure is pending in Parliament.

HUMAN RIGHTS IMPLICATIONS

The Right to Privacy

Widespread government use of real-time facial recognition that can identify people wherever they go will seriously interfere with the right to privacy, obliterating public anonymity, and chilling people from the exercise of other rights. Additionally, because mass surveillance is neither necessary nor proportionate to a legitimate government aim, the interference is not justified.[8]

Rights to Freedom of Expression, Assembly, and Association

Tracking individuals using facial recognition can reveal political affiliations or sexual orientation as well as reveal who attends protests and how people are connected interpersonally. This tracking has a chilling effect on free expression, assembly, and association, and can lead to self-censorship.[9]

Right to Liberty and Security of the Person

Facial recognition software for use within law enforcement risks unlawful arrest due to error and overreach.[10] Error rates of current facial recognition technology mean these inaccuracies will lead to inappropriate detainments, particularly in underfunded law enforcement departments that may have fewer accountability mechanisms.

Right to Non-Discrimination

Facial recognition can discriminate unwittingly,[11] as well as by design. Faception is a company that purports to categorize people through machine learning, classifying them as "high IQ" or "terrorist" based on faces alone. Law enforcement use of such a system encodes racial profiling.

HOW TO ADDRESS AI-RELATED HUMAN RIGHTS HARMS

Action is necessary to prevent and mitigate the myriad serious human rights harms AI will foreseeably cause. Because AI is a diverse field, the potential for human rights harms depends both on the type of data a system uses and the context in which it is implemented. The following four broad policy approaches could address many of the human rights risks posed by AI.

Comprehensive data protection laws

Because data drives AI, data protection laws are necessary for AI, which should include:

- **Notification:** people must be notified if their data is used for automated decision making;
- **Explanation**: people should understand how and why an automated decision is made;
- **Access and Correction:** People should be able to access information collected about them and amend and modify information it if it is incorrect, incomplete, or inaccurate;
- **Objection:** People should have the ability to contest the collection and use of their data.

8. See, necessaryandproportionate.org/.
9. See, e.g., https://pen.org/research-resources/chilling-effects/.
10. https://irlpodcast.org/season2/episode3/.
11. The ACLU scanned the faces of all members of Congress against 25,000 public mugshots. The Amazon software generated 28 false matches, 38% of which were people of color -- a larger share that the 20% of current members of Congress who are people of color. https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.

FACIAL RECOGNITION: DATA PROTECTION LAWS WILL ENSURE PEOPLE KNOW HOW AND WHEN THEIR BIOMETRICS ARE COLLECTED AND HAVE THE ABILITY TO OPT OUT OF INVASIVE PROGRAMS. THEY WILL HELP ENSURE THAT PEOPLE CAN OBJECT TO HARMFUL USES.

High standards for government use of AI

Governments have an obligation to promote, protect, respect, and fulfill human rights, and therefore should:[12]

- **Follow open procurement standards.** The procurement of any public-use AI system should be done openly, transparently, and include a period for public comment, with outreach to potentially affected groups to ensure they have input.
- **Conduct human rights impact assessments.** Governments must thoroughly investigate AI systems to identify potential human rights risks prior to development or acquisition, including analysis on whether current law is sufficient to protect human rights.
- **Ensure transparency and explainability.** Maximum possible transparency about a system must continue throughout a system's life cycle.
- **Establish accountability and procedures for remedy.** There should always be a human in the loop, with significant oversight for high-risk areas.
- **Develop redlines delineating contexts in which AI will not be used.** Governments must draw and regularly re-examine guidelines for themselves in their use of AI.

FACIAL RECOGNITION: FACIAL RECOGNITION SHOULD NEVER BE USED FOR PERVASIVE, MASS SURVEILLANCE. A COMPREHENSIVE REVIEW OF SURVEILLANCE LAWS SHOULD ENSURE PROTECTION OF HUMAN RIGHTS AND LAWS MUST PROVIDE FOR TRANSPARENCY AND ACCOUNTABILITY IN DEPLOYMENT OF THE TECHNOLOGY.

Company duties to respect human rights

Private entities must take ongoing proactive and reactive steps to ensure they do not cause or contribute to human rights abuses. A human rights review should be integrated into larger ethics review processes, which should consider:

- **Human rights due diligence.** Potential rights-harming outcomes should be identified and effective action taken to prevent and mitigate harms, as well as track the responses.
- **Transparency and explainability.** Private sector actors should endeavor to be as transparent as possible and provide meaningful information about how AI systems work.
- **Accountability and remedy.** Internal accountability mechanisms are needed and companies should ensure individuals have access to meaningful remedy and redress.

12. See https://www.ohchr.org/EN/ProfessionalInterest/Pages/InternationalLaw.aspx for a summary of state's human rights obligations under international law.

FACIAL RECOGNITION: COMPANIES MUST THOROUGHLY REVIEW POTENTIAL IMPACTS OF THEIR TOOLS AND REFUSE TO SELL THEIR SYSTEMS UNLESS THE APPROPRIATE LEGAL PROTECTIONS ARE IN PLACE.

Need for more research

All stakeholders must work together to investigate future uses of AI and explore potential human rights impacts. Emphasis should be placed on identifying and building response mechanisms for potential threats to ensure that negative implications are mitigated to the fullest extent possible.

FACIAL RECOGNITION: FACIAL RECOGNITION TECHNOLOGY CONTINUES TO EVOLVE. AS IT DOES WE MUST CONTINUE TO EVALUATE ITS USES, INCLUDING ANY BIAS BUILT IN OR DISCRIMINATORY IMPACTS.

accessnow

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.

accessnow.org