epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

UNITED KINGDOM BIOMETRICS AND SURVEILLANCE CAMERA COMMISSIONER

Regarding the

DRAFT UPDATED SURVEILLANCE CAMERA CODE OF PRACTICE

September 8, 2021

By notices published August 13, 2021, the United Kingdom government has opened a consultation regarding proposed revisions to the Surveillance Camera Code of Practice (the "Code"),[1] to close on September 8, 2021.[2] This will be the first update to the Code since it was introduced in June 2013. Current updates largely stem from updates in applicable legislation and court judgments and general streamlining.[3] This consultation will be overseen by Professor Fraser Sampson, the Biometrics and Surveillance Camera Commissioner (the "Commissioner").[4] Pursuant to the request for contributions from a wide range of stakeholders, the Electronic Privacy Information Center ("EPIC") submits the following comments.

---

[1] Draft Updated Surveillance Camera Code of Practice, Protection of Freedoms Act 2012, Section 30 (2021), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1010815/Surveillance_Camera_Code_of_Practice__update_.pdf (hereinafter "Draft Updated Surveillance Camera Code of Practice (2021)").

[2] *Open Consultation: Surveillance Camera Code of Practice,* Surveillance Camera Commissioner (August 13, 2021), available at https://www.gov.uk/government/consultations/surveillance-camera-code-of-practice.

[3] *Open Consultation: Grid of Amendments,* Surveillance Camera Commissioner (updated August 25, 2021), available at https://www.gov.uk/government/consultations/surveillance-camera-code-of-practice/grid-of-amendments.

[4] *Open Consultation: Surveillance Camera Code of Practice,* Surveillance Camera Commissioner (August 13, 2021), available at https://www.gov.uk/government/consultations/surveillance-camera-code-of-practice.

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.[5] EPIC has a long history of promoting transparency and accountability for use of systems used to surveil the public, at both a national and an international level.[6] EPIC has filed multiple Freedom of Information Act ("FOIA") requests regarding general surveillance use and surveillance of protestors specifically,[7] in addition to filing amicus curiae briefs to contribute to legislation.[8]

EPIC concurs that the Code is due for an update, particularly taking into consideration recent cases such as Bridges v. South Wales Police, updates in applicable regulations, and shifting public perceptions regarding surveillance. However, some of the proposed changes fail to address substantial critiques of certain surveillance technology systems and their uses and do not specify standards or requirements for accountability. In addition, further changes could be

---

[5] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html.
[6] *See* e.g. Comments of EPIC, *POST Act Disclosures,* New York Police Department (February 25, 2021), https://www.epic.org/apa/comments/EPIC-Comments-NYPD-POST-Act.pdf; Comments of EPIC, *Docket No. DHS-2007-0076 Notice of Privacy Workshop and Request for Comments,* Department of Homeland Security (Jan. 15, 2008), https://www.epic.org/privacy/surveillance/epic_cctv_011508.pdf; Spotlight on Surveillance, *More Cities Deploy Camera Surveillance Systems with Federal Grant Money,* EPIC (May 2005), https://epic.org/privacy/surveillance/spotlight/0505/; Constitution Project (EPIC, ACLU-NCA), *Letter to the D.C. Council Urging Full Examination of Proposed Surveillance System,* D.C. Council (May 9, 2008), https://www.epic.org/privacy/surveillance/dccouncil_050908.pdf; Letter of EPIC and coalition members, *Letter to Congress re: Funding of Surveillance Technology Aimed at Peaceful Protestors,* United States Congress (June 17, 2020), https://mediajustice.org/wp-content/uploads/2020/06/coalition_letter_defund_police_surveillance.pdf.
[7] EPIC FOIA Request, *FOIA Request Relating to the FBI's Engagement in Electronic Surveillance in Connection with Civil Protests Related to George Floyd's Death,* Department of Justice's Federal Bureau of Investigation (June 10, 2020), https://epic.org/foia/fbi/blm-protest-surveillance/EPIC-20-06-10-FBI-FOIA-20200610-Request.pdf; EPIC FOIA Request, *FOIA Request Relating to the DEA's Engagement in Electronic Surveillance in Connection with Civil Protests Related to George Floyd's Death,* Department of Justice's Drug Enforcement Administration (June 10, 2020), https://epic.org/foia/dea/blm-protest-surveillance/EPIC-20-06-10-DEA-FOIA-20200610-Request.pdf; EPIC FOIA Request, *FOIA Request Relating to the CBP's Engagement in Electronic Surveillance in Connection with Civil Protests Related to George Floyd's Death,* U.S. Customs and Border Protection (June 12, 2020), https://epic.org/foia/cbp/blm-protest-surveillance/EPIC-20-06-12-CBP-FOIA-20200612-Request.pdf.
[8] *See* e.g. Amicus Curiae Brief by EPIC in Nelson v. Salem State College, et al., *Brief of Amicus Curiae Electronic Privacy Information Center, In Support of Plaintiff-Appellant,* Supreme Judicial Court for the Commonwealth of Massachusetts (November 3, 2005), available at https://epic.org/privacy/nelson/epic_nelson_amicus.pdf (In this case, the plaintiff sued over a reasonable expectation of privacy when a hidden camera recorded her changing in a cubicle at work).

