epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

FEEDBACK OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

EUROPEAN COMMISSION

Regarding the

PROPOSAL FOR HARMONIZED RULES ON ARTIFICIAL INTELLIGENCE

August 06, 2021

The Electronic Privacy Information Center ("EPIC") submits the following feedback to the European Commission's Proposal for Harmonized Rules on Artificial Intelligence (hereinafter, the Artificial Intelligence Act or "AIA").[1]

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and human rights issues and to protect privacy, freedom of expression, and democratic values in the information age.[2] EPIC has a long history of promoting transparency and accountability for the use of systems with potential high-risk impacts on data subjects, at both a national and international level.[3] EPIC has litigated cases against the U.S. Department of Justice for documents regarding "risk assessment tools"[4] and against the U.S. Department of Homeland Security for documents about a program to assess the

---

[1] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021) 206 final (Apr. 21, 2021).

[2] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html.

[3] *See* e.g. Comments of EPIC, *Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics,* Federal Trade Commission (Aug. 20, 2018), https://epic.org/apa/comments/EPIC-FTC-Algorithmic-Transparency-Aug-20-2018.pdf; Comments of EPIC, *Developing UNESCO's Internet Universality Indicators: Help UNESCO Assess and Improve the Internet,* United Nations Educational, Scientific and Cultural Organization ("UNESCO") (Mar. 15, 2018), 5-6, https://epic.org/internetuniversality/EPIC_UNESCO_Internet_Universality_Comment%20(3).pdf; EPIC v. DOJ (D.C. Cir.) (18-5307), https://epic.org/foia/doj/criminal-justice-algorithms/; Comments of EPIC, *Proposal for a Legal Act of the European Parliament and the Council Laying Down Requirements for Artificial Intelligence,* European Commission (Sep. 10, 2020), https://epic.org/apa/comments/EPIC-EU-Commission-AI-Sep2020.pdf; Comments of EPIC, *Intellectual Property Protection for Artificial Intelligence Innovation*, U.S. Patent and Trademark Office (Jan. 10, 2020), https://epic.org/apa/comments/EPIC-USPTO-Jan2020.pdf; Testimony of EPIC, Massachusetts Joint Committee on the Judiciary (Oct. 22, 2019), https//epic.org/testimony/congress/EPIC-FacialRecognitionMoratorium-MA-Oct2019.pdf; Statement of EPIC, *Industries of the Future,* U.S. Senate Committee on Commerce, Science & Transportation (Jan. 15, 2020), https://epic.org/congress/EPIC-SCOM-AI-Jan2020.pdf; Comments of EPIC, *Request for Information: Big Data and the Future of Privacy,* Office of Science and Technology Policy (Apr. 4, 2014); EPIC, *Algorithmic Transparency* (2018), https://www.epic.org/algorithmic-tranparency/; EPIC, *Algorithms in the Criminal Justice System* (2018), https://www.epic.org/algorithmic-transparency/crim-justice/.

[4] EPIC, *EPIC v. DOJ (Criminal Justice Algorithms),* https://epic.org/foia/doj/criminal-justice-algorithms/.

probability that an individual may commit a crime in the future.[5] In 2018, EPIC, together with leading scientific societies, successfully petitioned the U.S. Office of Science and Technology Policy to solicit public input on U.S. Artificial Intelligence Policy.[6] EPIC has recently submitted comments relating to the AI system classification framework proposed by the OECD as well.[7]

While EPIC concurs that regulation of AI systems is desperately needed, EPIC believes that the AIA would not meaningfully address the identified privacy and human rights concerns related to use of AI systems. In particular, the combination of vague language and broad exemptions undermines the purpose of the AIA. In order to create more robust and meaningful protections and to remedy the current shortcomings of the AIA, EPIC recommends the following actions be taken:

- Close loopholes and remove exemptions on regulatory requirements for AI systems and expand prohibitions where necessary
- Mandate that individuals subject to AI system decision-making be notified prior to use of the system
- Fully ban emotion recognition and biometric categorization systems
- Require that conformity assessments be reviewed and approved by data protection authorities prior to use

EPIC urges the Commission to close the multiple exemptions and loopholes on regulatory requirements for AI systems within the AIA

The AIA contains extensive AI systems use requirements that appear to protect user privacy and curtail unnecessary or high-risk use. However, the current proposal undercuts its own impact by including numerous exceptions and loopholes. These gaps in protection would functionally allow for extensive use of AI systems that are high-risk, unnecessary, and manipulative while the existence of the AIA would give individuals a false sense of protection. We have highlighted the most significant exceptions—both those explicitly written into the AIA and those stemming from lack of clarity—that we propose be modified or removed in order to provide adequate protections for individuals.

