

## COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

### AUTORITEIT PERSOONSgegevens (NL) - DEPARTMENT FOR THE COORDINATION OF ALGORITHMIC OVERSIGHT (DCA)

AI Systems for Emotion Recognition in the Areas of Workplace or Education Institutions:  
Prohibition in EU Regulation 2024/1689 (AI Act)

[DCA-2024-02]

DECEMBER 17, 2024

---

By notice published on October 31, 2024, the Netherlands' Autoriteit Persoonsgegevens ("AP") sought input<sup>1</sup> on its interpretation of the sixth prohibition of Regulation (EU) 2024/1689 (hereinafter the "AI Act")<sup>2</sup> which prohibits AI systems intended to identify or infer the emotions or intentions of natural persons ("emotion recognition systems")<sup>3</sup> in the areas of workplace or education institutions based on biometric data ("Prohibition F").<sup>4</sup> The AP provided a list of questions for this

---

<sup>1</sup> "Call for input on prohibition on AI systems for emotion recognition in the areas of workplace or education institutions," Autoriteit Persoonsgegevens (Oct. 31, 2024), <https://www.autoriteitpersoonsgegevens.nl/en/documents/call-for-input-on-prohibition-on-ai-systems-for-emotion-recognition-in-the-areas-of-workplace-or-education-institutions>.

<sup>2</sup> Regulation (EU) 2024/1689 of the European parliament and of the Council of 13, June 2024 laying down harmonized rules on artificial intelligence and amending regulations (Artificial Intelligence Act) [2024] OJ L 2024/1689 [Hereinafter the "AI Act"].

<sup>3</sup> AI Act Art. 3, para. 39.

<sup>4</sup> AI Act Art. 5, para. 1, subpara f. Prohibition F is defined as "the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons."

comment opportunity, but also allows “other relevant input.”<sup>5</sup> Pursuant to this request, the Electronic Privacy Information Center (“EPIC”) submits the following comments.

EPIC is a public interest research center based in Washington, D.C. Over the last 30 years, EPIC has focused public and regulatory attention on emerging privacy and human rights issues and worked to protect privacy, freedom of expression, and democratic values in the information age.<sup>6</sup> EPIC has a strong history advocating for the rights of individuals subject to biometric and other automated systems and assessment tools, including emotion recognition systems.<sup>7</sup> EPIC has previously submitted comments calling for bans on the use of facial recognition and emotion recognition systems.<sup>8</sup>

Emotion recognition systems have already been recognized within the EU AI Act as an unacceptable risk in workplaces and education.<sup>9</sup> This call to provide clarity to the scope of the prohibition may, among other things, explore whether any uses of emotion recognition systems in these contexts may be permissible and look to what specific risks are inherent within emotion recognition systems.<sup>10</sup> Due to the high risk nature of these systems – and their inefficacy – we argue that emotion recognition systems should be banned in all contexts.

---

<sup>5</sup> Call for Input, “AI systems for emotion recognition in the areas of workplace or education institutions: Prohibition in EU Regulation 2024/1689 (AI Act),” Autoriteit Persoonsgegevens, para 10.

<sup>6</sup> *About Us*, EPIC (2023), <https://epic.org/about/>.

<sup>7</sup> *See, e.g., EPIC v. DHS – FAST Program*, EPIC, <https://epic.org/documents/epic-v-dhs-fast-program/> (last visited Dec. 12, 2024); *EPIC, Coalition Urge Zoom to Abandon Emotion Recognition*, EPIC (May 13, 2022), <https://epic.org/epic-coalition-urge-zoom-to-abandon-emotion-recognition/>; Comments of EPIC to DOJ and DHS on Law Enforcement’s Use of FRT, Biometric, and Predictive Algorithms 44-50 (Jan. 19, 2023), <https://epic.org/wp-content/uploads/2024/01/EPIC-DOJDHS-Comment-LE-Tech-011924.pdf>; Comments of EPIC to PCLOB AI in Counterterrorism July 2024, EPIC (July 1, 2024), available at [https://epic.org/documents/comments-of-epic-to-pclob-ai-in-counterterrorism-july-2024/#\\_ftn21](https://epic.org/documents/comments-of-epic-to-pclob-ai-in-counterterrorism-july-2024/#_ftn21); Comments of EPIC to the Office of the Privacy Commissioner of Canada Regarding the Update to Guidance on Handling Biometric Information, EPIC (Jan. 12, 2024), available at <https://epic.org/documents/comments-of-epic-to-the-office-of-the-privacy-commissioner-of-canada-regarding-the-update-to-guidance-on-handling-biometric-information/>.

<sup>8</sup> *Id.*

<sup>9</sup> AI Act Art. 5.

<sup>10</sup> Call for Input, “AI systems for emotion recognition in the areas of workplace or education institutions: Prohibition in EU Regulation 2024/1689 (AI Act),” Autoriteit Persoonsgegevens.

EPIC submits these comments to (1) support the AP’s actions in protecting the rights, dignity, and privacy of EU citizens; (2) set forth the failures, biases, and harms of emotion recognition systems and their violation of standing EU law; (3) document the current harms these systems perpetuate in both education and the workplace, and (4) provide recommendations regarding exceptions and language clarifications.

## **I. Structure and Intent of Emotion Recognition Systems**

### *Responsive to Questions 1, 2, 3, 7, and 8*

Emotion recognition is a broad field (so broad that even a single term cannot always be agreed on – “sentiment analysis” and “affective computing” are often used interchangeably with emotion recognition). Emotion recognition systems can vary widely in their scope, conclusions, and what data they use for analysis, but they are unified in goal: identifying human emotion. In these comments, we focus on automated emotion recognition systems. These may often include elements of signal or speech processing, machine learning, and other AI components. In discussing the variety and range of these systems and their impact, we look first at the different structures of emotion recognition systems and then at the proposed purposes and uses of these systems.

#### *a. Structure of emotion recognition systems*

Emotion recognition systems may use multiple different forms of computing<sup>11</sup> to conduct analysis, including multimodal approaches.<sup>12</sup> Put very simply, these automated systems perform a

---

<sup>11</sup> See, e.g., Yoshihiro Miyakoshi and Shohei Kato, “Facial emotion detection considering partial occlusion of face using Bayesian network,” 2011 IEEE Symposium on Comp. & Informatics (2011), <https://ieeexplore.ieee.org/document/5958891>; Hari Krishna Vydana et al., *Improved emotion recognition using GMM-UBMs*, 2015 Int’l Conference on Signal Processing and Communication Engineering Systems (2015), <https://ieeexplore.ieee.org/document/7058214/references#references>; B. Schuller et al., *Hidden Markov model-based speech emotion recognition*, 2003 Int’l Conference on Multimedia and Expo. ICME ’03 Proceedings (2003), <https://ieeexplore.ieee.org/document/1220939>.

<sup>12</sup> Soujanya Poria et al., *A review of affective computing: From unimodal analysis to multimodal fusion*, *Info. Fusion*, 37 (2017), <https://www.sciencedirect.com/science/article/abs/pii/S1566253517300738?via%3Dihub>.

series of steps to identify an emotion.<sup>13</sup> First, they take in the source (this may be text, audio, video, or biometric, as explained further below). Next, they extract key components of that source data for further analysis – for example, in facial recognition uses, it may identify the position of the eyebrows, how wide the eyes are, whether the mouth is open or closed, and so on. Finally, those key components are compared against training datasets that typically consist of a larger volume of similar key components that have been labeled or marked as correlating to a specific emotion. In identifying similar key components, the system then produces an output purporting to identify the emotion.

