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

IDENTITY AND TRUST TEAM (TECHNICAL POLICY)

of the

UNITED KINGDOM INFORMATION COMMISSIONER'S OFFICE

Regarding the

ICO Consultation on the Draft Biometric Data Guidance

October 20, 2023

By notices published August 18, 2023, the United Kingdom's Information Commissioner's Office (the "Commission") has solicited feedback on its draft biometric data guidance (hereinafter "Guidance"),[1] to close on October 20, 2023.[2] This Guidance is intended to address use of biometric technologies and processing of biometric data, including how data protection law applies to use of biometric recognition systems. The consultation includes a set response form with the option to send further response to the Identity and Trust Team (Technology Policy) of the Information Commissioner's Office. Pursuant to the request for views on biometrics to inform the Commission's work in this area, the Electronic Privacy Information Center ("EPIC") submits the following comments.

[1] *Guidance on Biometric Data*, available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/guidance-on-biometric-data/.
[2] Information Commissioner's Office, *ICO Consultation on the Draft Biometric Data Guidance,* Identity and Trust Team (Technology Policy) (Aug. 18, 2023), https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-biometric-data-guidance/.

EPIC is a public interest research center based in Washington, D.C., established in 1994 to focus public and regulatory attention on emerging privacy and human rights issues and to protect privacy, freedom of expression, and democratic values in the information age.[3] EPIC has a long history of promoting individual and societal privacy interests relating to biometric data, both nationally and internationally.[4] EPIC has submitted comments to proposed regulations, guidelines, and practices at the state, federal, and international level as well as filing amicus curiae briefs in cases addressing biometric data use and calling for a ban on face surveillance.[5]

EPIC welcomes this opportunity to contribute to the Commission's efforts to put forth clear guidance on the use of biometric data and technologies. While the Guidance provides some excellent and broad information and recommendations to aid private companies in ensuring that any use of biometric recognition systems is compliant with existing law, we believe that gaps exist. Filling those gaps would not only aid the public by clarifying standards on when using biometric systems is appropriate and how private companies may intersect with law enforcement in this area, but would also promote public confidence that the Commission is actively protecting

---

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

[4] *See, e.g.,* EPIC, *Face Surveillance and Biometrics* (last viewed Oct. 19, 2023), https://epic.org/issues/surveillance-oversight/face-surveillance/; Brief of Amicus Curiae EPIC, et al, Supporting Appellant, New Jersey v. Arteaga, No. A-3078-21T1 (N.J. Super. App. Div.) (Sept. 26,2022), available at https://epic.org/documents/new-jersey-v-arteaga/; Letter of EPIC, *Letter to the Senate Finance Committee Chair Supporting SB169/HB33,* Maryland General Assembly (Feb. 7, 2023), available at https://epic.org/documents/maryland-sb169-biometric-identifiers/; Comments of EPIC et al, *Regarding the Public and Private Sector Uses of Biometric Technologies,* Office of Science and Technology Policy (Jan. 15, 2022), available at https://epic.org/documents/epic-comments-to-ostp-on-public-and-private-sector-uses-of-biometric-technologies/; Comments of EPIC, *DHS Data Privacy and Integrity Advisory Committee; Committee Management; Notice of Federal Advisory Committee Meeting,* Department of Homeland Security Data Privacy and Integrity Advisory Committee (Dec. 10, 2018), available at https://www.dhs.gov/sites/default/files/publications/EPIC-Comments-DHS-DPIAC-Face-Rec-Report-Dec-2018.pdf; Comments of EPIC, *Request for Information on Federal Video and Image Analytics Research and Development Action Plan,* National Science Foundation, 87 Fed. Reg. 42,212 (Sept. 2, 2022), available at https://epic.org/documents/epic-comments-in-re-federal-video-and-image-analytics-research-development-action-plan/; Comments of EPIC, *Notice of Consultation and Call for Comments: Privacy Guidance on Facial Recognition for Police Agencies,* Office of the Privacy Commissioner of Canada (Oct. 15, 2021), available at https://epic.org/documents/draft-guidance-to-canadian-police-agencies-on-facial-recognition/.