First, the current draft purports to specifically prohibit certain systems—that is, artificial intelligence systems which use subliminal techniques to affect a person's behavior, exploit any vulnerability of a group due to age or disability, classify or evaluate a person's trustworthiness, or use "real-time" remote biometric identification in publicly accessible spaces for law enforcement.[8] However, the prohibitions are too narrowly drafted, applying solely to a small

[5] *See id.;* EPIC, *EPIC v. DHS (FAST Program),* https://epic.org/foia/dhs/fast/.
[6] EPIC, Petition to OSTP for Request for Information on Artificial Intelligence Policy (July 4, 2018), https://epic.org/privacy/ai/OSTP-AI-Petition.pdf.
[7] Comments of EPIC, *OECD Framework for Classifying AI Systems,* Organisation for Economic Cooperation and Development (June 30, 2021), https://epic.org/apa/comments/EPIC-Comments-OECD-AI-Classification-Framework-06-2021.pdf.
[8] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at Title II, Article 5(1)(a-d), COM (2021) 206 final (Apr. 21, 2021).

subset of harmful systems.[9] As an example of how the drafted scope severely limits application to AI systems, consider systems that use subliminal techniques.[10] According to the AIA, these systems may not be used if they (i) deploy subliminal techniques which are (ii) beyond a person's consciousness (iii) for the purpose of materially distorting a person's behavior (iv) in a manner that causes or is likely to cause that person or another person physical or psychological harm.[11] All of these factors must be present in order for the system to be banned.

Evaluating whether these elements are all present for a given system (and, thus, determining that the system should be prohibited) would be a highly subjective exercise that could lead to varied and inconsistent enforcement. How would an enforcement body determine whether the system materially distorted a person's behavior? How would an enforcement body conduct that evaluation? What level of technical and psychological expertise would be required to make the determination that a person's behavior was affected by a system, much less that the distortion was material? How can a person prove that techniques beyond their consciousness actually distorted their behavior when they would, presumably, be unaware of any techniques beyond their consciousness? The lack of clear answers or even methods for determining answers to these questions undermine the impact of this rule.

It is also unnecessarily limiting to only focus on physical and psychological harms caused by these systems, which would leave unaddressed a broad swathe of damage inflicted by manipulative AI. Indeed, the fact that an AI system is designed to intentionally and subliminally manipulate individuals should in and of itself be considered harm enough to trigger the prohibition. As mentioned in other analyses of the AIA, the specificity of the harm requirement severely limits the impact and scope of this prohibition, excluding reputational harms, financial, employment, educational, social, and more.[12] In addition, as many have already noted, this limitation would completely ignore the effects of cumulative harms.[13] We note that these harms are also disproportionately impactful on already-vulnerable groups, including minorities, the disabled, trans and non-binary individuals, the socioeconomically disadvantaged, and others.

An additional problem with these purported prohibitions—beyond the overly narrow definitions illustrated above—is an overabundance of exemptions. Let us consider another "prohibited" system type: real-time remote biometric identification systems in publicly accessible spaces.[14] In order for the prohibition to apply, several factors must be present and

---

[9] *Id.*
[10] *Id.* at Title II, Article 5(1)(a).
[11] *Id.*
[12] Michael Veale and Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act,* at 4, SocArXiv (July 6, 2021) (Noting "[a] cynic might feel the Commission is more interested in prohibitions' rhetorical value than practical effect.").
[13] *Id.* ("In real life, harm can accumulate without a single event tripping a threshold of seriousness, leaving it difficult to prove. These 'cumulative' harms are reinforced over time by their impact on individuals' environments…").
[14] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at Title II, Article 5(1)(d), COM (2021) 206 final (Apr. 21, 2021).

multiple exceptions may apply even where all factors are present, severely weakening the value of the prohibition.[15] The prohibition applies to use of (i) real time (ii) remote (iii) biometric identification systems (iv) in publicly accessible spaces (v) for the purposes of law enforcement.[16] These systems are NOT prohibited if their use is considered "strictly necessary" for targeted search for specific potential victims of crime; prevention of a specific, substantial, and imminent threat to the life or safety of natural persons or a terrorist attack; or pursuit of a suspect of a dizzying array of crimes (ranging from human trafficking, terrorism, and murder to computer crime, racism, corruption, and fraud).[17]

The AIA describes a balancing test weighing the potential harm if the system is not used against the potential impacts on the rights and freedoms of affected individuals if the system is used, stating that this test should be applied prior to use of a system for any of the listed exceptions and that necessary and appropriate safeguards should be applied.[18] Prior authorization is generally required to rely on of one of the listed exceptions—however, this requirement is waived until after use in "urgent" situations.[19] In addition, while competent authorities may be pre-authorized for "individual use" of a biometric system, it is unclear whether an "individual use" may be for thematic (i.e. broadly applicable to organizations, places, or purposes) or individual purposes, which would significantly broaden the pre-authorization scope.[20]

The extensive exemptions detailed above for real-time remote biometric tracking—combined with the option for Member States to authorize use of these systems in broad terms[21]—severely weaken the protections against biometric surveillance. Setting aside the numerous exceptions listed, the phrasing of the prohibition presents a veneer of limiting biometric surveillance while functionally allowing biometric tracking practices to continue with only minor inconvenience. The "real-time" stipulation allows for European law enforcement agency use of recognition software services like Clearview AI or Poland-based PimEyes on previously recorded footage or images to identify individuals, track their movements, and attempt to link their behavior to certain social categories.[22] The regulation also permits use of biometric identification systems to recognize sensitive characteristics, such as an individual's gender, sexuality, race, or ethnicity, leaving open the possibility of perpetuating existing harms