made in order to more clearly and fully encourage public trust and confidence and align the Code with public expectations and standards that uphold individual privacy and human rights. While EPIC disagrees with some assumptions contained in the updated draft,[9] we have limited our recommendations below to key textual changes. Some of the recommendations relate to newly-adapted text and some are proposals for additional changes to the Code:

- Clarify assessment criteria and necessary standards to ensure fitness of underlying data and databases used for ANPR and facial recognition (Principle 12.1)
- Formalize the consultation requirements contained within the Code (Principles 1.3, 2.5, 3.2, 3.3, and 4.1)
- Strengthen protections against improper use of facial recognition and biometric recognition systems (Principle 2.4)
- Promote public release of applicable policies to increase transparency (Principle 5.1)

[9] For example, Introduction and Overview, Section 5, of the Code states that "[i]t is the way in which technology is used that is potentially intrusive rather than the technology itself…" While technology certainly exists that can be used in both benign and harmful ways, many technologies are, by nature or design, intrusive. Spyware, autonomous weapons, keystroke logging, ankle monitors, behavioral advertising, parole apps, IMSI catchers, surveillance technology, and more have been identified by privacy experts (and sometimes their own creators) as being intentionally intrusive. Indeed, intrusion is the only way to gather the data that these technologies were designed to collect. The distinction is that users of this technology have determined that the intrusion is justified, warranted, or acceptable in the circumstances. *See* e.g. Todd Feathers, *"They Track Every Move": How US Parole Apps Created Digital Prisoners,* The Guardian (March 4, 2021), https://www.theguardian.com/global-development/2021/mar/04/they-track-every-move-how-us-parole-apps-created-digital-prisoners; *IMSI Catchers Legal Analysis Report,* Privacy International (June 2020), available at https://privacyinternational.org/sites/default/files/2020-06/IMSI%20catchers%20legal%20analysis.pdf; Nathan Gardels, Eric Schmidt, and Jared Cohen, *Google's Eric Schmidt: Internet will Let Chinese Rise Up,* Christian Science Monitor (May 8, 2013), https://www.csmonitor.com/Commentary/Global-Viewpoint/2013/0508/Google-s-Eric-Schmidt-Internet-will-let-Chinese-rise-up (Key Quote: "The communication technologies we use today are invasive by design, collecting our photos, comments and friends into giant databases that are searchable and, in the absence of regulation…[it is all] fair game."); *What is Spyware?,* BBC (October 10, 2012), http://www.bbc.co.uk/webwise/guides/about-spyware; Dan Swinhoe, *What is a Keylogger? How Attackers Can Monitor Everything You Type,* CSO (December 11, 2018), https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html; Natasha Lomas, *The Case Against Behavioral Advertising is Stacking Up,* TechCrunch (January 20, 2019), https://techcrunch.com/2019/01/20/dont-be-creepy/.

