The Office of the United Nations High Commissioner for Human Rights: Input for the preparation of the 2024 report of the United Nations High Commissioner for Human Rights pursuant to Human Rights Council resolution 47/21 on the “Promotion and protection of the human rights and fundamental freedoms of Africans and of people of African descent against excessive use of force and other human rights violations by law enforcement officers through transformative change for racial justice and equality”

16 April 2024

INCLO input for the preparation of the 2024 report of the United Nations High Commissioner for Human Rights pursuant to Human Rights Council resolution 47/21

Introduction

1. The International Network of Civil Liberties Organisations (INCLO) is a network of 15 civil liberties organizations from around the globe.[1] We would like to thank the Office of the United Nations High Commissioner for Human Rights for the opportunity to provide an input for the preparation of the 2024 report of the United Nations High Commissioner for Human Rights pursuant to Human Rights Council resolution 47/21 on the “Promotion and protection of the human rights and fundamental freedoms of Africans and of people of African descent against excessive

[1] Participating members from INCLO include: Agora International Human Rights Group (Russia); Centro de Estudios Legales y Sociales (Argentina); the Hungarian Civil Liberties Union (Hungary); the Human Rights Law Centre (Australia); Irish Council for Civil Liberties (Ireland); Kenya Human Rights Commission (Kenya); KontraS (Indonesia); the Legal Resources Centre (South Africa); and Liberty [UK]

use of force and other human rights violations by law enforcement officers through transformative change for racial justice and equality".

2. With reference to research carried out by INCLO members in respect of law enforcement use of Facial Recognition Technology (FRT), we outline how this discriminatory tool is having a disproportionate impact on the rights of Africans and people of African descent, with clear evidence emerging from the United States.

3. Facial Recognition Technology (FRT) is a flawed but very powerful "toxic"[2] technology that, when used by law enforcement directly or indirectly, risks the misidentification of individuals but also the creation of an enduring and long-term chilling effect on individuals' ability to freely participate in public protest and move freely in publicly accessible places. As a probability-based biometric technology, it attempts to identify a person by comparing a biometric template created from a face detected in an image or video against a reference database of biometric templates. An FRT search generally results in the production of potential candidates accompanied by similarity scores. A threshold value is fixed to determine when the software will indicate that a probable match has occurred. Should this value be fixed too low or too high, respectively, it can create a high false positive rate (i.e. the percentage of incorrect matches identified by the technology) or a high false negative rate (i.e. the percentage of true matches that are not detected by the software). There is no single threshold setting which eliminates all errors.[3] There is also no guarantee that a 'true match' will be at the top of the FRT search return list, or that a law enforcement official will choose the correct 'true-match' from the list,[4] if one is even present.[5] The multiple components of an FRT system, together with the

[2] Irish Council for Civil Liberties, Leading experts warn against Garda use of FRT, October 2023, https://www.iccl.ie/digital-data/leading-facial-recognition-technology-experts-have-warned-against-garda-use-of-frt-saying-use-of-the-toxic-tool-would-result-in-a-massive-step-change-in-police-sur/

[3] Buolamwini J., Ordóñez V., Morgenstern J., and Learned-Miller E., Facial Recognition Technologies: A Primer, May 29, 2020, https://assets.websitefiles.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf

[4] Press, E., Does A.I. Lead Police to Ignore Contradictory Evidence?, New Yorker, November 2023, Robert Williams was wrongfully arrested in front of his wife and children, detained and arraigned by Detroit police after they used FRT to try to identify a shoplifter who stole a watch. The image of Williams was only the ninth most likely match for the probe photograph, which was obtained from surveillance video of the incident. But the analyst who ran the search did an assessment and decided Williams' image was the most similar to the suspect's. Two other algorithms were then run. In one, which returned 243 results, Williams wasn't even on the candidate list. In the other—of an F.B.I. database—the probe photograph generated no results at all, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence

[5] Cagle, M., When it Comes to Facial Recognition, There is No Such Thing as a Magic Number, American Civil Liberties Union (ACLU), February 2024,

steps involved in the working of such a system, and the multitudinous outside factors which can affect the performance of that system, makes attempts to identify a person with FRT a probabilistic, and therefore a deeply problematic, endeavour.[6] This is further compounded by the fact that existing FRT accuracy tests do not control for the many variables characterizing real-world police use of FRT.[7]

4. The discriminatory effects of FRT are well documented. Error rates will vary depending on the multiple factors which can affect the performance of an FRT system including, but not limited to, the quality of images used, the lighting, the pose of the person in the image/video, the creation of the database of images against which an image will be compared, and the selected threshold setting for 'similarity'.