The source data used in an emotional recognition system could truly be any form of information, but current systems typically use one or more of the following:

- Video/image analysis: the most common of these focuses on facial expression analysis, but specific movements, gait, stance, posture, etc. may also be used in these visual systems
- Audio: audio analysis may use the content of what a person is saying, tone, volume, vocal stress, pitch, or more
- Text: text analysis will often identify key words or phrases or analyze content as a whole
- Physiology/biometrics: often generated from wearable devices, this data may include heart rate, pupil dilation, skin temperature, breathing rate, or more

*b. Intent and application of emotion recognition systems*

Broadly, the intent behind emotion recognition systems is to read, identify, and understand human emotions. This is often intended as a tool to allow for a human reaction to the identified emotion (seeing that someone is in distress and providing help, identifying aggression and addressing the

---

<sup>13</sup> See, e.g., Apriorit, *How does emotion recognition work?*, Medium (Jan. 5, 2024), <https://medium.com/that-feeling-when-it-is-compiler-fault/how-does-emotion-recognition-work-a94014389ff6>; *Facial emotion recognition: A complete guide*, Visage Technologies (Jul. 4, 2024), <https://visagetechologies.com/facial-emotion-recognition-guide/>.

possible threat, etc.), but some of these systems are designed to give machines emotional intelligence and the ability to simulate empathy.<sup>14</sup>

Though their applicability and usefulness are hotly contested (as discussed below), emotion recognition systems have already been used across multiple sectors and many more applications are envisioned. Currently, these systems are used in healthcare and wellness,<sup>15</sup> surveillance and security,<sup>16</sup>

---

<sup>14</sup> See, e.g., Sessa Bhargavi Velagaleti et al., *Empathetic Algorithms: The Role of AI in Understanding and Enhancing Human Emotional Intelligence*, J. Electrical Systems V. 20, Iss. 3s (2024), <https://www.proquest.com/openview/ebdccb03c2979c138444061f01dd87df/1?pq-origsite=gscholar&cbl=4433095>; Jale Narimisaei et al., *Exploring emotional intelligence in artificial intelligence systems: a comprehensive analysis of emotion recognition and response mechanisms*, Annals of Medicine & Surgery 86(8) (Aug. 2024), [https://journals.lww.com/annals-of-medicine-and-surgery/fulltext/2024/08000/exploring\\_emotional\\_intelligence\\_in\\_artificial.53.aspx](https://journals.lww.com/annals-of-medicine-and-surgery/fulltext/2024/08000/exploring_emotional_intelligence_in_artificial.53.aspx).

<sup>15</sup> Dr. Bertalan Mesko, *Ambient Intelligence And Emotion AI In Healthcare*, TMF (Jan. 12, 2023), <https://medicalfuturist.com/ambient-intelligence-and-emotion-ai-in-healthcare/>; *How Emotion Detection AI is Revolutionizing Mental Healthcare*, MoodMe (Mar. 15, 2024), <https://www.mood-me.com/how-emotion-detection-ai-is-revolutionizing-mental-healthcare/>; Muhammad Anas Hasnul et al., *Electrocardiogram-Based Emotion Recognition systems and Their Applications in Healthcare – A Review*, Sensors 2021, 21, 5015, available at <https://www.mdpi.com/1424-8220/21/15/5015>.

<sup>16</sup> Michael Standaert, *Smile for the camera: the dark side of China's emotion-recognition tech*, The Guardian (Mar. 3, 2021), <https://www.theguardian.com/global-development/2021/mar/03/china-positive-energy-emotion-surveillance-recognition-tech>; Alessia Dunn, *Smile, You're Being Watched: Disney Introduces Covert Cameras for Emotion Tracking, Records All Guests*, Inside the Magic (Sept. 11, 2024), <https://insidethemagic.net/2024/09/disney-adds-facial-recognition-parks-records-emotions-ad1/>; Nat Rubio-Licht, *Disney Could Bring Machine Learning to Parks' CCTV*, The Daily Upside (Jan. 4, 2024), <https://www.thedailyupside.com/technology/artificial-intelligence/disney-could-bring-machine-learning-to-parks-cctv/>.

the workplace,<sup>17</sup> education,<sup>18</sup> and criminal justice.<sup>19</sup> As the request for input specifically focused on workplace and education uses, we will limit our discussion to those areas.

## **II. Emotion Recognition Systems are Categorically Flawed and Violate EU Fundamental Rights**

*Responsive to Questions 1, 3, and 15*

Emotion recognition systems are dangerous tools that allow employers and school authorities to violate EU fundamental rights by instituting a mass surveillance system whose efficacy is unsubstantiated by scientific evidence. The conceit of these tools relies on heavily criticized studies that claim emotions are a) closely correlated to specific facial expressions and b) universal across all cultures.<sup>20</sup> Beyond their failed premise, these tools also exhibit various discriminatory biases and lack basic efficacy. This comedy of errors ends in a corrupt technology leveraged by people in positions of power to control the minutiae of students and employees, chilling free expression and violating various

---

<sup>17</sup> Dr. Aneish Kumar, *Behind the Smile: How Emotion Recognition Software Is Changing Job Interviews*, LinkedIn (Nov. 11, 2024), <https://www.linkedin.com/pulse/behind-smile-how-emotion-recognition-software-changing-kumar-m8quf/>; Angela Chen and Karen Hao, *Emotion AI researchers say overblown claims give their work a bad name*, MIT Tech. Rev. (Feb. 14, 2020), <https://www.technologyreview.com/2020/02/14/844765/ai-emotion-recognition-affective-computing-hirevue-regulation-ethics/>; Clem De Pressigny, *The creepy AI-driven surveillance that may be infiltrating your workplace*, Bsns. Insider (Nov. 20, 2023), <https://www.businessinsider.com/ai-surveillance-detects-emotion-at-work-gets-you-fired-2023-11>.

<sup>18</sup> EDPS, *Facial Emotion Recognition*, TechDispatch, Iss. 1 2021, available at [https://www.edps.europa.eu/system/files/2021-05/21-05-26\\_techdispatch-facial-emotion-recognition\\_ref\\_en.pdf](https://www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf); Angel Olider Rojas Vistorte et al., *Integrating artificial intelligence to assess emotions in learning environments: a systematic literature review*, *Frontiers in Psychology* (Jun. 19, 2024), <https://pmc.ncbi.nlm.nih.gov/articles/PMC11223560/>; Milly Chan, *This AI reads children's emotions as they learn*, CNN Bsns. (Feb. 17, 2021), <https://www.cnn.com/2021/02/16/tech/emotion-recognition-ai-education-spc-intl-hnk/index.html>.

<sup>19</sup> Tala Talaei Khoei and Aditi Singh, *A survey of Emotional Artificial Intelligence and crimes: detection, prediction, challenges and future direction*, 7 *J. of Comp. Social Sci.* 2359 (Jul. 17, 2024), <https://link.springer.com/article/10.1007/s42001-024-00313-3#citeas>; Lena Podoletz, "We have to talk about emotional AI and crime," *AI & Society* V. 38, Iss. 3, 1067 (May 5, 2022), available at <https://link.springer.com/article/10.1007/s00146-022-01435-w>.

<sup>20</sup> Kate Crawford et al., *2019 Report*, AI Now Inst. (Dec. 12, 2019), [https://ainowinstitute.org/wp-content/uploads/2023/04/AI\\_Now\\_2019\\_Report.pdf](https://ainowinstitute.org/wp-content/uploads/2023/04/AI_Now_2019_Report.pdf).

other fundamental rights guaranteed by the EU Charter of Fundamental Rights (“EU Charter”) and the General Data Protection Regulation (“GDPR”).

a. *Emotion recognition systems are unsubstantiated by scientific evidence and fail to address bias across cultures and other minority groups*

Emotion recognition systems are categorically flawed because the very goal of emotion recognition via external signifiers is likely impossible, as many have pointed out.<sup>21</sup> People often express emotions they are not actually feeling – for example, looking calm or amused when they are angry or under stress in order to soothe social situations or avoid conflict.<sup>22</sup> The expression and perception of emotion are also culturally and neurologically diverse, making any universal expression of emotion that these systems train on inaccurate across different groups of people. Finally, emotion recognition systems are often riddled with accuracy, bias, and reliability issues which furthers discrimination against protected groups like racial minorities.<sup>23</sup>

There is little evidence that the goal of these systems—identifying emotions from external data—is actually achievable. For example, emotion recognition systems using facial analysis rely on the faulty notion that certain facial muscle movements correlate with the feeling of a particular

---

<sup>21</sup> See, e.g., James Vincent, *Discover the Stupidity of AI Emotion Recognition with This Little Browser Game*, The Verge (Apr. 6, 2021), <https://www.theverge.com/2021/4/5/22369698/ai-emotion-recognition-unscientific-emojify-web-browser-game>; Kate Crawford, *Artificial Intelligence is Misreading Human Emotion*, The Atlantic (Apr. 27, 2021), <https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/>; Charlotte Gifford, *The Problem with Emotion-Detection Technology*, The New Economy (Jun. 15, 2020), <https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology>; Jay Stanley, *Experts Say ‘Emotion Recognition’ Lacks Scientific Foundation*, ACLU (Jul. 18, 2019), <https://www.aclu.org/news/privacy-technology/experts-say-emotion-recognition-lacks-scientific>.