1. *EPIC recommends that the Commissioner ban facial recognition technology or, in the absence of a ban, set forth clear assessment criteria and baseline standards to ensure that reference databases used for matching purposes are fit for those purposes*

Certain surveillance camera systems, such as facial recognition systems or Automatic Number Plate Recognition ("ANPR") systems, use matching technology to produce results, directly comparing information collected from the surveillance cameras to information in reference databases (for ease of reference, these will be referred to as "matching technologies" throughout this section). There are two major concerns with these system types: (i) whether the invasive nature of facial recognition—particularly live facial recognition—systems is ever justified, and (ii) whether the databases used for matching purposes are fit for those purposes.

First, facial recognition technology is subject to a wide range of accuracy errors, several of which perpetuate existing bias. Multiple reports have demonstrated exponentially increased rates of misidentification for people of color or transgender and non-binary individuals.[10] A federal study in the United States concluded that "Asian and African American people were up to 100 times more likely to be misidentified than white men."[11] Indeed, independent analysis commissioned by the Metropolitan Police found that matches made using the Metropolitan

---

[10] *See e.g.* Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Proceedings of Machine Learning Research 81 (2018), 1-15; Morgan Klaus Scheuerman, Jacob M. Paul, and Jed R. Brubaker, *How Computers See Gender: an Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services,* Proc. ACM Hum. Comput. Interact., Vol 3, No. CSC@, Article 144 (November 2019), available at https://docs.wixstatic.com/ugd/eb2cd9_963fbde2284f4a72b33ea2ad295fa6d3.pdf; Nicholas Furl, P. Jonathon Phillips, and Alice J O'Toole, *Face recognition algorithms and the other-race effect: computational mechanisms for a developmental contact hypothesis,* Cognitive Science Vol. 26, Issue 6 (Nov-Dec 2002), 797-815; Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* NIST, NISTIR 8280 (December 2019), available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[11] Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use,* The Washington Post (December 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/, citing Patrick Grother, Mei Ngan, and Kayee Hanaoka, *supra* note 10.

Police's facial recognition systems were inaccurate 81 percent of the time.[12] Even the most optimistic view of the technology concedes that high degrees of accuracy are only possible "in ideal conditions where there is consistency in lighting and positioning, and where the facial features of the subjects are clear and unobscured. In real world deployments, accuracy rates tend to be far lower."[13]

These bias and inaccuracy problems are exacerbated by additional concerns present in the use of live facial recognition technology. According to the most comprehensive study of active live facial recognition technology—in use by London's Metropolitan Police—the technology itself raises serious concerns relating to its deployment, how and why individuals are added to watchlists, and whether it is disproportionate to the purpose of the technology.[14] Of particular concern is the observation that police respond harshly to alerts from live facial recognition systems, even where the alert is clearly inaccurate. One particularly egregious case of misidentification involved a 14-year-old boy who was stopped, surrounded, pulled into a side street, and searched by plainclothes officers.[15] Further, the report deems it "highly possible" that the use of live facial recognition will be found unlawful by courts and "inadequate" under human rights law.[16]

Such damning review of these systems hardly inspires public trust and confidence. The text in the Code does little to alleviate concerns, mandating that chief police offers should

---

[12] Matt Burgess, *The Met Police will start using live facial recognition across London,* Wired (January 24, 2020), https://www.wired.co.uk/article/london-met-police-facial-recognition.
[13] William Crumpler, *How Accurate are Facial Recognition Systems – and Why Does It Matter?,* Center for Strategic & International Studies (April 14, 2020), https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter.
[14] Prof. Pete Fussey and Dr. Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology,* Human Rights Centre, University of Essex (July 2019), available at https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.
[15] *Id.* at 124.
[16] *Id.* at 53-54.

publish the categories of people to be included on a watchlist and the criteria used to determine where and when to deploy live facial recognition systems.[17] This language is overly broad, imposes no meaningful protections, and addresses few of the identified problems within these systems of disproportionality, misidentification, or transparency of use. A police officer could, in theory, state that the categories of people to be included on a watchlist are "suspected of criminal activity," "covering their features," or, as in the report, "violent."[18] These descriptors can easily apply to broad groups of people, do little to narrow the scope of invasive surveillance, and fail to explain or justify the process whereby a person is deemed sufficiently high-risk to warrant use of matching technologies. In light of these risks, EPIC recommends the Commissioner ban use of both standard and live facial recognition technology.