[5] *Id.*

their rights in the face of rapidly-shifting technology and industry claims of shifting norms.

Broadly, we recommend that the Commission do the following:

- Set forth specific obligations and guidelines relating to law enforcement use of biometrics systems provided by private companies or access to those biometric systems and the data therein.
- Ban the use of Live Facial Recognition.
- Mandate disclosure of any private companies providing biometric systems or information to law enforcement.
- Require a human in the loop of all automated decision making.
- Add specific baseline security requirements for any system processing biometric information, including a template risk assessment.
- Ban all use of "soft biometrics" such as biometric emotional analysis, criminal proclivity assessment, aggression detection, etc.

I. EPIC recommends that the Commission sets forth clear guidelines and legislation that addresses the pervasiveness of law enforcement ties to public companies' biometric systems and establishes clear limits and standards.

While we acknowledge that the Guidance is not intended to directly cover use of biometric systems for law enforcement purposes or security services, the line between public and private use is increasingly blurry. Circumstances in which law enforcement have access to private sector biometric recognition systems, either voluntarily or through legal order, should be addressed directly in the Guidance, associated regulations, and supplementary documents. Law enforcement and government bodies regularly either make contracts with private companies to use their biometric systems and data sets or informally request biometric data from private companies, evading legal standards requiring a reasonable basis for such requests. There must be guidelines and strong regulatory standards in place to establish when and under what conditions private companies and law enforcement may interact appropriately.

A. Law enforcement use of private/corporate biometric systems and data is expanding

One key area in which private companies' collection and use of biometric data is intertwined with government use is through facial recognition technologies. UK law enforcement has used facial recognition technology for years. Now, several police forces are deploying live facial recognition technology, including the Metropolitan Police and the South Wales Police.[6] Live facial recognition is running rampant in the UK across both public spaces and more sensitive locations, like schools.[7] Most notably, the Metropolitan Police used live facial recognition technology at King Charles's coronation earlier this year, an event that drew hundreds of thousands of people, making the event the largest use of live facial recognition in UK history.[8]

Researchers and privacy advocates, among others, have voiced numerous concerns about police use of this technology. In particular, privacy and civil liberties organizations Liberty and Big Brother Watch have warned that widespread police use of facial recognition could turn the UK into a surveillance state.[9] They also expressed concerns about the technology being inaccurate and discriminatory.[10] These same concerns were reflected in a 2020 case brought by a

---

[6] Paige Collings & Matthew Guariglia, *Ban Government Use of Facial Recognition in the UK*, Electronic Frontier Foundation (Sept. 26, 2022), https://www.eff.org/deeplinks/2022/09/ban-government-use-face-recognition-uk.
[7] Adam Satariano and Kashmir Hill, *Barred From Grocery Stores by Facial Recognition,* The New York Times (June 28, 2023, updated July 4, 2023), https://www.nytimes.com/2023/06/28/technology/facial-recognition-shoplifters-britain.html; Collings and Guariglia, *supra* note 6; *Biometric Britain: The Expansion of Facial Recognition Surveillance,* Big Brother Watch (May 23, 2023), available at https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf; *Facial Recognition Technology,* Metropolitan Police (accessed Oct. 19, 2023), https://www.met.police.uk/advice/advice-and-information/fr/facial-recognition-technology/; Jamie Grierson, *MPs and Peers Call for 'Immediate Stop' to Live Facial Recognition Surveillance,* The Guardian (Oct. 6, 2023), https://www.theguardian.com/technology/2023/oct/06/mps-and-peers-call-for-immediate-stop-to-live-facial-recognition-surveillance.
[8] Vikram Dodd, *Police Accused over Use of Facial Recognition at King Charles's Coronation*, The Guardian (May 3, 2023), https://www.theguardian.com/uk-news/2023/may/03/metropolitan-police-live-facial-recognition-in-crowds-at-king-charles-coronation.
[9] Big Brother Watch, *supra* note 7; *Facial Recognition Tech: Liberty 'Police Racism' Claim*, BBC (Apr. 8, 2023), https://www.bbc.com/news/uk-wales-65214494.
[10] *Id.*