[15] *Id.* at Title II, Article 5(1)(d)(i-iii).
[16] *Id.* at Title II, Article 5(1)(d).
[17] *Id.* at Title II, Article 5(1)(d)(i-iii); Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, Article 2(2), 2002/584/JHA.
[18] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at Title II, Article 5(2), COM (2021) 206 final (Apr. 21, 2021).
[19] *Id.* at Title II, Article 5(3).
[20] *See* Veale and Zuiderveen Borgesius, *supra* note 12, at 8 (Giving examples of individual purposes that may be pre-authorized, including "biometrics related to all those on a missing children list or subject to a European Arrest Warrant.").
[21] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at Title II, Article 5(4), COM (2021) 206 final (Apr. 21, 2021).
[22] *See* Amba Kak, *Regulating Biometrics: Global Approaches and Urgent Questions*, AI Now Institute (Sept. 2020), https://ainowinstitute.org/regulatingbiometrics.pdf.

towards historically marginalized communities and individuals.[23] Rather than enhancing community safety and security, the proposed regulation functionally permits the indiscriminate use of biometric recognition technologies in the public sphere so long as that recognition does not occur in real time under extremely particular circumstances.

This prohibition is limited to use for law enforcement purposes, allowing for biometric surveillance by private companies or actors, which would limited only by existing regulations, such as the General Data Protection Regulation. This is not a hypothetical impact. Such systems are already in use by private companies in the EU.[24] Finally, this modified "prohibition" falls far short of recommendations from public bodies and NGOs related to use of automated recognition systems in publicly accessible spaces.[25] As demonstrated here and above, the prohibitions listed in Article 5(1) of the AIA offer a façade of protection rather than the real thing.[26]

The scope of these exemptions would be incredibly broad. For example, AI systems developed or used exclusively for military purposes do not fall under the AIA.[27] Public authorities and international organizations using AI systems under international law enforcement or judicial cooperation agreements with the EU or Member States are also fully exempt.[28] All of these exemptions and gaps add to the sense that many, if not most, invasive AI systems and their use would be relatively unaffected by the AIA.

EPIC recommends that an explicit requirement to inform any data subjects who may be affected by AI decision making be added to the regulation

Requirements to inform affected individuals of processing by AI systems are limited in the current AIA and, when present, are not always consistent or clear. EPIC recommends that an

---

[23] *See e.g.*, Claudia Garcia-Rojas, *The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies*, Truthout (Mar. 3, 2016), https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police (Discussing Professor Simone Brown's research on how race and anti-Black colonial logics inform contemporary surveillance practices); James Vincent, *The Invention of AI 'Gaydar' Could be the Start of Something Much Worse*, The Verge (Sept. 21, 2017), https://www.theverge.com/2017/9/21/16332760/ai-sexuality-gaydar-photo-physiognomy.

[24] *See e.g.* Luca Montag, Rory Mcleod, Lara De Mets, Meghan Gauld, Fraser Rodger, and Mateusz Pelka, *The Rise and Rise of Biometric Mass Surveillance in the EU: A Legal Analysis of Biometric Mass Surveillance Practices in Germany, The Netherlands, and Poland,* European Digital Rights (July 7, 2021), available at https://edri.org/wp-content/uploads/2021/07/EDRI_RISE_REPORT.pdf; Matt Burgess, *"Europe makes the case to ban biometric surveillance,"* Wired (July 7, 2021), https://www.wired.co.uk/article/europe-ai-biometrics.

[25] *See* European Data Protection Board, "Guidelines 3/2019 on Processing of Personal Data through Video Devices (Version 2.0)," EDPB (Jan. 29, 2020); the "Reclaim Your Face" campaign with over 60 NGOs in support, https://reclaimyourface.eu/.

[26] *See e.g.* Friederike Reinhold, "AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – A major step with major gaps," AlgorithmWatch (April 22, 2021), https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/; Veale and Zuiderveen Borgesius, *supra* note 12 at 8.

[27] *See Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at Title I, Article 2(3), COM (2021) 206 final (Apr. 21, 2021).

[28] *Id.* at Title I, Article 2(4).

explicit requirement to inform data subjects who may be affected by AI decision making be added to the regulation, including notice to individuals affected by AI-generated recommendations even where humans take part in the final action.[29] EPIC urges the Commission to consider mandating that notification be given prior to system use, along with an option to reject or challenge the use of AI decision making.

A key inadequacy of the AIA is a lack of mandatory notification—particularly where automated decision-making systems are used. The proposal currently requires that people only be informed when they "interact with" an AI system, encounter a system that generates or manipulates content into "deep fakes," or when their emotions or characteristics are recognized through automated means.[30] The current draft does not define what constitutes an "interaction" with an AI system. Further, the AIA mandates notification to users that interact with an AI system UNLESS this is obvious from circumstances and context—a significant loophole.[31] What would render interaction with an AI system "obvious" is left undefined. The mandate to inform in each of the listed cases does not apply if the system is used to detect, prevent, investigate, or prosecute criminal offenses.[32]