Should matching technologies still be used within surveillance camera systems, the second concern with matching technology is the integrity, quality, source, and fitness of the databases used for matching with data collected from surveillance camera systems. The Code mandates that matching technologies not be introduced without "regular assessment to ensure the underlying data is fit for purpose."[19] However, not only does the language fail to specify who should perform the assessment, what that assessment should consist of, or how to determine that underlying data is fit for purpose, it is also unclear from the language what exactly "should not be introduced" where regular assessment to determine fitness is not in place: the questionable database or the matching technology itself.[20] To determine how these assessments would take place, we must first provide some background relating to databases used for matching technology.

[17] Draft Updated Surveillance Camera Code of Practice (2021) at Principle 12.3.
[18] Fussey and Murray, *supra* note 14 at 81.
[19] Draft Updated Surveillance Camera Code of Practice (2021) at Principle 12.1.
[20] *Id.*

Databases used for matching purposes in facial recognition systems may be supplied by multiple sources which themselves compile their databases from multiple sources. Researchers worldwide have compiled multiple datasets of faces for testing use, originating from security camera images, voluntary submissions, social media, government and professional images, and more.[21] Private companies often will create their own databases using similar information sources.[22] Law enforcement bodies not only create their own databases for facial recognition technology matching purposes, but will often share these databases with other law enforcement bodies, creating a massive database network.[23] Several matching technologies take advantage of multiple available databases when running a matching comparison.

As mentioned above, matching accuracy is highly dependent on ideal conditions, both of the image obtained by the surveillance camera system and of the image type and quality within the database.[24] The quality of the database used for matching purposes is of the utmost importance to avoid chronic misidentification. Therefore, a true assessment must not only look to the source of the database to determine whether they are trustworthy and to evaluate their methods for acquiring images to add to the database (including legality and quality control), but also ensure that policies are in place such that the quality of images is consistent throughout any

[21] *See e.g. "Databases,"* Face Recognition Homepage (last visited September 7, 2021), https://www.face-rec.org/databases/.
[22] *See id.;* Stuart Sumner, *You for Sale: Protecting your Personal Data and Privacy Online,* Elsevier Inc. (2016); Dave Gershgorn, *Is there any way out of Clearview's facial recognition database?,* The Verge (June 9, 2021), https://www.theverge.com/22522486/clearview-ai-facial-recognition-avoid-escape-privacy; April Glaser, *Facebook's Face-ID Database Could be the Biggest in the World. Yes, It Should Worry Us,* Slate (July 9, 2019), https://slate.com/technology/2019/07/facebook-facial-recognition-ice-bad.html.
[23] *See e.g.* Jose Pagliery, *FBI launches a face recognition system,* CNN Business (September 16, 2014), https://money.cnn.com/2014/09/16/technology/security/fbi-facial-recognition/; Paul Szoldra, *NSA Intercepts Millions of Photos for Massive Facial Recognition Database,* Business Insider (May 31, 2014), https://www.businessinsider.com/nsa-facial-recognition-2014-5; Burgess, *supra* note 12.
[24] Crumpler, *supra* note 13.

additions to the database.[25] Assessments of the databases used must be ongoing, just as the expansion of these databases will be ongoing, to consistently ensure fitness.[26]

Due to the greatly increased risk of misidentification if a database is not high quality and, therefore, the importance of these regular fitness assessments, EPIC recommends that the Commissioner designate themselves or another suitable authority as a body that may review and audit these assessments as needed, require renewed assessment on at least a yearly basis and upon the use of any new database systems, and either (i) create and distribute a template assessment form for use, to ensure consistent criteria and quality of assessment, or (ii) provide updated text that clearly lists what must be considered in an assessment and what baseline standards must be met for continued use of matching technology.

2. EPIC urges the Commissioner to formalize the consultation requirements within the Code

EPIC recommends that the Commissioner formalize the process of consultation referred to throughout the Code. The consultation process should specify the length of time for consultation, the parties which must be involved, how to clearly announce the consultation and solicit input, and disclosure of results.