civil liberties campaigner in which the court of appeal ruled that the South Wales police use of facial recognition technology violated privacy rights and equalities law.[11] Similarly, a 2022 report out of the University of Cambridge found that police use of live facial recognition violates ethical standards and human rights laws.[12]

Despite these concerns, police use of facial recognition is only increasing. For example, UK Policing Minister Chris Philp has called for all police forces across the UK to employ facial recognition technologies.[13] Additionally, in August, the government released plans to implement new biometrics systems across the nation over the next 12-18 months and asked private companies to submit their live facial recognition technologies for consideration.[14]

Live facial recognition systems are not the only concern. In the past couple of years alone, London signed a 3 million pound contract to buy retrospective facial recognition technology,[15] and courts approved contracts regarding DNA databases outsourced from private companies.[16]

Private companies do not develop technologies or policies in a vacuum – they are heavily influenced by law enforcement and government bodies' practices and stated desires. Widespread use of this technology lends itself to the continued erosion of the public and private divide. This

---

[11] Dan Sabbagh, *South Wales Police Lose Landmark Facial Recognition Case*, The Guardian (Aug. 11, 2020), https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case.
[12] Vikram Dodd, *UK Police Use of Live Facial Recognition Unlawful and Unethical, Report Finds*, The Guardian (Oct. 27, 2022), https://www.theguardian.com/technology/2022/oct/27/live-facial-recognition-police-study-uk.
[13] Bianca Gonzalez, *Policing Minister Pushes for Facial Recognition in All UK Police Forces Despite Criticism*, BiometricUpdate.com (May 16, 2023), https://www.biometricupdate.com/202305/policing-minister-pushes-for-facial-recognition-in-all-uk-police-forces-despite-criticism.
[14] Anna Gross & Madhumita Murgia, *UK Government Seeks Expanded Use of AI-Based Facial Recognition by Police*, Financial Times (Aug. 30, 2023), https://www.ft.com/content/858981e5-41e1-47f1-9187-009ad660bbbd.
[15] *Retrospective Facial Recognition System,* Mayor of London Office for Policing and Crime, DMPC Decision – PCD 1008 (Aug. 19, 2021), available at https://www.london.gov.uk/sites/default/files/pcd_1008_retrospective_facial_recognition_system.pdf.
[16] *M, R (On the Application Of) v The Chief Constable of Sussex Police*, Court of Appeal (Civil Division) on Appeal from the High Court of Justice, EWCA Civ 42 (Jan. 19, 2021) (Case No: C1/2019/2622 & C1/2019/2623), available at https://www.bailii.org/ew/cases/EWCA/Civ/2021/42.html.

intersection of private and public use of biometric systems is not new, and companies need guidance and enforceable regulations to adequately protect uniquely sensitive consumer data like biometric data.

B. Existing legal guidance, oversight, and standards in this area are insufficient.

The Commission must provide clear guidelines and regulations outlining what circumstances permit private companies to cooperate with law enforcement requests for biometric data. Current oversight for law enforcement and intelligence community use of biometric data is severely lacking. Commissions are created and left to decay.[17] Commissioners are given oversight power and then the position is dissolved and apportioned to other overstressed positions.[18] Even with some meagre safeguards in place on the public end of the transaction, the U.K. government is not adequately protecting biometric privacy. Guidance that fails to address government and law enforcement use of and interactions with private companies' biometric systems is incomplete.