5. However, these errors do not affect all individuals equally. Scientific studies have clearly demonstrated deeply inherent racial and gender biases in FRTs due to, in part, how they have been trained,[8] meaning women and people of color are more likely to be misidentified,[9] and therefore wrongly accused by police who use FRT, than light-skinned men. Computer vision models, the basis for FRT, have

https://www.aclu.org/news/privacy-technology/when-it-comes-to-facial-recognition-there-is-no-such-thing-as-a-magic-number

[6] Buolamwini J., Ordóñez V., Morgenstern J., and Learned-Miller E., Facial Recognition Technologies: A Primer, May 29, 2020, https://assets.websitefiles.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf

[7] Garvie, C., A Forensic Without the Science: Facial Recognition in U.S. Criminal Investigations at 15–16, Geo. L. Ctr. on Privacy & Tech. (2022), https://www.law.georgetown.edu/privacy-technology-center/publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/

[8] Buolamwini J., and Gebru T., Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. See also Deborah Raji I., and Buolamwini J., Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial ai products, Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, https://dl.acm.org/doi/10.1145/3306618.3314244. See also Cook C., Howard J., Sirotin Y., Tipton J., and Vemury A., Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2019 https://ieeexplore.ieee.org/document/8636231. See also NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, December 19, 2019. NIST wrote: "How accurately do face recognition software tools identify people of varied sex, age and racial background? According to a new study by the National Institute of Standards and Technology (NIST), the answer depends on the algorithm at the heart of the system, the application that uses it and the data it's fed — but the majority of face recognition algorithms exhibit demographic differentials. A differential means that an algorithm's ability to match two images of the same person varies from one demographic group to another." https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

[9] Press, E., Does A.I. Lead Police to Ignore Contradictory Evidence?: Too often, a facial-recognition search represents virtually the entirety of a police investigation, The New Yorker, November 13, 2023, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence

demonstrated how they are more likely to mislabel and mischaracterize Black men and Black women as 'chimpanzee', 'gorilla', 'orangutan', 'suspicious person', 'criminal', and 'thief';[10] and, disturbingly, how a Black man has a much higher chance of being classified as a 'criminal' than being classified as a 'human being'.[11]

6. Yet, however deeply discriminatory and defective FRT may be in respect of a given application, it is a technology which can enable powerful mass surveillance by stripping people of their anonymity, reducing people to walking license plates[12] and tilting the power dynamic inherent in police-civilian interactions further into the hands of police.[13] This is a particular risk when FRT is used on live or recorded video which threatens to allow police to efficiently track one or many individuals across multiple video feeds, or to pull up every instance of one or more persons appearing in video recordings over time.[14] This capability, which has already been used to devastating effect by some authoritarian governments,[15] threatens to chill people's fundamental rights to freedom of expression and protest. Members of the public, aware they are being watched, might alter their behavior and self-censor.[16] Such surveillance would also infringe on people's fundamental right to privacy. This technology threatens to give a government the unprecedented ability to

[10] Agarwal, S. et al., Evaluating CLIP: Towards Characterization of Broader Capabilities and Downstream Implications, August 2021, https://arxiv.org/pdf/2108.02818.pdf

[11] Birhane, A., et al, On haet scaling laws for data-swamps, June 2023, https://arxiv.org/pdf/2306.13141.pdf

[12] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted April 26, 2023, p.15, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

[13] Mozur, P., One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, New York Times, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Shahwan, N., From 'blue wolf' to 'red wolf': An automated Israeli occupation, Daily Sabah, May 15, 2023, https://www.dailysabah.com/opinion/op-ed/from-blue-wolf-to-red-wolf-an-automated-israeli-occupation

[14] ACLU Comment re: Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Exec. Order 14074, Section 13(e)), January, 2024, https://www.aclu.org/documents/aclu-comment-facial-recognition-and-biometric-technologies-eo-14074-13e

[15] See, e.g., Mozur, P., One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, New York Times, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Masri, L., How Facial Recognition Is Helping Putin Curb Dissent, Reuters, March 28, 2023, www.reuters.com, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/; Salaru, D., Int'l Press Inst., Russia: Facial Recognition Software Used to Target Journalists, International Press Institute, June 23, 2022, https://ipi.media/russia-facial-recognition-software-used-to-target-journalists/

[16] Murray, D., Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework, Modern Law Review, December 2023, https://onlinelibrary.wiley.com/doi/full/10.1111/1468-2230.12862

instantaneously identify and track anyone as they go about their daily lives; such invasive tracking could easily reveal sensitive details about an individual's political opinions, religious or philosophical beliefs, sex life or sexual orientation. The implications of police use of this "novel and untested"[17], "highly intrusive"[18], and "novel and controversial"[19] technology can vary depending on the purpose and scope of its use. But the use of FRT by law enforcement to locate, identify, track people, at scale, from a distance, without their knowledge, and often with significant discretion left to the law enforcement authority using the technology, can represent a seismic shift in the surveillance capabilities of police forces.[20] Some authorities have applied FRT to marginalized communities already over-surveilled,[21] for example the surveillance of Palestinians in the West Bank/Occupied Palestinian Territories,[22] meaning FRT can be used to deepen structural inequalities.

7. INCLO members previously documented 13 FRT case studies from around the world in its 2021 report *In Focus: Facial Recognition Tech Stories and Rights Harms from*

[17] Gullo K., Electronic Frontier Foundation, Victory! New Jersey Court Rules Police Must Give Defendant the Facial Recognition Algorithms Used to Identify Him, June 7, 2023, https://www.eff.org/deeplinks/2023/06/victory-new-jersey-court-rules-police-must-give-defendant-facial-recognition

[18] *Glukhin v Russia*, App no 11519/20, (European Court of Human Rights, 10 April 20203, https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-225655%22]}

[19] *R (Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058, par.201, https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

[20] Gainutdinov, D., International Network of Civil Liberties Organizations, In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World: Protesters under watch in Moscow, January 2021, p.15, https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf

[21] Amnesty International, Israel/OPT: Israeli authorities are using facial recognition technology to entrench apartheid, May 2, 2023, https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/ See also Fergus, R., American Civil Liberties Union, Facial recognition remains largely ungoverned - and dangerous - in Minnesota, February 2024, https://www.aclu-mn.org/en/news/biased-technology-automated-discrimination-facial-recognition#:~:text=The%20ACLU%20found%20that%20police,This%20simply%20isn't%20true

[22] Gan-Mor, G. and Pinchuk, A., International Network of Civil Liberties Organizations, In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World: Surveillance in the West Bank/Occupied Palestinian Territories, January 2021, p.11, https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf; see also Amnesty International, Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT, May 2023, https://www.amnesty.org/en/documents/mde15/6701/2023/en/; see also Frenkel S., Israel Deploys Expansive Facial Recognition Program in Gaza, New York Times, March 27, 2024, https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html?ugrp=c&unlocked_article_code=1.f00.5DIt.O0vT0ELrgEOM&smid=url-share

Around the World[23] and previously outlined in detail to the OHCHR[24] how FRT is harming people's fundamental rights across the globe. INCLO's work was subsequently cited twice in the OHCHR's Right to Privacy in the Digital Age report.[25] As INCLO members, and civil society coalitions all over the world,[26] have previously stated, the twin dangers of highly consequential misidentifications and pervasive surveillance mean law enforcement authorities should not be deploying FRT at all.[27]

8. When one assesses the potential human rights risks associated with FRT, one must consider many factors, including, but not limited to, the lifetime of an FRT system; its connection to other surveillance systems; the use, storage and destruction of the respective facial biometric identifiers; and the technical and organizational safeguards in place, or not, to protect those identifiers. Consideration must also be given as to whether there are any transparency and oversight mechanisms in place in respect of each component of an FRT system and each step involved in police use of FRT; the independence and efficacy, or lack thereof, of such mechanisms; and the question of how to hold ever-changing policing FRT systems, developers and manufacturers of those systems and users of those systems, accountable. There are many variables at play, and the tangible, real-life human rights implications of either identification or misidentification, of a person in photographs or video recordings, retrospective or live, are manifold.

[23] In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World, January 2021, INCLO, https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf

[24] INCLO input to the OHCHR for its report on The Right to Privacy in the Digital Age, June 2022, https://www.ohchr.org/sites/default/files/documents/issues/digitalage/reportprivindigage2022/submissions/2022-09-06/CFI-RTP-International-Network-of-Civil-Liberties-Organization.pdf

[25] Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/51/17, August 2022, https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf?token=TdRLrs22sZzOvcYt8N&fe=true

[26] European Digital Rights, Campaign "Reclaim Your Face" calls for a Ban on Biometric Mass Surveillance, November 2020, https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/

[27] Letter from ACLU et al. to Joseph R. Biden, President, United States of America (Feb. 16, 2021), https://www.aclu.org/sites/default/files/field_document/02.16.2021_coalition_letter_requesting_federal_moratorium_on_facial_recognition.pdf; Irish Council for Civil Liberties and Digital Rights Ireland, Submission to the Joint Oireachtas Committee on Justice Draft General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023, January 2024, https://www.iccl.ie/wp-content/uploads/2024/02/ICCL-and-DRI-FRT-submission.pdf; Liberty, Human Rights Coalition Calls for Immediate Ban on Facial Recognition, August 2021, https://www.libertyhumanrights.org.uk/issue/human-rights-coalition-calls-for-immediate-ban-on-facial-recognition/

9. We outline the rights engaged by policing FRT below. The level of impact on these rights would depend, like every individual use case of an FRT system by law enforcement, on many factors. These include the algorithm at the heart of the FRT system; the dataset it has been trained on; the purpose of the FRT use; who the technology is used against; and the consequences of its use. None of the following fundamental rights are absolute and it is acknowledged that states may interfere with fundamental rights in the pursuit of legitimate public interest objectives, provided the interferences are proportionate and are limited to what is necessary in a democratic society. A balance must be struck between ensuring that a state has effective and legitimate tools at its disposal in order to fulfill the functions of government, and the protection of fundamental rights and freedoms. But serious questions remain about the efficacy and legitimacy of FRT use by law enforcement. In the meantime, it should also be noted that when one considers the use of FRT by police, different jurisdictions respect and uphold the following rights differently and to differing degrees, with some jurisdictions not respecting them at all.

Right to dignity

10. A person's facial biometric data is permanently and irrevocably linked to their identity. The processing of biometric data under *all* circumstances constitutes a serious interference in itself with several rights, regardless of the outcome of the identification attempt (incorrect or correct).[28] This intrusiveness is one of the reasons a person's biometric data is given extra legal protection in certain jurisdictions.[29] This serious interference is linked with the right to dignity,[30] to be valued, respected, and to be treated ethically, and not as a commodity. Should a person feel they are under constant surveillance due to FRT, they may change their behavior in order to avoid locations, social scenarios or cultural events where FRT is deployed, thereby severely impacting their ability to live a dignified life.[31] As warned

[28] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted 26 April, 2023, p.5, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

[29] Article 4(14) of the EU General Data Protection Regulation defines 'biometric data' as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Under Article 9 GDPR the processing of biometric data is prohibited, save for certain circumstances. https://eur-lex.europa.eu/eli/reg/2016/679/oj. Also see Biometric Information Privacy Act, Illinois State Legislature, 2008,

[30] Article 1, Universal Declaration of Human Rights, "All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood., https://www.un.org/en/about-us/universal-declaration-of-human-rights