Imposing a notice requirement across both "high-risk" and "non-high-risk" AI systems would rightfully reflect an understanding of the dangers all AI systems pose to fundamental rights, regardless of whether or not the Commission has designated them as "deserving special consideration."[33] However, the proposed legislation stops short of providing meaningful information and transparency to individuals by limiting notification requirements to just three circumstances. There is no notification requirement for other "high risk" uses of AI systems, such as the use of AI-assisted decision-making systems for benefits eligibility, credit, education, or employment.[34] Despite the limited notice requirements present in the AIA (and discussed above), the existing transparency requirements are ultimately insufficient to ensure adequate transparency, fairness, and accountability in the design, development, and deployment of AI systems as stipulated by the Universal Guidelines for Artificial Intelligence.[35]

Using AI systems to make decisions about public benefits, health care, employment, or housing—whether or not those decisions are fully automated—can threaten fundamental rights, harm human dignity, and disproportionately affect historically marginalized groups.[36] These risks are exacerbated when individuals have no knowledge of the AI systems they encounter or their associated risks. In 2008, a Federal Trade Commission ("FTC") suit against a credit card company alleged that the company was using an undisclosed behavioral scoring algorithm to

---

[29] *Id.* at Title III, Article 14.
[30] *Id.* at Title IV, Article 52(1-4).
[31] *Id.* at Title IV, Article 52(1).
[32] *Id.* at Title IV, Article 52(1-3).
[33] *Id.* at Preamble, para 37.
[34] *Id.* at Preamble, paras 26-27.
[35] *See Universal Guidelines for Artificial Intelligence*, The Public Voice (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines/.
[36] *See e.g.* Danielle K. Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 5 (2014), https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2.

reduce consumer access to credit following transactions related to marriage counseling, therapy, and massages.[37] Individuals using the credit service had no prior knowledge that their conduct would be entered into an AI system, much less that such conduct would be used to determine their credit limits.[38] Similarly, LexisNexis' cache of over 45 billion records, including criminal records, bankruptcy information, cell phone numbers, and property history, is now being used to predict patients' health risks and costs.[39] These predictions may influence clinician decisions regarding medication prescriptions and have been shared with an actuarial firm that is testing how the scores could be used to price insurance plan premiums, all without the knowledge of the individuals affected.[40] Failing to inform individuals of AI system use meaningfully deprives them of actionable knowledge, the opportunity to protect their information from this use, and can have a detrimental effect on access to basic necessities, enacting real-world harm.

Limiting notice requirements solely to AI systems that interact with individuals, are used for biometric identification, or facilitate deep fakes may also deny equal access to services based on opaque and arbitrary analysis and allow inappropriate, skewed, or biased applications of technologies. In 2019, a study on a health care screening algorithm found that the algorithm routinely classified Black patients as ineligible for a specialized care management program.[41] According to the researchers, because less money was spent on Black patients who had the same level of need as equally sick White patients, the algorithm inaccurately concluded that the Black patients were healthier and did not need extra care.[42] While the algorithm did not use biometric information and instead relied on health care cost data in its analysis, that reliance on costs ultimately proved to be an unrecognized mechanism of bias. Though the algorithmic predictions were well-calibrated across races, that only served to obfuscate rather than mitigate bias and, in this case, enshrined an existing bias into ongoing care decisions.[43] A notice that an algorithm may be used to determine whether additional care is required would have been insufficient and would likely not have prompted the kind of examination that would reveal the inherent bias. As this case demonstrates, an effective notice requirement must not only ensure that individuals are informed that an AI system is in use, but also provide sufficient detail of how that system will

---

[37] Complaint for Permanent Injunction and Other Equitable Relief at 34-35, F.T.C. v. CompuCredit Corp., No. 1:08–CV–1976–BBM–RGV (N.D. Ga. Oct. 8, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/06/080610compucreditcmptsigned.pdf.
[38] *Id.*
[39] LexisNexis Risk Solutions, *LexisNexis Socioeconomic Data Coverage* (2016), https://www.lexisnexis.com/risk/downloads/literature/health-care/socioeconomic-data-coverages-br.pdf; Press Release, LexisNexis Risk Solutions, Milliman MedInsight to Use LexisNexis Risk Solutions Socioeconomic Health Attributes to Help Enhance Healthcare Intelligence (Oct. 24, 2017), https://www.prnewswire.com/news-releases/milliman-medinsight-to-use-lexisnexis-risk-solutions-socioeconomic-health-attributes-to-help-enhance-healthcare-intelligence-300541930.html.
[40] *See* Marshall Allen, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates*, ProPublica (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.
[41] Ziad Obermeyer et al., *Dissecting racial bias in an algorithm used to manage the health of populations*, Science (Oct. 25, 2019), https://science.sciencemag.org/content/366/6464/447.
[42] *Id.*
[43] *Id.*

function, its decision-making criteria, and known and foreseeable risks associated with it. For these reasons, EPIC recommends that Article 9(4) be adjusted to communicate residual risks of AI systems not only to the user, but also the data subject.

Though some have proposed that human intervention or final human decision-making would be sufficient to counteract biases or detrimental effects of AI-based recommendation systems, research demonstrates that human intervention fails to address major concerns about transparency or control; individual reviewers are often unable to evaluate quality and fairness of outputs or may have their own biases.[44] In addition, use of human "oversight" as a rubber stamp sign-off on AI system decision-making may remove protections for individuals, such as the GDPR requirement that individuals have the right not to be subject to decisions based solely on automated processing (the human oversight in this case making the decision no longer based "solely" on automated processing even if the bulk of the decision rests on automated processing).[45] Finally, human oversight blurs the lines of who is responsible for AI harms—the human operators or the systems they are tasked with understanding and controlling.[46] While it may be tempting to believe that a human oversight element can meaningfully address the inherent problems with AI system decision-making, the research does not bear this out.