Even where applicable legal protections exist, they are not always clearly or properly enforced. For example, the use of biometric data takes the existing issue of dragnet surveillance to new heights of invasiveness and fails to meet the standards of lawfulness, necessity, and proportionality under the Human Rights Act standard.[19] Abrogating the privacy rights in Article 8 of the Human Rights Act can only be done for certain purposes and in certain circumstances.

---

[17] Matthew Ryder QC, *The Ryder Review: Independent legal review of the governance of biometric data in England and Wales*, Ada Lovelace Institute at 41 (June 2022), available at https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf.

[18] Chris Burt, *UK Biometrics Commissioner resigns in anticipation of role's elimination*, Biometric Update (Aug. 8, 2023), https://www.biometricupdate.com/202308/uk-biometrics-commissioner-resigns-in-anticipation-of-roles-elimination.

[19] *See* Human Rights Act 1998; *Case of S. and Marper v. the United Kingdom* [GC], no. 30562/04 30566/04 § 101-104 (Apr. 12, 2008).

Law enforcement agencies often claim that the technology is necessary and proportionate, pointing to cases solved with the technology, but conveniently ignoring that most cases could have been solved by other methods or choosing not to admit when biometric technology failed to assist in cases or generated incorrect results.[20] Since there is little oversight over the procurement and use of this technology, this routine claim is rarely challenged.[21]

Further, law enforcement will often use the most extreme circumstances - such as terrorism and apprehending child abductors[22] - to justify widespread use of biometric technology. However, justification in extreme circumstances leads to dangerous mission creep. Now that the technology is in use, it seems as if it wouldn't be such a big shift to extend it to smaller cases – shoplifting, vandalism, protests, and more. Biometric technology's purported usefulness in extreme circumstances does not excuse the inordinate level of harm to UK citizens through the constant processing of their biometric data.[23]

Law enforcement use of biometric systems frequently extends far beyond what is strictly necessary to address the specific issue concerned and is wildly disproportionate since the same goals can be achieved through far less invasive methods. Law enforcement has been able to solve crime, see to public safety, and address national security effectively far before biometric systems came into existence – it is not suddenly impossible to do so without these invasive systems.

---

[20] Sebastian Klovig Skelton, *UK police double down on 'improved' facial recognition*, ComputerWeekly.com (Apr. 12, 2023), https://www.computerweekly.com/news/365535008/UK-police-double-down-on-improved-facial-recognition.

[21] *See, e.g., Bridges, R (On the Application Of) v The Chief Constable of South Wales Police*, Court of Appeal (Civil Division) on Appeal from the High Court of Justice, EWHC Civ 1058 (Aug. 11. 2020) (Case No: C1/2019/2670), available at https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

[22] Artificial Intelligence Act, Title II, Article 5(1)(d).

[23] *Countermeasures: The Need for new Legislation to Govern Biometric Technologies in the UK,* Ada Lovelace Institute (June 2022), available at https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/Countermeasures-the-need-for-new-legislation-to-govern-biometric-technologies-in-the-UK-Ada-Lovelace-Institute-June-2022.pdf.

Despite the massive expansion of biometric systems, government oversight in this area has been actively restricted and repealed. The Home Secretary established an Oversight and Advisory Board pertaining to law enforcement use of facial recognition.[24] The membership included the Surveillance Camera Commissioner (which no longer exists), the Information Commissioner, the Biometrics Commissioner (which also no longer exists), and the Forensics Science Commissioner.[25] The positions that no longer exist were dissolved and some (but not all) of their duties were absorbed into the remit Information Commissioner and the Investigatory Powers Commissioner, positions which already have full workloads outside of a biometrics specialty.[26] The Oversight and Advisory Board itself hasn't met since 2019, although the UK Government alleges it has been replaced with a different mechanism which remains unspecified.[27] By dissolving the positions focused solely on biometrics and surveillance techniques with the power and expertise to protect citizen privacy in this complex area, the UK government diluted the actual enforcement power and oversight of biometrics use.