At various points, the Code recommends or requires consultation relating to (i) extension of surveillance camera system purposes or data collected;[27] (ii) conducting a data protection impact assessment ("DPIA");[28] and (iii) development or review of any surveillance camera system.[29] However, no text describes any specific requirements that these consultations must

[25] Noting that these image databases are subject to ongoing expansion and growth, as mentioned in "*Databases,*" *supra* note 21.
[26] *Id.*
[27] Draft Updated Surveillance Camera Code of Practice (2021) at Principle 1.3.
[28] *Id.* at Principle 2.5.
[29] *Id.* at Principle 3.2, Principle 4.1.

meet to satisfy the Code's guidance. Indeed, nothing within the Code even specifies that consultations must be documented, making claims that consultations were conducted unverifiable. The Code includes no specifics or recommendations regarding how an entity performing a consultation should announce or promote it,[30] determine the length of time that a consultation must be open for response,[31] decide what level of detail to provide to participants in a consultation,[32] ensure that appropriate parties participate,[33] receive feedback,[34] or make received feedback publicly viewable or available to the Commissioner.[35] The Commissioner should impose clear and consistent standards to ensure that consultations have a meaningful impact on the implementation of surveillance camera systems and ensure transparency and accountability.

EPIC recommends that the Commissioner either (i) make "consultation" a defined term within the Code, including within the definition reference to forms or examples of consultations and specific details of at least the minimum requirements related to consultation criteria, length of time, parties from whom to solicit feedback, submission details, announcement and promotion, and transparency of feedback received through the consultation; or (ii) draft a

[30] The nature of announcement and publication of a consultation will greatly affect whether the public and other interested parties are aware of its existence and, therefore, able to meaningfully participate in the consultation.
[31] Principle 3.3 mentions that consultations must be "undertaken at a stage when there is a realistic prospect of influencing developments." This provides detail relating to the point in the process of development or expansion at which a consultation should occur but does not explain how long the consultation should be open in order to allow interested parties and respondents adequate time to prepare and provide meaningful feedback.
[32] In order for responding parties to provide substantive responses to a consultation, consultation announcements must include sufficient detail regarding the surveillance camera system under review, its scope, what data it collects, how that data is used, who that data is shared with, and the nature of the development or expansion in question.
[33] Principle 3.2 recommends engagement with "the public and partners (including the police)" during a consultation. EPIC believes that, where law enforcement is specifically solicited for input in a consultation, privacy and human rights advocates (particularly those specializing in public surveillance) should be solicited as well.
[34] Clear contact points, such as a dedicated email address or a mailing address, should be included in the consultation and simple to locate and access for respondents.
[35] Public access to consultation feedback would aid in transparency and would promote public trust in that the public could directly see what, if any, impact consultation feedback may have on the final system. EPIC recognizes that certain systems may not allow for public review of the consultation for security or safety purposes—in those circumstance, EPIC recommends that consultation results still be made available to the Commissioner, either by default or on request.

template consultation form including all of these categories and publicize it for use to meet the consultation requirements within the Code.

3. EPIC recommends that the Commissioner strengthen protections against improper use of facial recognition and biometric characteristic recognition systems

While nominal limitations on use of facial recognition or other biometric characteristic recognition systems are present in the Code, use of these systems is still permitted, subject to requirements that the use be "clearly justified," "proportionate" to the stated purpose, "suitably validated," and subject to human intervention prior to decisions taken with possible adverse effects.[36] This section—and the Code as a whole—does not include any mention of additional system types that may be used, such as emotion recognition systems or biometric categorization systems. EPIC has already recommended in Section 1 that the Commissioner fully ban facial recognition systems. In the event that the Commissioner chooses not to do so, EPIC recommends that the Commissioner substantially strengthen the listed criteria for acceptable use of facial recognition and biometric characteristic recognition systems and explicitly ban use of emotion recognition and biometric categorization systems, as the severe inaccuracy and bias inherent in these systems cannot be meaningfully mitigated.