<sup>22</sup> *Id.*

<sup>23</sup> For example, these systems often assign more threatening emotions to Black faces than White faces, regardless of expression. See Lauren Rhue, *Emotion-Reading Tech Fails the Racial Bias Test*, The Conversation (Jan. 3, 2019), <https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404>; Lauren Rhue, *Racial Influence on Automated Perceptions of Emotions*, SSRN, 1, 1 (2018), [https://papers.ssrn.com/so1113/papers.cfm?abstract\\_id=3281765](https://papers.ssrn.com/so1113/papers.cfm?abstract_id=3281765).

emotion, which can then be used to infer intent or motivation in a person’s mind.<sup>24</sup> A recent meta-analysis of over 1000 studies found that this attempted correlation has limited reliability, lacks specificity, and has limited generalizability.<sup>25</sup> Put simply, it doesn’t work.

First, the study found that the same category of emotion was not reliably expressed with or perceived from a common set of facial movements. Second, the study found that there is “no unique mapping between a single set of common facial movements” and instances of the same emotion. Finally, the study found that context and culture play a large role in the recognition of emotions, which algorithms do not account for. Other methods for engaging in emotion recognition, such as eye movement tracking,<sup>26</sup> auditory “aggression” detection,<sup>27</sup> and even human based monitoring for negative emotions,<sup>28</sup> similarly lack substantiating evidence of accuracy and efficacy. Even if an emotion recognition system could properly identify an emotion, it may still not be able to identify what triggered the emotion, any action the individual may take based on that action, other

---

<sup>24</sup> See, e.g., Douglas Heaven, *Expression of Doubt*, 578 *Nature* 502 (Feb. 27, 2020); Ifeoma Ajunwa, *Automated Video Interviewing as the New Phrenology*, 36 *Berkeley Tech. L.J.* 102 (2022).

<sup>25</sup> Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, 20 *Psychol Sci Pub. Int.* 1 (Dec. 2019), <https://pmc.ncbi.nlm.nih.gov/articles/PMC6640856/pdf/nihms-1021596.pdf>.

<sup>26</sup> Studies have debunked the idea that eye movement is a reliable indicator of lying; see, e.g., Richard Wiseman et al., *The Eyes Don’t Have It: Lie Detection and Neuro-Linguistic Programming*, 7 *PLoS ONE* (Jul. 12, 2012), available at <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0040259>. In fact, studies support the contrary, finding that the start position of the eyes, a marker that was thought to “indicate [that a] location is optimal for information extraction,” is the result of “a complex combination of visuo-motor effects and simple sampling strategies as well as cognitive factors” that are “very difficult to tease apart.” See Joseph Arizpe et al., *Start Position Strongly Influences Fixation Patterns during Face Processing: Difficulties with Eye Movements as a Measure of Information Use*, 7 *PLoS ONE* (Feb. 2, 2012), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3271097/>.

<sup>27</sup> Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (Jun. 25, 2019), <https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/>.

<sup>28</sup> GAO, GAO 14-159, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, 47 (2013), <https://www.gao.gov/assets/gao-14-159.pdf> (The United States Government Oversight Agency recommending limitation of funding to behavior detection activities because of lack of scientific evidence.).



characteristics about the person based on the emotional reaction to a particular situation, or any other internal feelings.<sup>29</sup>

Emotion recognition is further complicated by the fact that the expression and perception of emotions is culturally relative and riddled with bias. For example, western cultures and east Asian cultures associate different facial expressions with pain and pleasure.<sup>30</sup> Since there are often fundamental differences in cultural expression of emotions, it would be impossible for an emotion recognition system to account for all of these differences – a single facial expression could signal opposite emotions between cultures. There are often racial biases built into these systems as well. Racial minorities, particularly black people, are more often perceived as being aggressive by these systems and their facial expressions more likely to be linked to negative emotions than white counterparts, even when they have identical expressions.<sup>31</sup> This could have dire consequences, exacerbating bias and unfairness in employment, education, housing, finances, law enforcement, and more.<sup>32</sup>

*b. Emotion recognition systems are an egregious violation of the GPDR and EU fundamental rights*

Emotion recognition systems are neither necessary nor proportionate, and the problems they purport to solve can be addressed with less invasive means. Privacy and autonomy harms exist

---

<sup>29</sup> EDPS, *Facial Emotion Recognition*, TechDispatch, Iss. 1 2021, [https://www.edps.europa.eu/system/files/2021-05/21-05-26\\_techdispatch-facial-emotion-recognition\\_ref\\_en.pdf](https://www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf).

<sup>30</sup> Chen, C. et al., *Distinct facial expressions represent pain and pleasure across cultures*, Proc. Natl Acad. Sci. USA 115, E10013–E10021 (2018). <https://pmc.ncbi.nlm.nih.gov/articles/PMC6205428/>

<sup>31</sup> Lauren Rhue, *Racial Influence on Automated Perceptions of Emotions*, SSRN, 1, 1 (2018), [https://papers.ssrn.com/sol113/papers.cfm?abstract\\_id=3281765](https://papers.ssrn.com/sol113/papers.cfm?abstract_id=3281765); Paul Ekman and Wallace Friesen, *Universals and Cultural Differences in the Judgments of Facial Expressions of Emotion*, Journal of Personality and Social Psychology 53.4 (1987): 712-17; H. Elfinbein and N. Ambady, *Universals and Cultural Differences in the Judgements of Facial Expressions of Emotion*, Psychological Science, 12 (5), 159-164 (2003); K. Hugenberg and G. Bodenhausen, *Facing Prejudice: Implicit Prejudice and the Perception of Facial Threat*, Psychological Science, 14(6), 640-3 (2003), [https://www.researchgate.net/publication/222413010\\_Look\\_Black\\_in\\_Anger\\_The\\_Role\\_of\\_Implicit\\_Prejudice\\_in\\_the\\_Categorization\\_and\\_Perceived\\_Emoional\\_Intensity\\_of\\_Racially\\_Ambiguous\\_Faces](https://www.researchgate.net/publication/222413010_Look_Black_in_Anger_The_Role_of_Implicit_Prejudice_in_the_Categorization_and_Perceived_Emoional_Intensity_of_Racially_Ambiguous_Faces).

<sup>32</sup> See Section III.

regardless of the efficacy of the product, and several fundamental rights enshrined in the EU Charter of Fundamental Rights are implicated by the use of emotion recognition systems.