The proposed regulations' limited ban on law enforcement use of real-time biometric identification systems in publicly accessible spaces also presents a serious risk that many individuals will be subject to AI surveillance systems without prior notice. Because the current proposal contains numerous exceptions to a general prohibition on law enforcement use of AI systems for "real-time" biometric recognition (as discussed above), it leaves EU authorities with a broad ability to deploy AI surveillance.[47] The potential reach of law enforcement use of "real-time remote biometric identification" is further extended by the proposed regulation's broad definition of "publicly accessible space," which includes any physical space "accessible to the public" regardless of whether certain conditions for access, such as purchasing an admission ticket, apply.[48] This definition would allow roads, sidewalks, and public buildings to be monitored by intrusive surveillance systems. Individuals in transportation hubs, cultural centers, and sports arenas could also be impacted. While the Commission recognized that the use of AI systems for "real-time remote biometric identification" could "evoke a feeling of constant surveillance" and chill "the freedom of assembly and other fundamental rights," the broad

[44] *See* Ben Green and Amba Kak, *"The False Comfort of Human Oversight as an Antidote to A.I. Harm,"* Slate (June 15, 2021), https://slate.com/technology/2021/06/human-oversight-artificial-intelligence-laws.html; Rebecca Crootof, *A Meaningful Floor for "Meaningful Human Control,"* Temple Int'l & Comp. L.J. (2017), 53-62;
[45] General Data Protection Regulation, Article 22.
[46] *See* Green and Kak, *supra* note 44; Crootof, *supra* note 44; Madeleine Clare Elish, *Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction,* Engaging Science, Technology, and Society 5 (2019), 40-60.
[47] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain*, at Title II, Article 5, COM (2021) 206 final (Apr. 21, 2021).
[48] *Id.* at Title II, Article 3.

definition of publicly accessible space and sweeping exceptions for law enforcement use of biometric-based surveillance systems do little to prevent those substantial risks.[49]

In addition to providing notice of the AI system use to affected individuals, there should also be a meaningful option to opt-out of these systems. Merely informing individuals of AI system use without providing them a clear opportunity to opt-out could allow pernicious AI systems to operate behind a facade of consent. As has been the case with cookie consent under the GDPR, when notices are misleading or choices difficult to implement, the fact that use of a system has merely been disclosed does not establish consent as a legal basis for processing.[50] Researchers have highlighted the difficulty of opting out from biometric recognition systems and EPIC recommends that the Commission take these challenges into consideration when mandating an ability to opt out for AI systems. In particular, the Commission should consider mandating that the AI systems be structured as opt-in to more meaningfully protect privacy and inform individuals.[51] This recommendation, along with the recommendation to inform data subjects of all AI system use and mandate notification prior to AI system use, corresponds with the AI Ethics Guidelines finalized by the European Commission's High-Level Expert Group on Artificial Intelligence in 2019.[52] Fully informing individuals about AI systems is a critical step toward effective regulation, meaningful transparency, and actionable accountability.

EPIC recommends that emotion recognition systems and biometric categorization systems be fully banned

While nominal limitations on use of AI systems related to emotion recognition and biometric categorization are present in the AIA draft, use of these systems is still permitted in certain contexts. EPIC recommends that the Commission fully ban emotion recognition and biometric categorization systems, as the proposed notice requirements cannot mitigate the severe problems of inaccuracy and bias that are inherent within these technologies.

---

[49] *See id.* at Preamble, para 18; *see also* Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology*, 49 Conn. L. Rev. 1591, 1615-20 (2017), https://opencommons.uconn.edu/law_review/377 (Discussing how expanded surveillance networks equipped with facial recognition systems can increase the number of people subjected to law enforcement stops and infringe on fundamental rights of free speech, informational privacy, and protest); Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. Times (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html?module=inline.

[50] *See* noyb, *noyb Aims to End "Cookie Banner Terror" and Issues More Than 500 GDPR Complaints*, noyb (May 31, 2021), https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints; Natasha Lomas, *Europe's Top Court Says Active Consent is Needed for Tracking Cookies*, TechCrunch (Oct. 1, 2019), https://techcrunch.com/2019/10/01/europes-top-court-says-active-consent-is-needed-for-tracking-cookies/.

[51] *See e.g.,* Wojciech Wiewiórowski, *Facial recognition: A solution in search of a problem?*, European Data Protection Supervisor (Oct. 28, 2019), https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.