The current text of the Code related to use of facial recognition and biometric characteristic recognition systems is minimal and vague in its requirements. "Clearly justified" and "proportionate in meeting the stated purpose" are both subjective judgments, with no examples provided of what may be an example of a clearly justified use and no explanation of what the desire for use of these systems should be weighed against (rights of the data subject,

[36] Draft Updated Surveillance Camera Code of Practice (2021) at Principle 2.4.

data minimization requirements, other options for system type, risks and bias common to the system type, etc.) when making an assessment.[37] EPIC recognizes that these criteria may be intentionally open-ended to allow for flexibility in different circumstances and use contexts. However, EPIC recommends that the Commissioner provide examples of both justified use and proportionate use of these systems to provide clarity to system operators and to foster public trust that individual rights are given appropriate weight in this evaluation. We note that these examples should take into consideration the substantial racial and gender biases identified as frequently occurring within facial recognition systems, as previously detailed in Section 1.

The Code also states that use of these systems must be "suitably validated."[38] There is no clarification what body, position, or individual is qualified to issue this validation or, indeed, what form suitable validation would take in this process. EPIC recommends that the Code designate either a position within the Commissioner's office to review and validate these system uses or set forth criteria describing what constitutes a validation, who is qualified to issue said validation, and notice that validations may be reviewed or audited by the Commissioner at any time.[39]

The Code states that human intervention should always be involved "before decisions are taken that affect an individual adversely."[40] This language fails to provide sufficient safeguards in two ways. First, many decisions based on information from surveillance camera systems may have adverse effects that are unknown or unforeseen at the time the decision is made, making this ineffective as an absolute protection against adverse impact. Second, research demonstrates

[37] *Id.*
[38] *Id.*
[39] Additional options for a validating body or individual if the Commissioner's office cannot do so may include an organization's Chief Privacy Officer, Chief Security Officer, or a similar position. Validations of this type should be documented so that review and audit of validation is possible.
[40] Draft Updated Surveillance Camera Code of Practice (2021) at Principle 2.4.

that human oversight often fails to meaningfully address concerns stemming from technology systems because human reviewers may be unable to evaluate quality and fairness of outputs from these systems or to recognize their own biases.[41] Human oversight may actually make accountability for harm more difficult, blurring the line of responsibility between the human operators and overseers of a system and the systems themselves.[42]

Finally, the Code should specifically ban use of emotion recognition systems and biometric categorization systems. Despite multiple, sustained reports of large-scale inaccuracy and bias built into these systems, use of emotion recognition and biometric categorization systems has significantly expanded across multiple sectors.[43] These systems could in theory be implemented in public places, as defined within the Code. However, these systems operate from flawed premises and can cause significant harm to individuals.

Emotion recognition technology assumes the existence of universal emotional expression and a strong correlation between emotions and physical expression.[44] More recent analysis of this theory and the scientific literature purporting to demonstrate it reveals that no reliable evidence exists connecting an individual's emotional state from their physical actions.[45] Indeed, different cultural and social contexts may account for entirely unpredictable, inconsistent, and

---

[41] *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.

[42] *See* Green and Kak, *supra* note 41; Crootof, *supra* note 41; Madeleine Clare Elish, *Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction,* Engaging Science, Technology, and Society 5 (2019), 40-60.

[43] *See* 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/; 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.

[44] Gifford, *supra* note 43; Crawford, *supra* note 43.

[45] 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.

even directly oppositional emotional states expressed through the exact same physical expression.[46]

For example, women are often socialized to smile, even in tense or uncomfortable situations, in order to diffuse conflict, appear more pleasant and agreeable, and avoid negative repercussions.[47] An emotion recognition system would likely read that physical expression—incorrectly—as indicative of happiness. Emotion recognition systems have also been shown to hold significant racial bias.[48] Several systems have assigned more threatening emotions to Black faces than White faces, regardless of expression.[49] This does not begin to take into account individuals with physical expressions that are affected by physical or neurological differences whose facial expressions may vary from what a system considers "typical." Overall, emotion recognition systems provide little to no trustworthy information while posing a great risk to individual privacy, freedom of thought, and other fundamental rights by enforcing a culturally and individually-biased idea of standard emotional behavior on those it observes.