Finally, even where enforcement action is actually taken to protect citizen rights, private companies still refuse to obey. In May of 2023, the Austrian SA found that Clearview AI's dragnet capture of facial images and thereafter processing them for their algorithm and further matching those images for law enforcement purposes violated article 5, 6, 9, and 27 of the GDPR.[28] The company was told to designate a representative within the EU and to delete the personal data from its databases.[29] Clearview AI has already faced extensive legal actions from

[24] Ryder QC, *supra* note 17 at 41.
[25] *Id.*
[26] Burt, *supra* note 18.
[27] Ryder QC, *supra* note 17 at 41.
[28] Decision by the Austrian SA against Clearview AI Infringements of Articles 5, 6, 9, 27 GDPR, European Data Protection Board (May 12, 2023), available at https://edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en.
[29] *Id.*

international Data Protection Agencies for violations of privacy laws, including in Greece,[30] Sweden,[31] Germany,[32] Italy,[33] Belgium,[34] France,[35] Australia,[36] Canada,[37] and the UK itself.[38] Despite the wave of legal actions, orders to divest data, and fines levied, Clearview AI has not complied with orders or changed practices. The CNIL has had to fine Clearview AI again for its lack of compliance in deleting the personal data of its residents.[39] Biometric privacy cannot be regulated from just one angle. Both the private and public controllers of this highly sensitive data must be adequately regulated as well as given the teeth to actually enforce the (meagre) protections left in place. To that end, the Guidance must be updated and regulations put in place that would enforce privacy violations stemming from use of biometric systems.

---

[30] Natasha Lomas, *Selfie scraping Clearview AI hit with another €20M ban order in Europe,* TechCrunch (July 13, 2022), https://techcrunch.com/2022/07/13/clearview-greek-ban-order/.
[31] Natasha Lomas, *Sweden's data watchdog slaps police for unlawful use of Clearview AI,* TechCrunch (February 12, 2021), https://techcrunch.com/2021/02/12/swedens-data-watchdog-slaps-police-for-unlawful-use-of-clearview-ai/.
[32] *Clearview AI deemed illegal in the EU, but only partial deletion ordered,* NOYB (January 28, 2021), https://noyb.eu/en/clearview-ai-deemed-illegal-eu.
[33] *Facial recognition: Italian SA fines Clearview AI eur 20 million, bans use of biometric data and monitoring of Italian data subjects,* Garante per law Protezione dei Dati Personali (March 9, 2022), https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9751323#english.
[34] Pieter Haeck, *Belgian police watchdog rules use of Clearview AI 'unlawful',* Politico (March 10, 2022), https://subscriber.politicopro.com/article/2022/03/belgian-police-watchdog-rules-use-of-clearview-ai-unlawful-00016045.
[35] *Facial recognition: the CNIL orders Clearview AI to stop reusing photographs available on the internet,* CNIL (December 16, 2021), https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet.
[36] *Clearview AI breached Australians' privacy,* OAIC (November 3, 2021), https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy.
[37] Zack Whittaker, *Clearview AI ruled 'illegal' by Canadian privacy authorities,* TechCrunch (February 3, 2021), https://techcrunch.com/2021/02/03/clearview-ai-ruled-illegal-by-canadian-privacy-authorities/.
[38] *Clearview AI Inc. Monetary Penalty Notice,* ICO (May 26, 2022), https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/; *Clearview AI Inc. Enforcement Notice,* ICO (May 26, 2022), https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/.
[39] Natasha Lomas, *Clearview fined again in France for failing to comply with privacy orders,* TechCrunch (May 10, 2023), https://techcrunch.com/2023/05/10/clearview-ai-another-cnil-gspr-fine/.

Recommendations

1. The Commission must outline procedures and special protections required when selling a product that collects/processes biometrics, particularly when sold to or shared with law enforcement.

2. The Commission must issue clear guidelines as to the circumstances in which private companies can sell biometric systems to or share data from those systems with law enforcement.