[31] European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, 2020, p.20,

by the European Data Protection Board, “Human dignity requires that individuals are not treated as mere objects. FRT calculates existential and highly personal characteristics, the facial features, into a machine-readable form with the purpose of using it as a human license plate or ID card, thereby objectifying the face.”[32]

Right to privacy

11. The right to privacy,[33] including a reasonable expectation of privacy while in public, is recognised as a ‘gateway’ right, given it enables the realization of other rights. Should a policing FRT system enable members of the public to be identified in public spaces, and their movements, interests and associations tracked, either in real-time or in retrospect, they are not only at risk of losing their privacy rights; they are also at risk of losing the associated rights built upon privacy. These include the right to protest, to freely associate with others, and to express one’s sexuality, religious belief and political affiliation. The manner in which FRT engages the right to privacy can be exacerbated when and if the FRT system is used live from a distance, or after an event in retrospect, without the person’s consent or knowledge. This is a point of critical importance when one considers the use of FRT by police as some uses of FRT could amount to covert or sustained mass surveillance.

Right to protection of personal data

12. Just because a person may be aware, or might not be surprised to discover that they have been photographed on camera or recorded by CCTV in a public space, this does not mean that they have agreed to make their biometric data public or consented to this data being extracted from an image, processed to create a biometric template, and stored/used for identification purposes by police in real-time or at some point in the future. Different jurisdictions have varied, and in some cases no, legal safeguards for the retrieval of biometric data, and the use, retention or destruction of the same. Depending on the use case of FRT, its interference with the right to

https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

[32] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted 26 April, 2023, p.15, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

[33] Article 17, International Covenant on Civil and Political Rights, “1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.” https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

protection of personal data[34] would be heightened considerably when a person is subjected to any manner of 'profiling' or form of automated processing whereby a person's biometric facial data is used to evaluate certain personal aspects relating to them or to analyze or try to predict aspects concerning that person's personal preferences, interests, reliability, behavior, location or movements.

Right to equality and non-discrimination

13. As stated above, FRT errors do not affect all individuals equally. The use of FRT by law enforcement poses an unquestionable risk in relation to the prohibition of discrimination, given the known problems with respect to performance over certain protected characteristics.[35] The technology disturbingly produces significantly higher false-match rates for people of color and women than for white people and men. Highly regarded testing shows that face recognition algorithms misidentify Black people, people of color, and women at higher rates. Widely reported testing from the federal agency in the US, the National Institute for Standards and Technology (NIST) testing in 2019 found FRT algorithms were up to 100 times more likely to misidentify Asian and African American people than white men, and that women and younger individuals were also subject to disparately high misidentification rates.[36] While some reports indicate that demographic differentials in false-match rates have lessened for some algorithms, testing by NIST and academic researchers indicates that the problem persists.[37]

[34] Article 8, Charter of Fundamental Rights of the European Union, "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[35] Birhane, A., 'The unseen black faces of algorithms' (2022) Nature, https://www.nature.com/articles/d41586-022-03050-7

[36] Grother P., et al., U.S. Department of Commerce, National Institute for Standards and Technology, Face Recognition Vendor Test Part 3:Demographic Effects 2–3, 8 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; See also Harwell, D., Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use, 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/.

[37] Grother, P., U.S. Department of Commerce, National Institute for Standards and Technology, Facial Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials 15, July 2022, https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf; see also Aman Bhatta et al., The Gender Gap in Face Recognition Accuracy Is a Hairy Problem, Procs of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2023,

Rights of people with disabilities

14. The UN Special Rapporteur on the rights of persons with disabilities has documented that some FRT algorithms have inherent biases against people with disabilities and especially people with conditions such as Down syndrome, achondroplasia, cleft lip or palate, or other conditions that result in facial differences, and that these issues have resulted in some people with disabilities being "judged untrustworthy" because their face did not conform to the standard programmed in the respective FRT system. The special rapporteur has called on states to consider imposing a moratorium on the sale and use of FRTs.[38]

Right to freedom of peaceful assembly and association

15. If a law enforcement officer or authority uses FRT, in a live or retrospective manner, to monitor or identify people attending a protest in a public space, the technology could potentially reveal the political leanings of individuals or their religious beliefs. Even if the police were on the look-out for specific individuals, whom they have detailed on a watchlist in a legal manner, some uses of FRT could result in every person attending the demonstration, the majority of whom could be of no interest to police, having their biometric data processed, and possibly stored, in real-time or in retrospect, without their knowledge or consent. Such a use of FRT could severely affect people's right to protest,[39] their reasonable expectation of being anonymous in a public space, and result in a chilling effect on citizens' ability to gather, freely

https://openaccess.thecvf.com/content/WACV2023W/DVPBA/papers/Bhatta_The_Gender_Gap_in_Face_Recognition_Accuracy_Is_a_Hairy_WACVW_2023_paper.pdf; K.S. Krishnapriya et al., Issues Related to Face Recognition Accuracy Varying Based on Race and Skin Tone, 1 IEEE Transactions on Tech. & Soc'y 8, 2020, https://ieeexplore.ieee.org/document/9001031; K.S. Krishnapriya et al., Characterizing the Variability in Face Recognition Accuracy Relative to Race, 2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition Workshops, April 2019, https://arxiv.org/abs/1904.07325; ACLU Comment re: Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Exec. Order 14074, Section 13(e)), January, 2024, https://www.aclu.org/documents/aclu-comment-facial-recognition-and-biometric-technologies-eo-14074-13e

[38] Report of the Special Rapporteur on the rights of persons with disabilities on Artificial Intelligence and the rights of persons with disabilities, December 2021, https://www.ohchr.org/en/calls-for-input/2021/report-special-rapporteur-rights-persons-disabilities-artificial-intelligence

[39] Article 20, Universal Declaration of Human Rights, "1. Everyone has the right to freedom of peaceful assembly and association. 2. No one may be compelled to belong to an association." https://www.un.org/en/about-us/universal-declaration-of-human-rights

exchange information, and engage in behavior that is necessary and vital for a healthy democracy.