Similar false premises and threats exist in biometric categorization systems, which purport to link biometric data to specific traits, tendencies, or inclinations. This premise is virtually indistinguishable from phrenology and physiognomy—pseudoscientific and repeatedly debunked practices that inferred an individual's character from their physical appearance and which directly linked to nationalism, white supremacy, and xenophobia.[50] Companies offering

---

[46] *Id.; see also* Abeba Birhane, *The Impossibility of Automating Ambiguity,* Art. Life Vol. 27(1), 44-61.
[47] 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.
[48] 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.
[49] *Id., see also* Lauren Rhue, *Racial Influence on Automated Perceptions of Emotions*, SSRN, 1, 1 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.
[50] 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 43.

these systems claim they can do everything from identify sexuality to predict likelihood of engaging in criminal behavior to detect autism, and all from analyzing a person's face.[51]

However, these "predictive" technologies rely largely on historical data which carries with it historical bias, assumptions, and injustice. Systems predicting criminality extrapolate and train from datasets created by racist criminal justice systems which disproportionately punish people of color, perpetuating an ongoing racially discriminative system.[52] These systems impose a burden of suspicion on already-marginalized groups, including people of color, gender minorities, and people with disabilities, for no conclusive benefit, as there is no conclusive evidence that physical appearance is in any way connected to character traits.[53] Both emotion recognition and behavioral categorization systems are inherently flawed and biased, generating risk that will be disproportionately borne by already-vulnerable groups and providing little to no substantive benefit. Accordingly, EPIC recommends that they be explicitly banned by the Code.

---

[51] *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 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.

[52] *See* Pascu, *supra* note 51; 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 46 at 46 (Noting that predictive algorithms rely on historical data that reproduces harmful trends for marginalized individuals).

[53] *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.

4. EPIC urges the Commissioner to consider mandating public dissemination of policies and procedures for the operation of surveillance camera systems, particularly where the operator is a relevant authority

The Code states that clear policies and procedures relating to the operation of any surveillance camera system carry significant benefits.[54] EPIC concurs. However, EPIC believes that those benefits will be more consistently realized if the Code requires operators of surveillance camera systems to make their policies and procedures for operation public.

As noted in the Code's introduction, the goal of the Code is to enable users to "make legitimate use" of surveillance camera systems in such a way that meets public expectation and "maintains public trust and confidence."[55] Similarly, Principle 3 of the Code and its subsections repeatedly emphasize that "there must be as much transparency in the use of a surveillance camera system as possible."[56] Making the policies and procedures of the operation of these systems public would both demonstrate transparency and promote public trust and confidence in the systems and their application.

Further, the Code specifically notes that the published policies of operators which are relevant authorities "will form part of the body of law under which they operate."[57] Given the legal weight of these policies and procedures, they must be made publicly available for review and reference. While repeated reference to "publishing" and "published" policies seems to imply that these policies and procedures should be made publicly available, the text of the Code does not include a clear mandate to do so. Accordingly, EPIC recommends that the Commissioner add

[54] Draft Updated Surveillance Camera Code of Practice (2021) at Principle 5.1.
[55] Draft Updated Surveillance Camera Code of Practice (2021) at Introduction and Overview, Section 3.
[56] Draft Updated Surveillance Camera Code of Practice (2021) at Principle 3.
[57] Draft Updated Surveillance Camera Code of Practice (2021) at Principle 5.1.

text that explicitly requires that policies and procedures relating to the operation of surveillance camera systems be made publicly available.

Conclusion

The Commissioner should incorporate the recommendations for change and addition listed above into the Code in order to more fully align the updated Code with the current legal landscape, protect the fundamental rights of individuals, and engender public trust and confidence. EPIC urges the Commissioner to (i) formalize requirements for consultations and assessments, (ii) strengthen protections against improper use of facial recognition and biometric recognition systems, (iii) ban emotion recognition and biometric categorization systems, (iv) promote public access to relevant policies and procedures on use of these systems, (v) evaluate whether use of matching technologies is justified, and (vi) ban all forms of facial recognition technology. We believe that these actions will strengthen individual protections, guard against perpetuating bias, and aid in countering potential misuse of and discrimination through surveillance camera system use.

Respectfully Submitted,

Calli Schroeder
Calli Schroeder
EPIC Global Privacy Counsel