[52] *High-Level Expert Group on Artificial Intelligence Ethics Guidelines for Trustworthy AI*, at 34 (Apr. 8, 2019), https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Despite persistent reports of mass inaccuracy and intrinsic bias, in both real-world and theoretical applications, use of emotion recognition and biometric categorization systems has exploded across multiple sectors, many of them extremely high-impact for data subjects. For example, companies may employ emotion recognition systems to generate "employability" scores for job applicants, analyze the purported impact of advertisements and the emotional status of customers, and attempt to detect shoplifters.[53] Some firms have also suggested that these programs be used by law enforcement, claiming that the AI systems may detect signs of deception, anger, stress, and anxiety in detained individuals.[54] These systems all rely on algorithms based on early research that proposed the existence of universal emotions and a strong correlation between emotion and facial expression.[55] However, a 2019 meta-analysis of the relevant scientific literature revealed that there is actually no reliable evidence that an individual's emotional state can be inferred from their facial movements.[56] Emotion recognition technology is unable to "confidently infer happiness from a smile, anger from a scowl, or sadness from a frown" because it glosses over cultural and social contexts.[57]

Algorithms often fail to capture the complexity of human emotion when used in the real world.[58] For instance, data shows that people only scowl approximately 30% of the time when they're angry—therefore, if an algorithm views a scowl as a necessary component of anger, it will be wrong about the subject's emotional state about 70% of the time.[59] Similarly, since women are often socialized to smile in the workplace in order to avoid negative repercussions and appear more pleasant, a smile is not a reliable indicator of actual happiness or agreement.[60] In addition, emotion recognition systems do not consider other factors such as an individual's body movement, personality, and tone of voice in their perception of emotion, and cannot even distinguish between an intentional wink or an involuntary blink.[61] Many software companies

---

[53] James Vincent, *Discover the Stupidity of AI Emotion Recognition with This Little Browser Game*, The Verge (Apr. 6, 2021), https://www.theverge.com/2021/4/6/22369698/ai-emotion-recognition-unscientific-emojify-web-browser-game; *see also* 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/.

[54] Charlotte Gifford, *The Problem with Emotion-Detection Technology*, The New Economy (June 15, 2020), https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology.

[55] *Id.*; Crawford, *supra* note 53.

[56] Lisa Feldman Barret et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 Ass'n for Psych. Sci., 1, 46 (2019), available at https://journals.sagepub.com/doi/pdf/10.1177/1529100619832930.

[57] *Id.*; *see also* Krys, Kuba et al., *Be Careful Where You Smile: Culture Shapes Judgments of Intelligence and Honesty of Smiling Individuals*, Journal of Nonverbal Behavior Vol. 40, 101-116 (2016), available at https://doi:10.1007/s10919-015-0226-4; Gifford, *supra* note 54.

[58] *See* Abeba Birhane, *The Impossibility of Automating Ambiguity,* Art. Life Vol. 27(1), 44-61.

[59] James Vincent, *AI "Emotion Recognition" Can't Be Trusted*, The Verge (July 25, 2019), https://www.theverge.com/2019/7/25/8929793/emotion-recognition-analysis-ai-machine-learning-facial-expression-review.

[60] Cheryl Teh, "*Every Smile You Fake" – an AI Emotion-Recognition System Can Assess How "Happy" China's Workers are in the Office*, Insider (June 25, 2021), https://www.insider.com/ai-emotion-recognition-system-tracks-how-happy-chinas-workers-are-2021-6.

[61] Douglas Heaven, *Why Faces Don't Always Tell the Truth About Feelings*, Nature (Feb. 26, 2020), https://www.nature.com/articles/d41586-020-00507-5; Vincent, *supra* note 59.

claim high rates of accuracy but refuse to produce evidence corroborating that these automated techniques actually work, while other research has demonstrated how easy it is to "trick" these algorithms into perceiving certain emotions that don't reflect how an individual is truly feeling.[62] Ultimately, emotion recognition programs threaten individual privacy, freedom of thought, and additional fundamental rights by constantly surveilling a person's demeanor and forcing people to act according to an algorithm's frequently culturally and individually-biased idea of "mainstream" behavior in order to avoid getting flagged and potentially facing real-world consequences or losing real-world opportunities.[63]

Emotion detection technology also threatens to reinforce harmful racial stereotypes. These algorithms often have racial bias built in—for example, by assigning the faces of Black men more negative and threatening emotions than White men regardless of how much the Black men smiled.[64] One software system, Face++, rates Black faces twice as angry as their White counterparts, and Microsoft's Face API scores Black faces three times more "contemptuous" than White faces.[65] Using biased software will lead to disastrous consequences: not only could people of color be prematurely eliminated from company hiring pools, but individuals flagged as "threats" by government agencies are also more likely to be followed, detained, placed on a no-fly list, or even face criminal sanctions.[66]

Biometric categorization systems, which attempt to link an individual's biometric data to certain traits and proclivities, are similarly based on false assumptions and threaten dangerous repercussions. Far from an objective method of analysis, biometric categorization harkens back to the dark days of phrenology and physiognomy, when researchers attempted to draw character inferences based on an individual's skull measurements and facial features.[67] These pseudoscientific techniques have historically been used to fuel nationalism, white supremacy, and xenophobia, and the spurious science behind new biometric technologies threatens to entrench these same insidious power structures.[68] At least one company currently offers automated services that it claims can predict how likely someone is to be a terrorist or pedophile based only on facial features, and other researchers have advertised algorithms that can predict autism, detect a person's sexuality, or predict a person's likelihood of engaging in criminal behavior just from analyzing their face.[69]