Right to effective remedy

16. Given the “novel and untested”[40] nature of this technology as a law enforcement tool, and the varying level of knowledge amongst members of the public in different jurisdictions as to whether or not law enforcement is even using FRT, or in what manner and when, it is unclear what happens in most jurisdictions when an FRT system misidentifies an innocent person; when a person is wrongfully arrested and subjected to a decision based solely on automated processing and which produces an adverse legal effect on them; and what remedy is available to that person, or if they even have a means seek a remedy. There are several cases currently before the courts in the US.[41]

Right to presumption of innocence

17. The use of FRT by a law enforcement authority requires them to run a biometric template against a reference database of biometric templates. This process, by its nature, and as outlined in paragraph 3, effectively necessitates the generation of multiple false matches. What this means is that every person who is in a reference database, but who has nothing to do with a specific crime being investigated and for which a FRT search is carried out, is being subjected to a virtual line-up with potentially gravely dangerous consequences for their right to the presumption of innocence as has happened in the case of misidentifications, as outlined below. If a person’s biometric template is kept in a specific reference database routinely used or accessed by a law enforcement authority, such as a jurisdiction's driver’s license

[40] Gullo K., Electronic Frontier Foundation, Victory! New Jersey Court Rules Police Must Give Defendant the Facial Recognition Algorithms Used to Identify Him, June 7, 2023, https://www.eff.org/deeplinks/2023/06/victory-new-jersey-court-rules-police-must-give-defendant-facial-recognition

[41] ACLU and ACLU of NJ File Friend-of-the-Court Brief in Challenge to Wrongful Arrest due to Face Recognition Tech, January 2024, https://www.aclu.org/press-releases/aclu-and-aclu-of-nj-file-friend-of-the-court-brief-in-challenge-to-wrongful-arrest-due-to-face-recognition-tech; see also ACLU, Farmington Hills father sues Detroit Police Department for wrongful arrest based on faulty facial recognition technology, April 2021, https://www.aclumich.org/en/press-releases/farmington-hills-father-sues-detroit-police-department-wrongful-arrest-based-faulty; see also Ryan-Mosley, T., The new lawsuit that shows facial recognition is officially a civil rights issue, MIT, April 2021, https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/

database, each person in that database could be said to be trapped in a perpetual virtual line-up, even if they have no link to crime whatsoever.[42]

Law enforcement use of FRT is resulting in racial discrimination and putting innocent people at risk of being wrongfully convicted

18. The real-life racial discriminatory impact of the aforementioned biases in FRT is devastating. In the US alone, there are, at the time of writing, six known cases of law enforcement wrongfully arresting and incarcerating Black people on the basis of the police using error-prone FRT.[43] It is unknown how many people wrongfully arrested and incarcerated may have taken plea deals in the U.S.[44] The six known cases are:

    a. **Robert Williams:** In 2020, Mr Williams was handcuffed and arrested, in front of his wife and two daughters, by Detroit police officers after FRT wrongfully identified him on suspicion of stealing watches from a Detroit watch shop. Mr Williams was detained for nearly 30 hours before he was released. Mr Williams is the first *known* case of someone being wrongfully arrested in the United States due to a false face recognition 'match'.[45]

    b. **Michael Oliver:** In 2019, Mr Oliver was driving to work in Michigan when a police officer pulled him over and told him there was a felony warrant out for his arrest. He was subsequently detained and charged with larceny. A judge later dismissed the case, in part because an image of the actual suspect had no face or arm tattoos, unlike Mr Oliver. Almost a year later, Mr Oliver learned his wrongful arrest was based on an erroneous match using FRT.[46]

    c. **Njeer Parks:** In 2019, Mr Parks was accused of shoplifting and trying to hit a police officer with a car in New Jersey. The police wrongfully identified him

[42] Garvey, C., The Perpetual Line-Up, Unregulated Police Face Recognition in America, Georgetown Law: Center on Privacy and Technology, October 2016, https://www.perpetuallineup.org/

[43] American Civil Liberties Union, ACLU calls on Detroit Police Department to end use of faulty facial recognition technology following yet another wrongful arrest, August 2023, https://www.aclumich.org/en/press-releases/aclu-calls-detroit-police-department-end-use-faulty-facial-recognition-technology

[44] Press, E, New Yorker, Does A.I. Lead Police to Ignore Contradictory Evidence?: Too often, a facial-recognition search represents virtually the entirety of a police investigation, November 13, 2023, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence

[45] Williams, R., I Did Nothing Wrong. I Was Arrested Anyway, American Civil Liberties Union, July 15, 2021, https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway

[46] Stokes, E., Wrongful arrest exposes racial bias in facial recognition technology, November 2020, https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/

using FRT, even though he was 30 miles away at the time of the incident. Mr Parks was subsequently detained for 10 days in jail, allegedly notwithstanding that his fingerprints and DNA did not match those left at the crime scene and that he provided an alibi at the time of his detention.[47]

d. **Randal Reid:** Mr Reid was wrongfully arrested and held for nearly a week in jail after FRT misidentified him for a suspect who was wanted for using stolen credit cards to buy approximately $15,000 worth of designer purses in Louisiana, a state he had never even visited. Mr Reid was eventually released after his lawyers sent multiple pictures of him to the police, outlining they had the wrong person.[48]

e. **Alonzo Sawyer:** Mr Sawyer was arrested and detained for assaulting a bus driver and stealing his phone near Baltimore in Maryland, after police use of FRT wrongfully labeled him as a possible match with the suspect in CCTV footage. Mr Sawyer was eventually released after nine days in jail.[49]

f. **Porcha Woodruff:** In 2023, Ms Woodruff was eight months' pregnant when six Detroit police officers arrived on her doorstep and arrested her, in front of her two daughters as they prepared to go to school, for carjacking. The police had used FRT which wrongfully identified Ms Woodruff. The true suspect was not pregnant. Ms Woodruff was detained for 11 hours and suffered early contractions from the incident.[50]

19. In addition to the above cases in the US, in December 2023, the US Federal Trade Commission banned pharmacy retail chain Rite Aid from using FRT for surveillance purposes for five years after finding that, from 2012 to 2020, Rite Aid used FRT to identify customers who may have been engaged in shoplifting or other problematic behavior but failed to take reasonable measures to prevent harm to consumers, who, as a result, were erroneously accused by employees of wrongdoing because FRT wrongfully flagged the consumers as matching someone who had previously been

[47] Bryan, K., et al, Government Users of Facial Recognition Software Sued by Plaintiff Alleging Wrongful Imprisonment Over Case of Mistaken Identity, The National Law Review, January, 2021, https://www.natlawreview.com/article/government-users-facial-recognition-software-sued-plaintiff-alleging-wrongful

[48] Hill, K., and Mac, R., Thousands of Dollars for Something I Didn't Do, The New York Times, April 2023, https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html

[49] Johnson, K., Face Recognition Software Led to His Arrest. It Was Dead Wrong, Wired, February 2023, https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/

[50] Hill, K., Eight months pregnant and arrested after false facial recognition match, The New York Times, August 6, 2023, https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html

identified as a shoplifter. The FTC found Rite Aid's use of FRT led to thousands of false-positive 'matches', with their actions disproportionately impacting people of color. It found Rite Aid's FRT was more likely to generate false positives in stores located in plurality-Black and Asian communities than in plurality-White communities.[51]

20. In Toronto, a Black woman from Africa, years after making a successful refugee claim in Canada, had her refugee status wrongfully revoked due to an FRT misidentification. After she walked into the licensing office of the Ontario Ministry of Transportation (MTO) to have her photograph taken for her driver's license and the ministry's FRT's system mismatched her to some other woman in its database and the MTO passed this information to Immigration, Refugee and Citizenship Canada (IRCC).[52]

21. In Argentina, Guillermo Ibarrola was also misidentified by an FRT system and wrongfully arrested, detained and accused of carrying out an armed robbery in a city he had never previously visited, some 600 kilometers from his home city in Buenos Aires.[53]

22. These are just a snapshot of the documented cases and it is safe to argue, due to the extensive and increasing use of FRT (including by authoritarian regimes) and the well-documented problems of these discriminatory systems, that the documented cases are likely to be a small subset of all the cases of unacceptable and irreparable impacts on human rights.

Datasets and training data

23. INCLO member organization the American Civil Liberties Union (ACLU) has comprehensively explained[54] how, while early coverage of racial and gender

[51] US Federal Trade Commission, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards, December 2023, https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without

[52] Christian, G., AI FRT: the black box hurting Black people, Toronto Star, August 2023, https://www.thestar.com/opinion/contributors/ai-facial-recognition-technology-the-black-box-hurting-black-people/article_67c4a8e6-e377-55c6-9e63-2bd209e99dc3.html

[53] Naundorf, K, The Twisted Eye in the Sky Over Buenos Aires, Wired, September 13, 2023, https://www.wired.com/story/buenos-aires-facial-recognition-scandal/

[54] ACLU Comment re: Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Exec. Order 14074, Section 13(e)), January, 2024,

disparities in FRT false-match rates focused on the lack of equal representation by race and gender in photo datasets used to train the algorithms,[55] it has become clear that ensuring more diverse representation in training datasets will *not* eliminate the problem of demographic disparities in false-match rates. While other factors may also be at play, this is partly because the color-contrast settings in digital cameras disproportionately result in underexposed images of darker-skinned people,[56] which reduces FRT accuracy when attempting to process and match those images.[57]

FRT compounds pre-existing racial disparities in policing

24. The use of FRT compounds pre-existing racial disparities in policing in other ways. Research shows that law enforcement use of FRT in the U.S. "contributes to greater racial disparity in arrests," with an increase in Black arrest rates and decrease in white arrest rates. This may be partly a result of cognitive biases of officers who decide when to run FRT searches and how heavily to rely on FRT results, and on racial disparities in the makeup of photograph databases used to attempt to generate matches, including arrest photographs (i.e ., "mugshot") databases that reflect long-standing over-policing of people of color in the U.S.