3. The use of Live Facial Recognition must be banned for all parties. If there is not an outright ban of Live Facial Recognition, the Guidance should follow the Proposed EU AI Act standard limiting the use of the technology to active terrorist threat and other exceedingly high priority and exigent circumstances. Those circumstances should be strictly limited and explicitly laid out in the Guidance rather than allowing for individual or law enforcement department-level discretion as to what constitutes "exigent circumstances."

4. Private companies that work with police and disclose biometrics or license the use of biometric data or systems must be legally required to disclose this fact to consumers upfront prior to any consumer biometric data collection or processing.

5. Companies must be required to include law enforcement use of their product when drafting their DPIAs. There should be a section on accuracy/bias/discrimination and the impact on literal life and liberty of individuals interacting with the UK law enforcement system, assigning clear liability for any wrongful, discriminatory, inaccurate, or improper biometric use and resulting impact on individuals. Security of this data should also be expanded in available documents (for example, the Commission-issued "Guide to Data Security" does not currently mention biometrics or the heightened security risks and requirements associated with biometric data and processing).[40]

6. Ban use of facial analysis as crime prediction.[41]

7. For any automated decision-making system interfacing with law enforcement, mandate that there must be a human in the loop conducting final review of any automated decisions or results.

---

[40] *A guide to data security*, Information Commissioner's Office (accessed Oct. 18, 2023), available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security.

[41] Xiaolin Wu and Xi Zhang, *Automated Inference on Criminality Using Face Images,* arXiv 1611.04135v1 (Nov. 13, 2016, https://arxiv.org/abs/1611.04135v1; Kevin Bowyer, Michael King, Walter Scheirer, and Kushal Vangara, *The "Criminality From Face" Illusion,* IEEE Transactions on Technology and Society Vol. 1, No. 4, 175 (Dec. 2020), available at https://ieeexplore.ieee.org/document/9233349.

II. EPIC recommends that the Commission set forth baseline security standards for any biometrics processing, including a template or example risk assessment.

The Guidance includes some discussion of appropriate security measures in "Data protection requirements when using biometric data: How do we deal with security risks?" This section briefly addresses the high sensitivity of biometric data, its largely unalterable nature, and the need for proper security measures. However, this section should either be expanded or the Commission should take additional steps beyond the Guidance itself to address security needs more thoroughly. Specifically, we believe that the Commission must enact strict privacy, data minimization, and cybersecurity standards to meet the unique threats posed by biometric data breaches.

As is mentioned in the Guidance, biometrics can pose a serious security risk when compromised because biometric characteristics are immutable. A person cannot simply reset their fingerprints, irises, or face geometry as they can a compromised password. When companies hold valuable data like biometrics, the question isn't if a data breach will happen, but when.

We have repeatedly seen over the past two decades that entities holding large volumes of biometric data will eventually experience a breach. In both the U.S. and the UK, data breaches are common across both government and private sector systems, with significant losses of biometric data occurring at regular intervals. Take, for example, the highest profile UK biometric data breach in recent years - the breach of UK security company Suprema's Biostar 2 database.[42] The Biostar 2 database was particularly poorly designed, storing more than 1 million unencrypted fingerprint scans and facial recognition images in a system integrated into high-

[42] Josh Taylor, *Major breach found in biometrics system used by banks, UK police and defence firms*, The Guardian (Aug. 14, 2019), https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

security facility access used around the world. Security researcher Noam Rotem, who found the breach, noted that the security flaws underlying Biostar 2 were far from unique: "'It's very common. There's literally millions of open systems, and going through them is a very tedious process,' he said. 'And some of the systems are quite sensitive.'"[43]

UK government bodies are not exempt from the problem of improperly processing unnecessary biometric data. For example, the UK's tax authority, HM Revenue and Customs, collected more than 7 million voiceprints between 2017 and 2019 – 5 million of those without proper consent.[44] It was ordered to delete all records lacking fully informed consent once this practice came to light.[45] This entire debacle need never have occurred – it was always possible to use standard passwords without biometric voiceprints being collected at all. This highlights the pervasive problem with leaping to biometric data use when there are less invasive alternatives available. Mandating data minimization and requiring companies to demonstrate that no viable alternative approach exists before processing biometric data would address serious security and misuse problems.