Emotion recognition systems violate both the GDPR and Articles 7 and 8 of the EU Charter. Emotion recognition relies heavily on the mass processing of biometric data points. Processing occurs both at the stage of developing and training an AI system as well as during the operational use of the technology. First, many of these algorithms, particularly the ones using facial recognition, train on data that is unlawfully scraped from the internet. The Dutch DPA recently released guidance on the limitations of scraping the internet for training data,<sup>33</sup> and the Court of Justice of the European Union (“CJEU”) has similarly been hesitant to allow indiscriminate data collection without further legal basis for processing requirements.<sup>34</sup> Second, highly sensitive data is also collected throughout operational use. Under the GDPR, a separate legal basis for processing such data is necessary for biometric data and other sensitive data.<sup>35</sup> The existence of these massive datasets also opens the door to data breaches, whereby sensitive data could be leaked.<sup>36</sup> Even if legal bases for processing are established for emotion recognition systems, any secondary processing (like notifying authorities or third parties of alerts raised) would require separate processing bases as each processing activity requires its own declared processing basis.<sup>37</sup>

Emotion recognition systems also run afoul of free expression and anti-discrimination protections. Instituting granular surveillance programs in the workplace and school settings risks

---

<sup>33</sup>Scraping door particulieren en private organisaties, Autoriteit Persoonsgegevens, (May 2024), <https://www.autoriteitpersoonsgegevens.nl/actueel/ap-scraping-bijna-altijd-illegaal>.

<sup>34</sup> CJEU, *Meta Platforms Inc and Others v Bundeskartellamt*, Case C-252/21, para. 126, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0252>.

<sup>35</sup> General Data Protection Regulation, 2016/679 Art. 6, 9. [Hereinafter “GDPR”].

<sup>36</sup> *See, e.g., The Changing Cyber Threat Landscape: Europe*, Cyfirma (Mar. 22, 2024) <https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-europe/>.

<sup>37</sup> GDPR Art. 6 and 9.

chilling free speech and expression, which are both rights enshrined in the EU Charter.<sup>38</sup> Free expression relies on freedom of thought, associational rights, and privacy in public. Engaging in surveillance of such intimate information like emotions of a person chills this expression and affects individual's behaviors. These systems also have low accuracy rates for racial minorities, children, the elderly, and disabled people, all of whom enjoy a right to freedom from discrimination under the EU Charter.<sup>39</sup>

Importantly, AI used in emotion recognition systems also creates a major liability question: who is at fault for the violations of these rights? The body creating the system, employing the system, or others? The EU charter guarantees the right to effective remedy,<sup>40</sup> but without appropriate liability chains, it is difficult for victims to get effective redress. Victims often are unaware that they have been subject to automated systems, particularly screening systems in the school and job application process.<sup>41</sup> The deployers of these systems also may be unaware of the deficiencies and limitations of the products they are using because of deceptive advertising by the system providers.

### **III. Emotion Recognition Has Widespread Application and Harm in Education and Workplaces**

*Responsive to Questions 1, 3, 4, 5, 7, 8, 9, 10, 12, and 13*

EPIC applauds the AI Act's ability to protect and empower students, educators, and workers through its ban on emotion recognition systems in education and workplace settings. As discussed in

---

<sup>38</sup> In the Case of *Glukhin v. Russia*, App. No. 11519/20 (Jul. 4, 2023), [https://hudoc.echr.coe.int/#%7B%22itemid%22:\[%22001-225655%22\]%7D](https://hudoc.echr.coe.int/#%7B%22itemid%22:[%22001-225655%22]%7D) (stating that the use of facial recognition in public is disproportionate in part because of the burden on free expression); see also Jeramie D. Scott, *Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, 12 J. Bus. & Tech. L. 151 (2017), <https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2>.

<sup>39</sup> EU Charter of Fundamental Rights 2000/C 364/01 Art. 21, 22, 23, 24, and 26.

<sup>40</sup> EU Charter of Fundamental Rights 2000/C 364/01 Art. 47.

<sup>41</sup> See, e.g., *À France Travail, l'essor du contrôle algorithmique*, La Quadrature du Net (Jun. 25, 2024), <https://www.laquadrature.net/2024/06/25/a-france-travail-lessor-du-controle-algorithmique/>.

Section II, emotion recognition systems operate based on fundamentally flawed assumptions, paltry research, and biased datasets. In fact, strong evidence supports the conclusion that emotion recognition will never be able to meet its claims. Despite this evidence and emotion recognition’s capacity for harm, use of emotion recognition systems has grown at an incredible rate in education and the workplace. In Section II, we established that there is little evidence that emotion recognition systems work. We stand by that assessment but examine the existing harms from these systems in education and the workplace that remain of critical concern whether or not the systems themselves function as intended.

a. *Using emotion recognition in education is counterproductive and threatens educators’ and students’ civil liberties while fostering distrust*

Emotion recognition systems deployed in school settings tend to fall under three main purposes: 1) tracking student performance, focus, and reaction to teaching materials; 2) surveilling students to detect cheating during exams; and 3) detecting violence or security breaches. Emotion recognition is not effective to achieve any of these purposes and also poses grave threats to students’ privacy, autonomy, freedom of expression, and right to be free from discrimination. Furthermore, the use of emotion recognition systems can create distrust between students and educators, create distractions, and undermine a supportive educational environment.

Increase in remote learning due to the pandemic, decrease in educational staffing and resources, and parents’ anxieties about the educational performance of their children have created a strong incentive for schools to use education aids – which emotion recognition systems often purport to be. For example, classrooms in China were reported to have cameras that snapped photos of student faces every second, analyzing student states such as whether students are “focused” based on whether

their gaze is directed at the board or “distracted” based on their rifling through the desk.<sup>42</sup> The system also noted whether students were sleeping, writing, answering questions, or engaging with other students.<sup>43</sup> One Chinese firm combines emotion recognition with academic performance to categorize students.<sup>44</sup> For instance, the ‘falsely earnest type’ is assigned to a student who ‘attentively listens to lectures [but has] bad grades.’<sup>45</sup> Another system tracks student faces for emotions and monitors how long students take to answer questions.<sup>46</sup> It combined this data with past grades and performance to report on strengths, weaknesses, motivation levels, and forecasts on their grades.<sup>47</sup> Obviously, this kind of categorization can have hugely detrimental effects by denying students with certain classifications opportunities, falsely labeling students due to incorrect assumptions, penalizing students with learning disabilities or neurological differences, and more. In 2017, the Ecole Supérieure de Gestion business school in Paris applied eye-tracking and facial expression-monitoring software to detect attention levels of online class attendees.<sup>48</sup> The system gave notifications to the student and the professor when the system assessed a student was not paying attention.<sup>49</sup>

Remote provision of exams during the pandemic also incentivized the adoption of technology that purports to detect cheating.<sup>50</sup> About half a dozen companies in the U.S. claim their software can

---

<sup>42</sup> Meaghan Tobin and Louise Matsakis, *China is home to a growing market for dubious “emotion recognition” technology*, Rest of World (Jan. 25, 2021), <https://restofworld.org/2021/chinas-emotion-recognition-tech/>.

<sup>43</sup> *Id.*

<sup>44</sup> *Emotional Entanglement: China’s emotion recognition market and its implications for human rights*, Article19 (Jan. 2021), <https://www.article19.org/emotion-recognition-technology-report/> [Hereinafter “Article19 Report”].

<sup>45</sup> *Id.*

<sup>46</sup> Milly Chan, *This AI reads children’s emotions as they learn*, CNN Bsns. (Feb. 17, 2021), <https://www.cnn.com/2021/02/16/tech/emotion-recognition-ai-education-spc-intl-hnk/index.html>.

<sup>47</sup> *Id.*

<sup>48</sup> A. Toor, *This French School is Using Facial Recognition to Find Out When Students Aren’t Paying Attention*, The Verge (May 26, 2017), <https://www.theverge.com/2017/5/26/15679806/ai-education-facial-recognition-nestor-france>.

<sup>49</sup> Milly Chan, *This AI reads children’s emotions as they learn*, CNN Bsns. (Feb. 17, 2021), <https://www.cnn.com/2021/02/16/tech/emotion-recognition-ai-education-spc-intl-hnk/index.html>.

<sup>49</sup> A. Toor, *This French School is Using Facial Recognition to Find Out When Students Aren’t Paying Attention*, The Verge (May 26, 2017), <https://www.theverge.com/2017/5/26/15679806/ai-education-facial-recognition-nestor-france>.