25. In the U.S. jurisdictions that are required to track demographic information related to FRT searches, data shows disproportionate use on people of color. In New Orleans, for example, "nearly every use of the technology from October 2022 to August 2023 was on a Black person."[58] In Detroit, all 129 FRT searches in 2020 were conducted on images of Black people.[59] In light of these dynamics, it is unsurprising that every known case of a wrongful arrest in the U.S. due to police reliance on an incorrect FRT result has involved the arrest of a Black person. Concerns about FRT

https://www.aclu.org/documents/aclu-comment-facial-recognition-and-biometric-technologies-eo-14074-13e

[55] Grother P., et al., U.S. Dep't of Com., Nat'l Inst. for Standards & Tech., Face Recognition Vendor Test Part 3: Demographic Effects 71 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[56] See Lewis, S., The Racial Bias Built into Photography, N.Y. Times (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html

[57] See Haiyu Wu et al., Face Recognition Accuracy Across Demographics: Shining a Light into the Problem, arXiv No. 2206.01881 (Apr. 16, 2023), https://arxiv.org/abs/2206.01881

[58] Alfred Ng, 'Wholly Ineffective and Pretty Obviously Racist': Inside New Orleans' Struggle with Facial-Recognition Policing, Politico (Oct 31, 2023), https://www.politico.com/news/2023/10/31/new-orleans-police-facial-recognition-00121427

[59] Detroit Police Department, Annual Report on Facial Recognition, 2020 (Jan. 27, 2021), https://detroitmi.gov/sites/detroitmi.localhost/files/2021-02/Facial%20Recognition%202020%20Annual%20Report.pdf

exacerbating existing racism in policing has motivated many of the bans on police use of the technology at the U.S. state and local level.[60]

Discriminatory FRT is being used by law enforcement without safeguards

26. INCLO members oppose the use of FRT by law enforcement due to the fundamental rights risks involved. Should a jurisdiction create a legal basis for a law enforcement authority to use FRT, it must include, at a minimum, a significant number of robust safeguards enshrined in law, a number of which we include here. To prevent racial discrimination specifically these safeguards must include, but not be limited to, a non-delegable duty on the part of the law enforcement authority to carry out a series of impact assessments with respect to all fundamental rights prior to any deployment of any new use case of FRT. These assessments must include, but not be limited to, an assessment of the impact on fundamental rights and an assessment of the strict necessity and proportionality of the FRT use.

27. The former must identify, assess and address the adverse effects of an FRT deployment on human rights. This assessment must explicitly outline:
    - The specific parameters of its use, including who it will be used against, what type of FRT use will be used, where it will be used, why it will be used, and how it will be used;
    - The rights impacted, in particular rights to privacy, protection of personal data, freedom of expression and peaceful assembly and non-discrimination;
    - The nature and extent of the risks to those rights;
    - How each of those risks will be mitigated;
    - A demonstrated justification for how and why the benefits of the FRT deployment would outweigh the rights' impacts; and
    - The remedy available to someone who is either misidentified or whose biometric data was processed when it should not have been processed.

28. Any assessment of the strict necessity and proportionality of the FRT use must detail the necessity of the deployment for a stated and legitimate objective and include:

[60] See, e.g., King County, Wash., Ordinance No. 19296, Statement of Facts ¶¶ 2–3 (2021) ("The council finds that the propensity for surveillance technology, specifically facial recognition technology, to endanger civil rights and liberties substantially outweighs the purported benefits, and that such technology will exacerbate racial injustice…Bias, accuracy issues and stereotypes built into facial recognition technology pose a threat to the residents of King County."); Minneapolis, Minn., Code of Ordinances art II, §41.10(c) ("Facial recognition technology has been shown to be less accurate in identifying people of color and women. Facial recognition technology has the potential to further harm already disadvantaged communities through incorrect identifications.").

- Evidence as to the problem being addressed by the FRT deployment;
- An evidence-based explanation as to how the FRT deployment would be genuinely effective in addressing the problem; and
- A demonstration of why existing and less intrusive measures, which do not include FRT, would not be sufficient to meet the legitimate objective.

29. An authority must not deploy any new use case of FRT if an impact assessment determines that the FRT system, and the demographic composition of the system's algorithm training dataset, results in biases prohibited by international human rights law, directly or indirectly, against any protected characteristic including race, gender or age, in an operational setting. Additionally, a law enforcement authority must not deploy any new use case of FRT if it is neither strictly necessary nor proportionate.

30. As FRT algorithms are created and developed by private companies; they are often not generally open to independent audits or risk assessments, despite the inherent risks to people's fundamental rights. It is unclear what, if any, steps are taken by law enforcement authorities to independently audit the veracity of the vendor's claims about the FRT system/respective algorithm. Often, proprietary interests prevent police from obtaining information about how an algorithm works, and the risks it poses. It is also often the case that there is no legal mechanism to oblige vendors to publish or disclose certain information about their algorithms. This essentially amounts to citizens and residents being forced to simply tolerate discriminatory policing methods. This is unacceptable.