Companies can make breaches much less likely and severe by implementing heightened security measures on biometric information from the start and by default. Part of this process includes risk assessments. The current Guidance does urge readers to carry out a risk analysis, but the listed considerations are woefully incomplete. Even the linked guide to data security does not clearly state that biometric data is a high-risk form of personal data and must be subject to additional protections. We recommend that the Commission put forth a template or example risk

---

[43] *Id.*
[44] Natasha Lomas, *UK tax office ordered to delete millions of unlawful biometric voiceprints,* TechCrunch (May 10, 2019), https://techcrunch.com/2019/05/10/uk-tax-office-ordered-to-delete-millions-of-unlawful-biometric-voiceprints/.
[45] *Id.*

analysis which includes questions that must be asked. For example, i) is there a way to achieve the goal without processing biometric data, ii) have we confirmed that only the minimum amount of biometric data necessary is collected, iii) is biometric data deleted immediately after the purpose for which it was collected is fulfilled, iv) is the data held in an encrypted form, v) is access to the data strictly limited and are access controls regularly reviewed and updated, vi) is sharing of biometric data performed only with data protection agreements in place, etc.

In short, strong data minimization and cybersecurity requirements for biometrics are a necessity. The best and most secure use of biometric data is for on-device 1:1 matching for identity verification purposes. Whenever this shifts (biometric data is used or held off-device, the matching is many to one, the data is used for purposes beyond identity verification, etc.), the risk of breach or improper data use dramatically increases.

III. *EPIC recommends that the Commission ban all use of "soft biometrics" and add additional details on the risks of scale and scope of harm that accompany AI integration with biometric systems.*

The high risks created by biometric data processing will only be exacerbated as artificial intelligence ("AI") systems are increasingly used for mass data analysis and incorporated into existing systems. Biometric data can be subjected to algorithmic systems for analysis, which results in a massive expansion of the reach, impact, and risk potential of biometric systems. The Guidance currently discusses the risk of bias and discrimination in biometric systems using AI, frequently a problem of accuracy or access. This is a serious problem and should be probed. However, this is not the only risk raised by the combination of AI and biometrics.

AI systems can scan biometrics at a speed and scale far beyond human review. This poses a serious risk to privacy rights – and risk of misuse. The voice recognition technology that responds in systems like Alexa or Siri has also been used for years by the NSA to automatically

identify speakers through voiceprints and monitor that voice across millions of recordings.[46] This is ostensibly to search for criminals or terrorists, but can be (and has been) easily misused to track individuals like politicians, whistle blowers, protest leaders, journalists, their sources, and more.[47] With billions of recordings of faces, fingerprints, voices, movements, and other biometric data, the potential for surveillance and misuse is near limitless.

The risks of these systems are not just the scale of expanded biometric data processing, but the type of processing. AI incorporation gives companies and people false confidence that a system has some hidden insight into matters that frequently either require expertise or cannot be accurately determined through biometric evaluation. This frequently means evaluating "behavioral attributes," such as emotional state, mental state, personality traits, moral characteristics, and other generalizable qualities, referred to by some experts as "soft biometrics."[48] For example, AI has already been incorporated into systems that claim the ability to scan biometrics to sense a person's emotion,[49] evaluate employability,[50] identify mental disorders,[51] determine if a person is drowsy or distracted,[52] or even determine likelihood of criminality.[53]