<sup>50</sup> Clive Thompson, *What AI College Exam Proctors Are Really Teaching Our Kids*, Wired (Oct. 20, 2020), <https://www.wired.com/story/ai-college-exam-proctors-surveillance/>.

accurately detect and prevent cheating in online tests.<sup>51</sup> One example is Respondus, a type of “online proctoring” software that locks down a student’s laptop so they cannot switch tabs, and uses visual AI to analyze the student, including their head movements to determine if they are looking at the screen or body movements that are deemed “suspicious.”<sup>52</sup> Because these systems monitor remote tests, they often film private living spaces of students, sometimes requiring the student to use the camera to show the entire room.<sup>53</sup> Professors can access the recordings and the student’s location is also accessible through the IP addresses.<sup>54</sup>

Many schools in the U.S. have installed emotion recognition systems claiming to increase safety. For example, companies using face and gesture recognition to detect “aggression” supplied schools in Florida and New York with their products, despite criticisms that predicting aggression based on emotion detection is extremely difficult, unproven, and frequently subject to bias.<sup>55</sup> Other emotion recognition systems use microphones to detect aggression<sup>56</sup> or screams.<sup>57</sup> One firm claims their system enables security officers to “engage antagonistic individuals immediately, resolving the conflict before it turns into physical violence.”<sup>58</sup> Device makers and school officials claim that

---

<sup>51</sup> Shea Swauger, *Software that monitors students during tests perpetuates inequality and violates their privacy*, MIT Tech. Rev. (Aug. 7, 2020), <https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/>.

<sup>52</sup> Clive Thompson, *What AI College Exam Proctors Are Really Teaching Our Kids*, Wired (Oct. 20, 2020), <https://www.wired.com/story/ai-college-exam-proctors-surveillance/>.

<sup>53</sup> Shea Swauger, *Software that monitors students during tests perpetuates inequality and violates their privacy*, MIT Tech. Rev. (Aug. 7, 2020), <https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/>.

<sup>54</sup> *Id.*

<sup>55</sup> Drew Harwell, *Parkland School Turns to Experimental Surveillance Software that can Flag Students as Threats*, Washington Post, (Feb. 13, 2019), <https://www.washingtonpost.com/technology/2019/02/13/parkland-school-turns-experimental-surveillance-software-that-can-flag-students-threats/>; Mariella Moon, *Facial Recognition is Coming to US Schools, Starting in New York*, Engadget (May 30, 2019), <https://www.engadget.com/2019-05-30-facial-recognition-us-schools-new-york.html>.

<sup>56</sup> Jack Gillum and Jeff Kao, *Aggression Detectors: The Unproven, Invasive, Surveillance Technology Schools Are Using to Monitor Students*, ProPublica, (Jun. 25, 2019), <https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/>.

<sup>57</sup> *Id.*

<sup>58</sup> *Id.*

deploying emotion recognition surveillance systems in public spaces like hallways and cafeterias will allow them to anticipate and prevent everything from mass shootings to underage smoking.<sup>59</sup>

There are many issues with attempting to use emotion recognition systems on students across all three purposes.

First, the data that the systems collect is intimate. Emotion recognition in schools collects and processes biometric data of students, which is considered sensitive personal information, making the technology inherently high-risk.<sup>60</sup> Voices and contents of conversation are also highly sensitive. However, at least one firm supplying “aggression detectors” in U.S. schools were reported to have microphones that allow administrators to record, replay, and store snippets of conversation indefinitely.<sup>61</sup> The European Court of Human Rights has already found that indefinite storage of biometric data violates the right to privacy, so this type of technology cannot be allowed in the EU.<sup>62</sup> Allowing the use of emotion recognition systems in schools also means that school administrators and technology companies will have access to deeply sensitive data about students. While the GDPR requires additional bases for processing data for a secondary purpose, such as sharing data with law enforcement or selling it to data brokers, students often have no visibility into the uses of these technologies and have no ability for redress should such a violation occur.

Next, the collection of such deeply sensitive data can easily lead to mission-creep, where the data is used for purposes other than what was originally declared. For example, some schools have used such technology to track students searching for terms relating to sexual orientation and gender identity, under the guise of preventing self-harm or searching for sexual materials, which resulted in

---

<sup>59</sup> *Id.*

<sup>60</sup> GDPR Art. 9.

<sup>61</sup> Jack Gillum and Jeff Kao, *Aggression Detectors: The Unproven, Invasive, Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (Jun. 25, 2019), <https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students>.

<sup>62</sup> *Case of S. and Marper v. the United Kingdom* [GC], no. 30562/04 30566/04 § 101-104 (Apr. 12, 2008).

outing the student to their parents and school administrators who are potentially hostile.<sup>63</sup> A report by the Center for Democracy and Technology also found that student monitoring ultimately resulted more in student discipline rather than keeping students safe.<sup>64</sup>

In addition, the power dynamics make it virtually impossible to obtain student consent in a school setting. Consent under GDPR must be freely given, informed and unambiguous, and specific.<sup>65</sup> Emotion recognition systems are used on all students in the physical or virtual classroom, regardless of an individual student's wishes. These systems can track their every move and are incentivized to over-report students as potentially at risk. Students often lack the power to withdraw consent or switch schools to avoid emotion recognition systems.

Further, none of the educational use cases have been shown to be accurate. For example, ProPublica analyzed one aggression detection tool in 2019.<sup>66</sup> The detector, which was trained in a Dutch pub district rather than an American educational setting, was less than reliable.<sup>67</sup> Cheering, loud laughter, and generally high-pitched rough or strained noises, like coughing, triggered the detector.<sup>68</sup> In security settings, officers may be overwhelmed by false alarms or students forced into unnecessary confrontations.<sup>69</sup>

---

<sup>63</sup> Alejandra Caraballo, *Remote Learning Accidentally Introduced a New Danger for LGBTQ Students*, Slate (Feb. 24, 2022), <https://slate.com/technology/2022/02/remote-learning-danger-lgbtq-students.html>; Marine Protais, *Orientation sexuelle ou politique... quand l'ia pretend lire sur nos visages*, L'AND (Jan. 18, 2021), <https://www.ladn.eu/tech-a-suivre/ia-machine-learning-iot/orientation-sexuelle-ou-politique-quand-lia-pretend-lire-sur-nos-visages/>.

<sup>64</sup> Elizabeth Laird et al., *Report-Hidden Harms: The Misleading Promise of Monitoring Students Online*, CDT (Aug. 3, 2022), <https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/>.

<sup>65</sup> GDPR Art. 7.

<sup>66</sup> Jack Gillum and Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (Jun. 25, 2019), <https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/>.

<sup>67</sup> *Id.*

<sup>68</sup> *Id.*

<sup>69</sup> Drew Harwell, *Parkland School Turns to Experimental Surveillance Software that can Flag Students as Threats*, Washington Post, (Feb. 13, 2019), <https://www.washingtonpost.com/technology/2019/02/13/parkland-school-turns-experimental-surveillance-software-that-can-flag-students-threats/>.



Even though the purported benefits of emotion recognition are illusory, the harms are real. Emotion recognition can exacerbate systematic inequities in school settings. As mentioned in Section II, many of the methods tech companies are using “reproduce racist, culturally biased assumptions about how humans express emotions.”<sup>70</sup> For example, proctoring software consistently prompted one black female university student “to shine more light on her face,” and denied her exam access because the system could not validate her identity.<sup>71</sup> Emotion recognition systems also tend to label disabled or neurodivergent students as suspicious.<sup>72</sup> Because different disabilities may affect how an individual looks, moves, communicates, expresses themselves, processes information, or copes with anxiety, they are at a higher risk of being flagged as suspicious when their demeanor simply differs from the majority.<sup>73</sup> Combining emotion recognition with facial recognition technology that has been shown over and over to be racist,<sup>74</sup> sexist,<sup>75</sup> and unable to shake the gender binary<sup>76</sup> imposes culturally biased and racist assumptions about how humans should act in any given situation and utilizes technology to impose majoritarian control over marginalized individuals.