---

[62] Heaven, *supra* note 61; Vincent, *supra* note 59.
[63] Teh, *supra* note 60.
[64] 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.
[65] *Id.*
[66] *See* Lauren Rhue, *Racial Influence on Automated Perceptions of Emotions*, SSRN, 1, 1 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.
[67] Blaise Aguera y Arcas et al., *Physiognomy's New Clothes*, Medium (May 6, 2017), https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a; Crawford, *supra* note 53.
[68] Aguera y Arcas et al., *supra* note 67.
[69] *See* Sally Adee, *Controversial Software Claims to Tell Your Personality From Your Face*, New Scientist (May 27, 2016), https://www.newscientist.com/article/2090656-controversial-software-claims-to-tell-personality-from-your-face/; *Researchers are Using Machine Learning to Screen for Autism in Children*, Duke

However, since predictive algorithms rely heavily on historical data, they tend to reproduce traditions and practices of the past that have been unjust to marginalized individuals. For instance, algorithms that purport to predict the likelihood of a person's criminality are trained using data from racist criminal justice systems that punish people of color at disproportionate rates, which results in a similarly racist algorithm.[70] Similarly, attempting to use biometric data to determine an individual's sexuality is not only methodologically flawed, but may also be used to discriminate against people believed to be gay.[71] Biometric technologies also frequently depend on categorizations inherently harmful to trans and non-binary individuals, since scientists inevitably use their own perceptions of gender to train their algorithms to recognize various traits, which means that these systems are infused with dominant norms and stereotypes.[72] Ultimately, biometric categorization systems tend to subject anyone whose appearance deviates from imposed norms to heightened scrutiny, resulting in larger burdens on people of color, gender minorities, and people with disabilities.[73] Finally, no conclusive evidence that physical appearance is clearly tied to character traits in such a way that biometric categorization would ever be successful.

Given the current state of these system types and lack of any clear path to resolving these systemic issues, a total ban on emotion recognition and biometric categorization systems is the only adequate solution to the myriad of harms these technologies present to individuals. Article 52(2) of the AIA draft currently mandates that subjects exposed to these systems must be informed of the operation, with the exception of automated systems of biometric categorization used by law enforcement. However, mere notice of use—particularly with such a broad caveat—

Pratt School of Engineering (July 11, 2019), https://pratt.duke.edu/about/news/amazon-autism-app-video; Paul Lewis, *"I was Shocked it was so Easy": Meet the Professor Who Says Facial Recognition Can Tell if You're Gay*, The Guardian (July 7, 2018), https://www.theguardian.com/technology/2018/jul/07/artificial-intelligence-can-tell-your-sexuality-politics-surveillance-paul-lewis; Madhi Hashemi & Margaret Hall, *Criminal Tendency Detection from Facial Images and the Gender Bias Effect*, 7 J. Big Data, 1, 1 (2020), https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0282-4#Sec9 (since retracted); Luana Pascu, *Biometric Software that Allegedly Predicts Criminals Based on Their Face Sparks Industry Controversy*, Biometric Update (May 6, 2020), https://www.biometricupdate.com/202005/biometric-software-that-allegedly-predicts-criminals-based-on-their-face-sparks-industry-controversy.

[70] *See* Pascu, *supra* note 69; Luana Pascu, *Scientists, Sociologists Speak Out Against Biometrics Research that Allegedly Predicts Criminals*, Biometric Update (June 23, 2020), https://www.biometricupdate.com/202006/scientists-sociologists-speak-out-against-biometrics-research-that-allegedly-predicts-criminals; *Facial Recognition to "Predict Bias" Sparks Row Over AI Bias*, BBC News (June 24, 2020), https://www.bbc.com/news/technology-53165286; *see also* Birhane, *supra* note 58 at 46 (Noting that predictive algorithms rely on historical data that reproduces harmful trends for marginalized individuals).

[71] Vincent, *supra* note 23; Sam Levin, *LGBT Groups Denounce "Dangerous" AI that Uses Your Face to Guess Your Sexuality*, The Guardian (Sept. 8, 2017), https://www.theguardian.com/world/2017/sep/08/ai-gay-gaydar-algorithm-facial-recognition-criticism-stanford.

[72] *See* Rosa Wevers, *Unmasking Biometrics' Biases: Facing Gender, Race, Class and Ability in Biometric Data Collection*, 21 TMG J. Media Hist., 89, 92 (2018), https://www.tmgonline.nl/articles/10.18146/2213-7653.2018.368/; Os Keyes, *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition*, 2 Proc. ACM on Human-Computer Interaction, 1, 12 (2018), available at https://ironholds.org/resources/papers/agr_paper.pdf.

[73] *See* Wevers, *supra* note 72.

is a disproportionately lenient response to the societal wrongs these systems perpetuate, as notice does nothing to ease the inaccuracies and biases these mass surveillance technologies propagate, nor is it accompanied by a clear and simple method for individuals to refuse to be included in the operations. Indeed, permitting use of these systems in any context appears to validate them. Research suggests that AI programs will never be able to classify human behavior accurately and consistently because human behavior is inherently open-ended, fluid, and ambiguous, with makes our behavioral pathways too complex and unpredictable for an automated system to grasp.[74] Therefore, it is not possible to simply reform these technologies to be less biased or more accurate, and they must be banned in order to fully protect the privacy and freedom of individuals.

