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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

Regarding the

UPDATE TO GUIDANCE ON HANDLING BIOMETRIC INFORMATION

January 12, 2024

By notices published October 11, 2023, the Office of the Privacy Commissioner of Canada ("OPC") has solicited input on its guidance for both public[1] and private[2] sector organizations handling biometric information, to close on January 12, 2024.[3] These guidance documents are intended to update the biometrics guidance first published in 2011 and address evolutions in biometric technology and use as well as addressing how both the Personal Information Protection and Electronic Documents Act ("PIPEDA") and the Privacy Act intersect with biometric information processing. Pursuant to the request for input on the updated guidance documents, the Electronic Privacy Information Center ("EPIC") submits the following comments.

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.[4] EPIC has an

[1] *Draft Guidance for processing biometrics – for public institutions*, available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-bio/gd_bio_fed/.

[2] *Draft Guidance for processing biometrics – for organization*, available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-bio/gd_bio_org/.

[3] *Privacy Commissioner seeks input on draft biometrics guidance documents,* Office of the Privacy Commissioner of Canada (Oct. 11, 2023), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_231011/.

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

extensive history of promoting individual and societal privacy and civil rights interests relating to biometric information processing, both nationally and internationally.[5] 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 information use and calling for a ban on face surveillance.[6]

EPIC welcomes this opportunity to support the OPC's extensive work in putting forth clear guidance on the use of biometric information and technologies. We note the particular importance of this effort in light of the broader rise of development and use of biometric technologies and appreciate the efforts to counter the serious risks to individuals. The current guidance drafts are well-formed, including clear case examples, incorporating data principles, and setting forth what organizations must and should do relating to biometric information processing. However, we believe some gaps exist. Filling these gaps and clarifying the points listed below would not only aid organizations by clarifying standards for biometric information use, but would also promote public

[5] *See, e.g.*, EPIC, *EPIC Urges UK ICO To Address Law Enforcement Use of Private Data/Systems, Security Issues, AI, and "Soft Biometrics" in Draft Biometric Data* Guidance (Oct. 23, 2023), https://epic.org/epic-urges-uk-ico-to-address-law-enforcement-use-of-private-data-systems-security-issues-ai-and-soft-biometrics-in-draft-biometric-data-guidance/; 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/.

[6] *Id.*

confidence that the OPC is actively protecting their rights in the face of rapidly-shifting technology and industry claims of shifting norms. Broadly, we recommend that the OPC:

- Update both guidelines to specifically address the high risks of bias and discrimination when using biometric information, include measures to factor these risks into required assessments, and mitigate these risks where possible
- Set forth clear requirements on when and how the government can request access to biometric information held or processed by private organizations
- Ban all use of "soft biometrics"
- Address the heightened risks present where AI is used to analyze biometric information or is incorporated into biometric systems

1. ***EPIC recommends that both guidelines be updated to include specific mention of potential bias and discrimination when using biometric information***

While the draft guidelines currently make passing mention of potential bias problems, particularly when discussing accuracy, the pervasive and serious bias issues present in biometric information use warrant more explicit mention. Facial recognition technology alone has been demonstrated to misidentify people of color and transgender or non-binary individuals at a vastly increased rate to white and cisgender individuals.[7] 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

[7] *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 (Nov. 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 (Dec. 2019), available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

white men."[8] Independent analysis commissioned by the United Kingdom's Metropolitan Police found that matches made using the Metropolitan Police's facial recognition systems were inaccurate 81 percent of the time.[9] While the best commercially available algorithms available today display little bias in controlled testing conditions, the range in facial recognition products is broad, and even the best testing cannot account for all real-world deployments.[10] As input photo quality declines and novel types of image are submitted for facial recognition searches, bias becomes more likely. Further, even where facial recognition is formally unbiased, the systems built around facial recognition can unintentionally enshrine and amplify bias, resulting in heavily biased outcomes.[11]

The risk of misidentification is highest for population groups that already face outsized societal bias and discrimination. This concern must be addressed when assessing whether biometric information processing is appropriate. This should be done either by acknowledging where the risk of discrimination and bias is too high such that other methods should be used or by putting mitigating measures in place that will substantially reduce the risk of harm, like mandatory human review of the algorithm's output before any decision is made based off those results. We recommend that notice of the risk of bias and discrimination in biometric information use be explicitly included in both sets of guidance in the Overview section, in Identifying an Appropriate Purpose, in Limiting

[8] Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, The Washington Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

[9] Matt Burgess, *The Met Police will start using live facial recognition across London*, Wired (Jan. 24, 2020), https://www.wired.co.uk/article/london-met-police-facial-recognition.

[10] NIST, Face Recognition Technology Evaluation (FRTE) 1:N Identification, last updated 2023-09-29, https://pages.nist.gov/frvt/html/frvt1N.html.

[11] *See* Clare Garvie, *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Georgetown Center on Privacy and Technology (Dec. 6, 2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/; Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Georgetown Center on Privacy and Technology (May 16, 2019), https://www.flawedfacedata.com.