---

<sup>70</sup> Meaghan Tobin and Louise Matsakis, *China is home to a growing market for dubious “emotion recognition” technology*, Rest of World (Jan. 25, 2021), <https://restofworld.org/2021/chinas-emotion-recognition-tech/>.

<sup>71</sup> Shea Swauger, *Software that monitors students during tests perpetuates inequality and violates their privacy*, MIT Tech. Rev. (Aug. 7, 2020), <https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/>; see also Mitchell Clark, *Students of color are getting flagged to their teachers because testing software can’t see them*, The Verge (Apr. 8, 2021), <https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning>.

<sup>72</sup> Lydia X. Z. Brown, *How Automated Test Proctoring Software Discriminates Against Disabled Students*, CDT (Nov. 16, 2020), <https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/>.

<sup>73</sup> *Id.*

<sup>74</sup> Karen Hao, *A US Government Study Confirms Most Face Recognition Systems are Racist*, MIT Tech. Rev. (Dec. 20, 2019), <https://www.technologyreview.com/2019/12/20/79/ai-face-recognition-racist-us-government-nist-study/>; see also James Cook, *‘Racist’ Passport Photo System Rejects Image of a Young Black Man Despite Meeting Government Standards*, The Telegraph (Sept. 19, 2019), <https://www.telegraph.co.uk/technology/2019/09/19/racist-passport-photo-system-rejects-image-young-black-man-despite/>.

<sup>75</sup> *Amazon Face-Detection Technology Shows Gender and Racial Bias, Researchers Say*, CBS News (Jan. 25, 2019), <https://www.cbsnews.com/news/amazon-face-detection-technology-shows-gender-racial-bias-researchers-say/>.

<sup>76</sup> Lisa Marshall, *Facial Recognition Software Has a Gender Problem*, CU Boulder Today (Oct. 8, 2019), <https://www.colorado.edu/today/2019/10/08/facial-recognition-software-has-gender-problem>.

These systems are not necessary nor proportionate, because the persistent surveillance and imposition of their normative rules creates emotional and psychological stress for students. Contrary to the technology's goals, engaging in such surveillance tactics may increase student distrust and alienation.<sup>77</sup> Rather than implementing solutions that get to the root of emotional distress in students, such as additional counseling, schools are opting for highly invasive, temporary technological bandages.<sup>78</sup>

Emotion recognition also threatens students' freedom to express and form opinions.<sup>79</sup> Imposing ideas of "right" ways to behave, express themselves, or look chills the right to freedom of expression. Students will be more vulnerable to this chilling effect.<sup>80</sup> The mass surveillance of students also chills the freedom to develop and express ideas anonymously, as well as their right to not speak, if surveillance brings to light beliefs that they did not want to express.<sup>81</sup> CDT's report on school surveillance reported that 58% of students reported refraining from sharing their honest thoughts because of monitoring.<sup>82</sup> Especially in a school setting where impressionable young students are meant to be developing skills and knowledge to express their own ideas and beliefs, educational institutions should not impose digital surveillance that will threaten to discriminate against their students and infringe on their rights to privacy, access to opportunities, and freedom of expression.

---

<sup>77</sup> Jack Gillum and Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (Jun. 25, 2019), <https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/>.

<sup>78</sup> *Id.*

<sup>79</sup> Article 19, *Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights* at 25-32 (Jan. 2021), <https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf>.

<sup>80</sup> *Id.* at 37; Hugh Grant-Chapman, Elizabeth Laird, and Cody Venzke, *Sustained Surveillance: Unintended Consequences of School-Issued Devices*, CDT Research (Sept. 21, 2021), <https://cdt.org/wp-content/uploads/2021/09/Sustained-Surveillance-One-Pager-Unintended-Consequences-of-School-Issued-Devices.pdf>.

<sup>81</sup> Article 19, *Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights* at 37 (Jan. 2021), <https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf>; Alejandra Caraballo, *Remote Learning Accidentally Introduced a New Danger for LGBTQ Students*, Slate (Feb. 24, 2022), <https://slate.com/technology/2022/02/remote-learning-danger-lgbtq-students.html>.

<sup>82</sup> Hugh Grant-Chapman, Elizabeth Laird, and Cody Venzke, *Sustained Surveillance: Unintended Consequences of School-Issued Devices*, CDT Research (Sept. 21, 2021), <https://cdt.org/wp-content/uploads/2021/09/Sustained-Surveillance-One-Pager-Unintended-Consequences-of-School-Issued-Devices.pdf>.

b. Emotion recognition is deployed across the lifespan of a job and poses significant threats to workers' dignity, privacy, and civil rights and liberties

Workplaces are often early adopters of harmful emerging technologies. AI is one such harmful technology.<sup>83</sup> In 2021, the Netherlands reported that 13 percent of employers used some form of AI, despite numerous examples of bias, discrimination, privacy violations, and more in the technology.<sup>84</sup> In 2023, the World Economic Forum estimated that 75% of surveyed employers would adopt AI.<sup>85</sup> Emotion recognition, which often is built with AI, is another harmful technology. And, as of 2023, over 50% of large U.S. employers across a wide array of industries—such as call centers, finance, health, retail, and caregiving—had adopted emotion recognition.<sup>86</sup> Companies that create and sell emotion recognition systems market them as solutions for all stages of the employment process: recruitment, employee retention and evaluation, and dismissal.<sup>87</sup> They promise that their system will reduce absenteeism, improve communication and productivity, support decision-making and

---

<sup>83</sup> See Grant Fergusson et al., *Generating Harms: Generative AI's Impact & Paths Forward*, EPIC (May 2023), <https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf> and Grant Fergusson et al., *Generating Harms II: Generative AI's New & Continued Impacts*, EPIC (May 2024), <https://epic.org/wp-content/uploads/2024/05/EPIC-Generative-AI-II-Report-May2024-1.pdf>.

<sup>84</sup> White House, *The Impact of Artificial Intelligence on the Future of Workforces in the European Union and the United States of America*, at 13, <https://www.whitehouse.gov/wp-content/uploads/2022/12/TTC-EC-CEA-AI-Report-12052022-1.pdf>.

<sup>85</sup> World Economic Forum, *Future of Jobs Report 6* (May 2023), [https://www3.weforum.org/docs/WEF\\_Future\\_of\\_Jobs\\_2023.pdf](https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf).

<sup>86</sup> Nazanin Andalibi, *Emotion-Tracking AI on the Job: Workers Fear Being Watched—and Misunderstood*, *The Conversation* (Mar. 6, 2024), <https://theconversation.com/emotion-tracking-ai-on-the-job-workers-fear-being-watched-and-misunderstood-222592>.