EPIC recommends that all conformity assessments be reviewed and approved by data protection authorities prior to the relevant AI systems being used in the market

Currently, the AIA requires that all high-risk AI systems listed in Annex III undergo conformity assessments to ensure compliance with the AIA.[75] Not all of these conformity assessments, however, must be reviewed by a third-party auditor. Indeed, with a few exceptions—for example, if the high-risk AI system involves remote biometric identification[76] or is already regulated under existing product safety law[77]—conformity assessments are purely internal processes: the provider completes an internal assessment procedure[78] and self-reports compliance by affixing a "CE marking of conformity" to the high-risk AI system.[79]

EPIC recommends that the Commission mandate that all conformity assessments be reviewable by trained and qualified enforcement authorities, as well as available to the public, rather than remaining purely internal. These enforcement authorities could be the same notified bodies already appointed to oversee conformity assessments for certain high-risk AI systems, provided that those bodies are public entities endowed with enforcement powers.[80] Without third-party oversight, there is no guarantee that these conformity assessments will accurately or comprehensively reflect the robustness or shortcomings of the development, design, and deployment of high-risk AI systems. Because of the sensitive nature of these high-risk AI systems—and their potential to inflict widespread harm if not managed appropriately—independent review is a crucial mechanism for oversight and quality assurance. While we

---

[74] Birhane, *supra* note 58.
[75] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at Title III, Article 43, COM (2021) 206 final (Apr. 21, 2021).
[76] *Id.* at Explanatory Memorandum, 5.2.3.
[77] *Id.* at Explanatory Memorandum, 1.2.
[78] *Annexes to the Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,* at Annex IV, COM (2021) 206 final (Apr. 21, 2021).
[79] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at Title III, Article 49, COM (2021) 206 final (Apr. 21, 2021).
[80] *Id.* at Title II, Article 33.

recognize that this imposes an additional obligation for AI system developers, solely internal assessments could quickly devolve into meaningless box-checks.

Making conformity assessments available to the public would also increase the transparency and public accountability of high-risk AI systems. Currently, public notice under the AIA is achieved primarily through a requirement that providers enter "meaningful information about their systems and the conformity assessment" into a broader EU database.[81] There is little guidance, however, on what "meaningful information" includes. EPIC recommends that this EU database include the conformity assessments submitted for all high-risk AI systems, with possible exceptions or redactions for trade secrets and otherwise sensitive information.

The importance of independent review and public transparency is rooted in the existing scholarship on impact assessments. A report released this year on algorithmic impact assessments emphasized that these assessments, which mirror conformity assessments in form and intent, "cannot achieve genuine accountability" unless they are reviewed by an external forum able to mandate changes to an AI system.[82] The same report held that "the broader the public access to an IA's [impact assessment's] processes and documentation, the stronger its potential to enact accountability."[83]

EPIC also recommends that the Commission develop clearer guidelines for determining when high-risk AI systems should undergo re-assessment, both for compliance certifications issued by third parties and for any CE markings of conformity. For high-risk AI systems that are subject to third-party auditing by notification bodies, compliance certifications are valid for no more than five years. Any change to the AI system that could affect compliance, moreover, must be reported to the notified body, which would then decide whether a new conformity assessment is required.[84] Otherwise, the AIA states simply that high-risk AI systems subject only to internal conformity assessments must undergo a new conformity assessment "whenever they are substantially modified."[85] EPIC recommends that the Commission clarify this language and hold that any changes in the AI system or its use should entail immediate re-assessment. This would ensure compliance with the AIA's regulations at all stages of a high-risk AI system's development and evolution.

---

[81] *Id.* at Explanatory Memorandum, 5.1.
[82] Moss et al., *Assembling Accountability: Algorithmic Impact for the Public Interest*, Data & Society 9 (2021).
[83] *Id.* at 15; also *see*, e.g., Roger Clarke, *An evaluation of privacy impact assessment guidance documents*, 1 Int'l Data Priv. L. 111, 115-116 (2011); David Wright et al., *A Comparative Analysis of Privacy Impact Assessment in Six Countries*, 9 J. Contemp. Eur. Rsch. 161, 164 (2013).
[84] *Annexes to the Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,* at Annex VII 4.7, COM (2021) 206 final (Apr. 21, 2021).
[85] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at Title III, Article 43.4, COM (2021) 206 final (Apr. 21, 2021).

Conclusion

The European Commission should incorporate the recommendations listed above into the AIA in order to protect the fundamental rights of individuals against the risks posed by AI systems. Addressing the myriad exemptions and loopholes, mandating notification of AI system use to individuals, banning emotional recognition and biometric categorization systems, and requiring review and approval of conformity assessments will strengthen protections for individuals, enact meaningful enforcement of compliance requirements, and counter potential misuse of and discrimination through AI system use.

Respectfully Submitted,

Calli Schroeder
Calli Schroeder
EPIC Global Privacy Counsel

Ben Winters
Ben Winters
EPIC Equal Justice Works Fellow

Alexa Daugherty
Alexa Daugherty
EPIC IPIOP Clerk

Hannah Hunt
Hannah Hunt
EPIC IPIOP Clerk

Peggy Xu
Peggy Xu
EPIC IPIOP Clerk