Use, Disclosure, and Retention, in Safeguards, in Accuracy, and in Accountability. The risk of bias affects each of these sections substantially and should be specifically noted.

Finally, the "biometric categorization" section in the Overview should note that certain categorizations are extremely high-risk and should either not be performed or should only be performed in exceptional circumstances. For example, sorting individuals by race or gender can lead to additional discrimination unless there is a strong and legitimate justification for doing so. Even where these categorizations prove to be performed accurately, there are few uses that do not carry with them elements of discrimination and high potential for misuse that would violate civil liberties.[12]

2. ***EPIC recommends that the OPC set forth clear guidelines addressing the pervasive law enforcement ties to private companies' biometric systems and establish clear limits and standards.***

The line between public and private data collection and use is increasingly blurry. It is common for law enforcement to access private sector biometric recognition systems, both through third party contracts and through voluntary information sharing requests. The draft guidance for public organizations mentions requirements for privacy review before contracting with third party service providers which is an excellent step in addressing this overlap. However, law enforcement and government bodies regularly make informal requests for biometric information or access to biometric systems held by private companies, evading legal standards requiring a legitimate basis and formal process like warrants. The OPC has an opportunity to establish protections against this practice and make clear under what conditions private companies and law enforcement may appropriately interact.

[12] *See*, *e.g.*, Canada Human Rights Act, Part I (3).

Canadian law enforcement expanded their use of biometric technology, such as facial recognition, in the last few years. The OPC's investigation (in partnership with provincial authorities in Quebec, Alberta, and British Columbia) into the RCMP's use of Clearview AI concluded that Clearview AI's biometric information collection processes were legally non-compliant and that the RCMP failed to properly assess whether the practice was compliant with the Privacy Act before implementation.[13] Despite this finding and the subsequent suspension of Clearview AI use, the RCMP has continued to use at least two additional facial recognition tools and has failed to make public all biometric information processing practices.[14] The Minister of Citizenship and Immigration used Clearview AI's facial recognition software to strip two women of their refugee status – a decision that was ordered under review by a federal court due to possibly being based on a misidentification.[15]

This rise in law enforcement use of biometric information and lack of safeguards on law enforcement access to privately-held biometric information add up to a volatile and dangerous social precedent. Privacy and civil liberty advocates have repeatedly noted that expanded law enforcement use of biometric information could effectively create surveillance states.[16] The technology's embedded problems with accuracy and discrimination add to concerns over improper application and potentially harmful results for individuals.

[13] *Report of Finding: Investigation into the RCMP's collection of personal information from Clearview AI (involving facial recognition technology),* Office of the Privacy Commissioner of Canada (Jun. 10, 2021), https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#toc1.

[14] Maura Forrest, *RCMP's use of facial recognition extends well beyond Clearview AI,* Politico (Sept. 30, 2022), https://www.politico.com/news/2022/09/30/rcmps-facial-recognition-clearview-ai-00059639.

[15] Nicholas Keung, *Did Canada use facial-recognition software to strip two refugees of their status? A court wants better answers,* The Toronto Star (Sept. 19, 2022), https://www.thestar.com/news/canada/did-canada-use-facial-recognition-software-to-strip-two-refugees-of-their-status-a-court/article_83bc5ce7-8e0e-52e1-8a94-22d18ed058b1.html.

[16] *See, e.g., 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 Tech: Liberty 'Police Racism' Claim*, BBC (Apr. 8, 2023), https://www.bbc.com/news/uk-wales-65214494.

The OPC can help to directly address this problem by incorporating mandates in both sets of guidelines. First, the guidelines for private companies should explicitly state in the "keep a tight circle" portion that private organizations must require a warrant from law enforcement before sharing biometric information or allowing law enforcement to access biometric information that the private organization holds. Requiring warrants rather than allowing the organizations to comply with mere requests for access will provide better protections for individual information, provide more clarity for private companies regarding how they are legally permitted and required to limit access to biometric information, and encourage law enforcement to establish a reasonable basis for accessing biometric information.

Second, the guidelines for public institutions should include explicit language stating that they must obtain a warrant before requesting biometric information from private organizations. This makes expectations clear for public institutions, will provide limitations that keep law enforcement from improperly using their authority to intimidate private organizations into sharing biometric information without a reasonable basis, and may encourage law enforcement to seek out less invasive means of exercising authority.

3. ***EPIC recommends the OPC take note of the scale and scope of harms present where AI is integrated with biometric systems and ban use of biometrics to evaluate behavioral attributes***

Artificial intelligence ("AI") systems, which are becoming endemic to mass data analysis, exacerbate the existing high risks common in biometric information processing. Biometric information may be subjected to algorithmic systems for analysis, resulting in expanded reach, impact, and risk potential. Biometric systems using AI not only face bias and discrimination risks, but also risks due to the speed and scale of AI scanning and the types of processing biometric information may be used for.