<sup>87</sup> See EDPS, *Facial Emotion Recognition*, *TechDispatch*, Iss. 1 at 2 (2021), available at [https://www.edps.europa.eu/system/files/2021-05/21-05-26\\_techdispatch-facial-emotion-recognition\\_ref\\_en.pdf](https://www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf); Karen Boyd and Nazanin Andalibi, *Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work*, *CSCW1 PACM on Human-Computer Interaction*, 95:23-29 (Apr. 2023); Calli Schroeder, Ben Winters, and John Davisson, *We Can Work It Out: The False Conflict Between Data Protection and Innovation*, 20 *Colo. Tech. L.J.* 251, 270 (2023); Scott Monteith, Tasha Glenn, et al., *Commercial Use of Emotion Artificial Intelligence (AI): Implications for Psychiatry*, 24 *Current Psychiatry Reports* 203 (2022); EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem* at 102 (Nov. 2022), <https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf>.

creativity, promote employee well-being, and identify employees at risk of quitting, patterns of workplace relations, and even security risks.<sup>88</sup>

Emotion recognition systems rely on incredibly invasive procedures to function. In addition to the biometric data discussed in Section I,<sup>89</sup> some systems may draw on information such as the worker's location, mobile data, medical and family data, and other personal data.<sup>90</sup> Workers are not easily able to avoid revealing this information, both due to the inherent power dynamic at play and the opaque nature of the technology. They may use company equipment in their homes, be required to install invasive applications on personal devices, or feel pressured to reveal information in order to keep their jobs. Workers are often unaware that emotion recognition is being deployed and, even when they are aware of its use, they are unlikely to understand how the system works or be in a position to refuse to engage with it.<sup>91</sup> This subjects workers to a “black box” where they are required to surrender personal information and submit to algorithmic evaluations that make authoritative claims about them.<sup>92</sup>

As discussed in Section II, emotion recognition systems pose significant harm to a worker's privacy, dignity, and autonomy. These systems also threaten the worker's livelihood and continued employment. Many emotion recognition systems will suggest which workers to promote or lay-off based on their perceived stress or their emotions toward colleagues, customers, and work tasks.<sup>93</sup>

---

<sup>88</sup> Scott Monteith, Tasha Glenn, et al., *Commercial Use of Emotion Artificial Intelligence (AI): Implications for Psychiatry*, 24 *Current Psychiatry Reports* at 206 (2022).

<sup>89</sup> See Section I.

<sup>90</sup> Karen Boyd and Nazanin Andalibi, *Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work*, CSCW1 PACM on Human-Computer Interaction, 95:14 (Apr. 2023).

<sup>91</sup> Alexander Hertel-Fernandez, *Estimating the Prevalence of Automated Management and Surveillance Technologies at Work and Their Impact on Workers' Well-Being*, Washington Center for Equitable Growth (Oct. 1, 2024), <https://equitablegrowth.org/research-paper/estimating-the-prevalence-of-automated-management-and-surveillance-technologies-at-work-and-their-impact-on-workers-well-being/>.

<sup>92</sup> Ifeoma Ajunwa, *The “Black Box” at Work*, 7 *Big Data & Society* 1 (Oct. 19, 2020).

<sup>93</sup> Karen Boyd and Nazanin Andalibi, *Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work*, CSCW1 PACM on Human-Computer Interaction, 95:17 (Apr. 2023).

Workers are rightly concerned that the recommendations of such systems will not be questioned despite the system's unreliability and reliance on unstable norms.<sup>94</sup> These concerns invisibly add more work to the individual worker's plate as they now need to perform emotional labor, or labor to manage the performance of their own emotions to conform to the system's normative expectations.<sup>95</sup> This contradicts the point of these systems in many ways. Workers will either spend less time on productive tasks or deal with more stress, burnout, and safety risks while attempting to keep pace with their standard and emotional workloads.<sup>96</sup>

Emotion recognition systems also blur the boundaries between personal and workplace problems and prompt workers to reveal medical or mental health information that the worker may prefer to keep private. This may occur in different ways. Several emotion recognition systems alert supervisors to the worker's perceived negative emotional state or automatically enact security protocols that alert law enforcement and shut off employee system access.<sup>97</sup> A few systems even recommend diagnoses or contact mental health professionals.<sup>98</sup> These system actions force

---

<sup>94</sup> Nazanin Andalibi, *Emotion-tracking AI on the job: Workers Fear Being Watched—and Misunderstood*, The Conversation (Mar. 6, 2024), <https://theconversation.com/emotion-tracking-ai-on-the-job-workers-fear-being-watched-and-misunderstood-222592>; see also, Alexander Hertel-Fernandez, *Estimating the Prevalence of Automated Management and Surveillance Technologies at Work and Their Impact on Workers' Well-Being*, Washington Center for Equitable Growth (Oct. 1, 2024), <https://equitablegrowth.org/research-paper/estimating-the-prevalence-of-automated-management-and-surveillance-technologies-at-work-and-their-impact-on-workers-well-being/>.

<sup>95</sup> Karen Boyd and Nazanin Andalibi, *Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work*, CSCW1 PACM on Human-Computer Interaction, at 4, 22-24 (April 2023).

<sup>96</sup> See Alexander Hertel-Fernandez, *Estimating the Prevalence of Automated Management and Surveillance Technologies at Work and Their Impact on Workers' Well-Being*, Washington Center for Equitable Growth (Oct. 1, 2024), <https://equitablegrowth.org/research-paper/estimating-the-prevalence-of-automated-management-and-surveillance-technologies-at-work-and-their-impact-on-workers-well-being/> (discussing how automated productivity tracking can cause workers to increase pace and result in injury, anxiety, and stress).

<sup>97</sup> Karen Boyd and Nazanin Andalibi, *Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work*, CSCW1 PACM on Human-Computer Interaction at 20 (Apr. 2023).

<sup>98</sup> *Id.*

uncomfortable interactions and put pressure on the worker to disclose information in order to complete job tasks, avoid law enforcement interactions, or keep their jobs.<sup>99</sup>

Emotion recognition systems also threaten worker autonomy by limiting the worker's authority over their position and putting pressure on collective workplace action. For example, several systems respond to emotion input by creating unnecessary meetings, ignoring worker commands, or redirecting work tasks.<sup>100</sup> These system actions limit worker autonomy. Instead of the worker maintaining discretion, the system now determines what they may do in the workplace and when. The ever-watchful systems also limit the ability of the worker to leverage power individually or collectively. Any system of constant surveillance threatens to chill collective action. However, emotion recognition systems also monitor workers to identify patterns of worker interaction and produce risk scores that predict worker dissatisfaction based on perceived negative emotions. This allows employers to identify and lay off dissatisfied workers who may be engaging in protected activity while using the pretext of the system's output to shield their actions.

#### **IV. Recommendations**

*Responsive to Questions 4, 5, 6, 9, 10, 12, 13, and 15*

- a. *The AP should decline to make exceptions to Prohibition F given the limits of emotion recognition and the severe risks of discrimination and harm to civil rights and liberties posed by emotion recognition systems*

The AI Act limits the scope of Prohibition F to allow for AI systems intended to be used strictly for medical or safety reasons.<sup>101</sup> However, emotion recognition systems are based on research with

---

<sup>99</sup> See Calli Schroeder, Ben Winters, and John Davisson, *We Can Work It Out: The False Conflict Between Data Protection and Innovation*, 20 Colo. Tech. L.J. at 266-276 (2023).

<sup>100</sup> Karen Boyd and Nazanin Andalibi, *Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work*, CSCW1 PACM on Human-Computer Interaction at 21 (Apr. 2023).

<sup>101</sup> AI Act Art.5(1)(f) (2024).

shoddy methodology as well as unsupported assumptions that states like pain and emotion are universally felt and presented.<sup>102</sup> Further, emotion recognition has serious technological limitations and entrenches biases and discrimination.<sup>103</sup> Emotion recognition is not required to support the medical and safety needs of workers and students and is more likely to cause harm than good. For these reasons, EPIC recommends that the AP implement Prohibition F with no exceptions, even for safety and medical uses. If the AP declines to prohibit the use of emotion recognition systems altogether, we urge it to draw the medical and safety exceptions narrowly considering emotion recognition’s limitations and high likelihood for harm and misuse.

Several emotion recognition systems claim to be able to detect criminal or terrorist intent through biometrics-based emotion analysis, including systems intended to be used in workplaces and schools.<sup>104</sup> This is not based on sound science.<sup>105</sup> Like attempts to measure other emotions or intentions, the concept of criminal intent is vague and incapable of external measurement.<sup>106</sup> Further, the systems are primed to discriminate against already marginalized communities such as disabled people and people of color.<sup>107</sup> As discussed in Section II, emotion recognition systems are particularly bad at labeling the emotions of people with disabilities, people with neurodivergences, and people of color.<sup>108</sup>

---

<sup>102</sup> See Section II.