---

[46] Ava Kofman, *Finding Your Voice: Forget About Siri and Alexa – When It Comes to Voice Identification, the "NSA Reigns Supreme,"* The Intercept (Jan. 19, 2018), https://theintercept.com/2018/01/19/voice-recognition-technology-nsa/.
[47] *Id.*
[48] Xiaowei Wang, Shazeda Ahmed, *Bodily Harms: Mapping the Risks of Emerging Biometric Tech*, Access Now at 6 (Oct. 2023), available at https://www.accessnow.org/wp-content/uploads/2023/10/Bodily-harms-mapping-the-risks-of-emerging-biometric-tech.pdf.
[49] Nick Haber, Catalin Voss, Dennis Wall, *Upgraded Google Glass Helps Autistic Kids "See" Emotions*, IEEE Spectrum (Mar. 26, 2020), https://spectrum.ieee.org/upgraded-google-glass-helps-autistic-kids-see-emotions.
[50] Drew Harwell, *A face-scanning algorithm increasingly decides whether you deserve the job*, The Washington Post (Nov. 6, 2019), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.
[51] Ingrid K. Williams, *Can A.I.-Driven Voice Analysis Help Identify Mental Disorders?,* The New York Times (Apr. 5, 2022), https://www.nytimes.com/2022/04/05/technology/ai-voice-analysis-mental-health.html.
[52] Interior Sensing AI, https://go.affectiva.com/auto.
[53] Sidney Fussell, *An Algorithm That 'Predicts' Criminality Based on a Face Sparks a Furor*, Wired (June 24, 2020), https://www.wired.com/story/algorithm-predicts-criminality-based-face-sparks-furor/.

The real-life impacts of using AI as a decision maker in these serious areas can be catastrophic. If a biometric system algorithmically predicts that a person is likely to be a criminal, will they be the target of unjust law enforcement surveillance or harassment? Will it affect job, housing, or financial prospects? What is the recourse when an AI uses biometrics to determine that a job applicant should be rejected or a student looking away from a computer screen is cheating on a test?[54] Will we no longer have privacy in public at all if our voice, face, expressions, are movements are continually monitored and scanned?

We recommend that the Commission addresses the elevated risks of incorporating AI into biometric systems within the Guidance by noting that scale and scope of biometric evaluations is substantially expanded when AI is incorporated into the systems and setting forth the heightened review, assessment, limitations, and legal liabilities associated with algorithms incorporated into biometric systems. We further recommend that there be a full ban – both within the Guidance and in legislation - on using biometrics for emotion, characteristic, criminality, mental health, or other "soft biometrics" purposes.

Conclusion

The Commission should make the recommended updates to the Guidance and provide necessary supplemental documents in the areas mentioned above to bring further clarity, stability, and protection of privacy rights relating to biometric system use in the UK. These updates would reflect current discussions in biometric ethics and privacy rights and further establish the UK as a leader in human rights protections in emerging technology. EPIC urges the Commission to (i) set forth specific obligations and guidelines relating to law enforcement use of

[54] *See* Morgan Meaker, *This Student is Taking on 'Biased' Exam Software*, Wired (Apr. 5, 2023), https://www.wired.com/story/student-exam-software-bias-proctorio/.

biometrics systems provided by private companies or access to those biometric systems and the data therein; (ii) ban the use of Live Facial Recognition; (iii) mandate disclosure of any private companies providing biometric systems or information to law enforcement; (iv) require a human in the loop of all automated decision making; (v) add specific baseline security requirements for any system processing biometric information, including a template risk assessment; and (vi) ban all use of "soft biometrics" such as biometric emotional analysis, criminal proclivity assessment, aggression detection, etc. We believe that these actions will strengthen privacy protections, guard against harmful surveillance practices, and aid in mitigating several of the major harms of invasive biometric systems.

Respectfully submitted,

Calli Schroeder
Calli Schroeder
EPIC Senior Counsel and Global Privacy Counsel

Maria Villegas Bravo
Maria Villegas Bravo
EPIC Fellow

Kara Williams
Kara Williams
EPIC Fellow