AI systems are able to scan biometric information at speed and scale far beyond human review. This poses serious risks to privacy rights and high potential for misuse. For example, the voice recognition technology used in systems like Alexa or Siri has also been used for years by the NSA to automatically identify speakers through voiceprints and monitor individual speakers across millions of recordings.[17] While the NSA claims this is used to search for criminals or terrorists, it also can be (and has been) easily misused to track individuals like politicians, whistle blowers, protest leaders, journalists, their sources, and more.[18] With billions of biometric information points available for analysis by AI systems, the potential for surveillance and misuse is near limitless.

The applications of biometric information processing are also a high risk. AI incorporation often gives organizations and individuals false confidence that a system has some hidden insight into matters that either require expertise to determine 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, sometimes referred to as "soft biometrics."[19] For example, systems with AI incorporation have already claimed the ability to scan biometrics to determine a person's emotions,[20] evaluate employability,[21] identify mental disorders,[22] or determine when individuals are drowsy or

[17] 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/.

[18] *Id.*

[19] 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.

[20] 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.

[21] 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/.

[22] 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.

distracted.[23] There have even been claims that biometrics can be used to assess "criminality" through facial analysis – essentially amounting to digital phrenology.[24]

Many of these claims are literally not possible. There is no facial characteristic that ties to criminality and systems claiming to identify such a connection extrapolate and train from datasets created by racist criminal justice systems which disproportionately punish people of color, perpetuating historic injustice and an ongoing racially discriminative system.[25] Evaluations of emotion or employability will react incorrectly across cultural or neurologically diverse variances in expression. As noted in some academic rebuttals to the idea of emotion recognition, people regularly outwardly project emotions they are not feeling in order to appear more professional, pleasant, or nonconfrontational.[26] Emotion recognition technology assumes the existence of universal emotional expression and a strong correlation between physical expression and actual emotional state – neither of these things are reliable. Further, emotion recognition systems have been shown to hold

[23] Interior Sensing AI, https://go.affectiva.com/auto.

[24] 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; 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/.

[25] *See* 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-redicts-criminals-based-on-their-face-sparks-industry-controversy; 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.

[26] *See* James Vincent, *Discover the Stupidity of AI Emotion Recognition with This Little Browser Game*, The Verge (Apr. 6, 2021), https://www.theverge.com/2021/4/5/22369698/ai-emotion-recognition-unscientific-emojify-web-browser-game; Kate Crawford, *Artificial Intelligence is Misreading Human Emotion*, The Atlantic (Apr. 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/; Charlotte Gifford, *The Problem with Emotion-Detection Technology*, The New Economy (June 15, 2020), https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology.

significant racial bias, often assigning more threatening emotions to Black faces than White faces, regardless of expression.[27]

The impacts of combining AI with biometric information and using the results to make serious decisions can be catastrophic. Use of soft biometrics could subject individuals to unjust law enforcement surveillance and harassment, affect employment and housing prospects, impact financial and educational opportunities, and further marginalize communities already facing discrimination.

We recommend that the OPC explicitly ban or strictly limit use of biometric information for emotion, characteristic, criminality, mental health, or other soft biometrics purposes – including adjusting the language in the "biometric categorization" section of the overview of both guidance documents to remove mention of emotion recognition as if it is uncontroversial technology. We further recommend that the guidance address the elevated risks of AI incorporation into biometric information analysis and mandate heightened review, assessment, limitations, and legal liabilities for systems that use AI.

Conclusion

The OPC has clearly put substantial effort into carefully considering how best to guide both private and public organizations in their use of biometric information. We believe that the recommendations listed above would further improve the guidance, providing more substantial protections for consumers relating to privacy and civil liberties. We also feel these additions will benefit the organizations using biometric information by providing clarity and insight into what the

[27] Lauren Rhue, *Emotion-Reading Tech Fails the Racial Bias Test*, The Conversation (Jan. 3, 2019), https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404; Lauren Rhue, *Racial Influence on Automated Perceptions of Emotions*, SSRN, 1, 1 (2018), https://papers.ssrn.com/sol13/papers.cfm?abstract_id=3281765.

OPC expects. These updates would reflect current discussions in biometric ethics and privacy rights and further establish Canada as a leader in human rights protections in emerging technology. To that end, EPIC urges the OPC to (i) update the guidelines to specifically address the high risks of bias and discrimination tied to biometric information use and include recommendations to address these risks, (ii) set forth clear and enforceable requirements on where and how law enforcement can request access to biometric information held or processed by private organizations, (iii) ban all use of "soft biometrics," and (iv) address the heightened risks present where AI intersects with biometric information. We believe that these actions will strengthen privacy protections, guard against harmful surveillance practices, and aid in mitigating several major harms of invasive biometric systems.

Respectfully submitted,

Calli Schroeder

Calli Schroeder

EPIC Senior Counsel and Global Privacy Counsel