<sup>103</sup> *Id.*

<sup>104</sup> Karen Boyd and Nazanin Andalibi, *Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work*, CSCW1 PACM on Human-Computer Interaction at 202-23 (Apr. 2023); see also Niamh Kinchin, *AI facial analysis is scientifically questionable. Should we be using it for border control?*, The Conversation (Feb. 23, 2021), <https://theconversation.com/ai-facial-analysis-is-scientifically-questionable-should-we-be-using-it-for-border-control-155474> (discussing the use of emotion recognition and other systems at European borders); EPIC, Comments to the U.S. Dep’t of Justice and Dep’t of Homeland Security at 42 (Jan. 19, 2024), <https://epic.org/wp-content/uploads/2024/01/EPIC-DOJDHS-Comment-LE-Tech-011924.pdf> (discussing the use of emotion recognition to prevent school shootings).

<sup>105</sup> EPIC, Comments to the U.S. Dep’t of Justice and Dep’t of Homeland Security at 42-46 (Jan. 19, 2024), <https://epic.org/wp-content/uploads/2024/01/EPIC-DOJDHS-Comment-LE-Tech-011924.pdf>.

<sup>106</sup> *Id.*

<sup>107</sup> See Section II.

<sup>108</sup> *Id.*

emotion recognition entrenches biases against these individuals by setting ableist and racist emotional norms and forcing individuals who deviate from the norms into unnecessary, dangerous, and stigmatizing confrontations with law enforcement. Rather than being an objective safety tool, emotion recognition feels like an echo of the long-debunked pseudoscience of phrenology.<sup>109</sup>

Using emotion recognition systems for security compromises the civil rights and liberties of individuals. As discussed in Section I, the attribution of emotions is determined by the party deploying the technology, which collects and categorizes the information. This raises serious potential for misuse, as someone could identify particular non-normative traits to target. In effect, the systems can be used to identify and harass minority groups. Using emotion recognition for security further implicates the right against self-incrimination as enshrined in Article 14(3)(g) of the ICCPR.<sup>110</sup> Because emotion recognition systems claim to detect and signal guilt, an emotional state, the systems invert this right and infringe on personal freedoms.<sup>111</sup> Furthermore, the CJEU has been trending towards restricting member state national security interests in favor of fundamental rights enshrined in the EU Charter, so the AP has the competency to limit the safety exemption in its implementation of the AI Act.<sup>112</sup>

Finally, emotion recognition systems are unnecessary to support the safety and medical needs of students and workers. For example, vehicle operation is a frequently cited safety use case for emotion recognition.<sup>113</sup> However, emotion recognition is not necessary for recognizing whether an

---

<sup>109</sup> See, e.g., EPIC, Comments to the Office of the Privacy Commissioner of Canada Regarding the Update to Guidance on Handling Biometric Information (Jan. 12, 2024), <https://epic.org/documents/comments-of-epic-to-the-office-of-the-privacy-commissioner-of-canada-regarding-the-update-to-guidance-on-handling-biometric-information/>.

<sup>110</sup> International Covenant on Civil and Political Rights, Art. 14(g) (1966).

<sup>111</sup> See Article 19, *Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights* (Jan. 2021), <https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf>.

<sup>112</sup> See, e.g., *Kadi v. Al Barakaat International Foundation* C-402/05 P, C-415/05 P (2008).

<sup>113</sup> See, e.g., EDPS, *Facial Emotion Recognition*, TechDispatch, Iss. 1 2021, available at [https://www.edps.europa.eu/system/files/2021-05/21-05-26\\_techdispatch-facial-emotion-recognition\\_ref\\_en.pdf](https://www.edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf); *In-Cabin Sensing AI*, Affectiva.com (last accessed Dec. 13, 2024), <https://www.affectiva.com/product/in-cabin-sensing-ai/>.



individual is falling asleep at the wheel. For example, regulations address drowsiness by restricting driving time and mandating breaks.<sup>114</sup> Technology already exists to monitor driving time, sense steering wheel changes,<sup>115</sup> and detect swerving.<sup>116</sup> Further, better and more proportionate legislative supports for transportation and other high-stress workers are the solution to a tired, hungry, and distracted workforce—not invasive emotion recognition. The same can be said for education. Emotion recognition is touted as a solution for disengaged students because it claims to interpret a student’s emotional state and adjust curriculums or measure engagement. But support for students and education workers is far more likely to address these issues than emotion recognition.

Emotion recognition systems are capable of creating or facilitating great harm to the autonomy, dignity, privacy, and freedom of workers, students, and educators. For these reasons, EPIC urges the AP to strengthen Prohibition F by prohibiting emotion recognition systems in education and workplaces altogether and declining to include medical and safety exceptions. If the AP instead opts to include these exceptions to Prohibition F, we urge it to draw the exceptions for emotion recognition systems narrowly and consider further steps it could take to mitigate the harms posed by the technology.

*b. The AP should clarify that Prohibition F applies to systems that have the effect of inferring or identifying emotion or intent in order to resolve ambiguity in the Prohibition*

Prohibition F applies to the emotions or intentions of natural persons. However, as the AP notes in its call for input, Prohibition F does “not include the detection of readily apparent expressions, gestures, or movements, unless they are used to identify or infer emotions.”<sup>117</sup> This limitation on the

---

<sup>114</sup> Regulation (EC) No. 561/2006.

<sup>115</sup> *Driver Drowsiness Detection*, Bosch-Mobility.com, <https://www.bosch-mobility.com/en/solutions/assistance-systems/driver-drowsiness-detection/> (last accessed Dec. 16, 2024).

<sup>116</sup> Morgan Carter, *Driver Fatigue Detection Systems: How does Anti-Sleep Tech Work?* CarBuzz.com (Oct. 7, 2022), <https://carbuzz.com/car-advice/driver-fatigue-detection-systems-how-does-anti-sleep-tech-work/>.

<sup>117</sup> *Id.*

scope of Prohibition F is unclear. Companies will exploit this language as a loophole, agreeing that emotion recognition systems cannot identify a person’s inner state in order to exempt their systems that have the effect of inferring or identifying emotions. For example, the AI company Retorio states that its AI coaching technology for customer service employees is not subject to the AI Act because its AI is simply “checking facial expressions.”<sup>118</sup> However, its AI suggests to employees how others may emotionally label their facial expression—essentially completing the task of emotion recognition. We urge the AP to clarify that systems that have the effect of inferring or identifying emotion are considered emotion recognition systems subject to Prohibition F.

## CONCLUSION

EPIC appreciates the significant efforts AP has made in carefully considering how best to implement the AI Act and the various technologies it encompasses. We strongly believe that emotion recognition systems should be prohibited in the workplace and education for the reasons delineated above. Emotion recognition has failed to demonstrate its usefulness but has repeatedly succeeded in demonstrating substantial harms to the rights and lives of EU residents. Due to the high risks related to this technology, we urge the AP to (i) either fully ban emotion recognition systems with no exceptions or draw exceptions for medical and safety reasons extremely narrowly and with adequate protections in place and (ii) clarify that Prohibition F applies to systems intended to infer or identify emotion or intent whether or not the system is successful in doing so. We believe that taking these actions will strengthen privacy and human rights protections for EU residents, guard against extending surveillance through emotion recognition systems, and further establish the AP as a leader in protecting human rights in the face of emerging technology. We are happy to be explicitly mentioned

---

<sup>118</sup> See *What is the AI Act?*, Retorio.com (last accessed Dec. 13, 2024), <https://www.retorio.com/en/ai-act>.

in the AP's public response, if that is useful, and are willing to provide any additional clarification, discussion, or resources desired.

Respectfully submitted,

/s/ Abigail Kunkler

Abigail Kunkler  
EPIC Law Fellow

/s/ Calli Schroeder

Calli Schroeder  
EPIC Senior Counsel, Global Privacy Counsel,  
and AI and Human Rights Lead

/s/ Mayu Tobin-Miyaji

Mayu Tobin-Miyaji  
EPIC Law Fellow

/s/ Maria Villegas Bravo

Maria Villegas Bravo  
EPIC Law Fellow