31. A court case in the UK (*Ed Bridges v South Wales Police* – the world's first legal challenge against police use of FRT) revealed that the police did not satisfy themselves that the technology they were using was not discriminatory, as they were obliged to do by law under a public sector equality duty (a legislative obligation for government bodies to respect the human rights of their staff and service users and combat discrimination).[61] The *Bridges* ruling also noted that the lack of access to private company data regarding the possible discriminatory impact of the FRT the police were using, "for reasons of commercial confidentiality", was *not* a sufficient reason for the South Wales Police to discharge themselves of the duty to

[61] *R (Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058, par.201 https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

ensure the tool was not discriminatory.[62]

32. The UK Court of Appeal held that, even if companies are opaque and do not share certain data, the police must either not use the technology or carry out their own investigation into the technology's discriminatory impacts. Following this decision, the South Wales Police have investigated FRT on its own and released a study claiming that it is not discriminatory. However, the study was not independent, it was not tested in operational settings, and the images used to test the algorithm were different to the typical images used by the police applying FRT.[63] In other words, the police's own assessment did not reflect the police force's actual use of this invasive and intrusive technology.[64]

33. The *Ed Bridges* case was also significant as it found that the South Wales Police use of FRT breached privacy rights, data protection laws, and equality laws. It held that the police were given too much discretion in regards to who would be selected to be placed on a watch list,[65] and where the live FRT would be deployed.[66] It found the policies on the use did not sufficiently set out the terms on which the discretionary powers could be exercised. As such, the Court of Appeal held that the policies did not have the necessary quality of law. Given the court ruled on the legality of the measure, and found it wanting, it did not need to address the other principles of necessity and proportionality.[67]

34. Similarly, the Court of Appeal in Buenos Aires, in finding that the city's FRT system was unconstitutional, held that the implementation of the system in the city had to be preceded by, among other things, robust studies to establish if the use of the system was discriminatory by having a differential impact based on people' personal

[62] *R (Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058, par.199 https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf; see also Sabbagh, D., South Wales police lose landmark facial recognition case, The Guardian, August 2020, https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case

[63] Science and Technology in Policing, Operational Testing of Facial Recognition Technology, April 2023, https://science.police.uk/delivery/resources/operational-testing-of-facial-recognition-technology/

[64] Irish Council for Civil Liberties, Leading experts warn against Garda use of FRT, October 2023, https://www.iccl.ie/digital-data/leading-facial-recognition-technology-experts-have-warned-against-garda-use-of-frt-saying-use-of-the-toxic-tool-would-result-in-a-massive-step-change-in-police-sur/

[65] *R (Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058, par.124, https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf

[66] Ibid, par. 130

[67] *R (Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058, https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf

characteristics (such as gender or skin color). The court held that this was necessary in order to determine whether the system deployed violated the right to equality and non-discrimination and, therefore, constitutional or not.[68]

35. Law enforcement authorities must fulfill their assessment obligations above to carry out fundamental rights impact assessments, regardless of any absence of a legal mechanism to oblige FRT system vendors to publish or disclose certain information about their algorithms and source data.

36. Having such a powerful, yet flawed, tool such as FRT in the hands of police who are untrained as to how to use it and understand it; and the absence of any independent oversight and assessment of that use could only serve to further entrench and expand the issues with police use FRT, including issues around the right to protection of personal data. It has been reported that, while the US Federal Bureau of Investigation (FBI) has carried out tens of thousands of FRT searches over recent years, just 5% of its 200 agents who use the technology have taken the bureau's own course on how to use it.[69] It's unclear what training takes place in other jurisdictions where FRT is used by police. In respect of oversight, in the UK there is a Biometrics Surveillance Camera Commissioner, however changes to the Commissioner's role and regime, including the forthcoming abolition of the Surveillance Code of Practice, has to concerns that there will be "vulnerabilities for users of technologies and for the rights of individuals subject to them"[70] and, in the absence of a clear plan for how the Commissioner's functions will be replaced, risks there being more rather than less regulatory complexity.[71] In the US there have been calls for a regulatory office to oversee the management and regulation of complex technologies such as FRT, similar to how the pharmaceutical industry is regulated[72] and, similarly, an

[68] Cámara de Apelaciones en lo Contencioso Administrativo y Tributario de la Ciudad de Bs. As., Sala I; Case: "OBSERVATORIO DE DERECHO INFORMATICO ARGENTINO O.D.I.A. Y OTROS CONTRA GCBA SOBRE AMPARO - OTROS"; N° EXP 182908/2020-0 (April 28th, 2023)); see also CELS, The Court of Appeals of the City of Buenos Aires confirmed the unconstitutionality of the use of the fugitive facial recognition system (SRFP) implemented by the Buenos Aires city government, April 2023, https://www.cels.org.ar/web/en/2023/04/the-court-of-appeals-of-the-city-of-buenos-aires-confirmed-the-unconstitutionality-of-the-use-of-the-fugitive-facial-recognition-system-srfp-implemented-by-the-buenos-aires-city-government/

[69] FBI Agents Are Using Face Recognition Without Proper Training, Wired, September 2023, https://www.wired.com/story/fbi-agents-face-recognition-without-proper-training/

[70] Fussey, P., and Webster, W., Independent report on changes to the functions of the Biometrics and Surveillance Camera Commissioner arising from the Data Protection and Digital Information (No.2) Bill, Centre for Research Into Information, Surveillance and Privacy, p.6, October 2023, https://assets.publishing.service.gov.uk/media/653f7128e6c968000daa9cae/Changes_to_the_functions_of_the_BSCC.pdf

[71] Ibid, p.7

[72] Facial Recognition Technologies in the Wild: A Call for A Federal Office, Erik Learned-Miller, Vicente Ordóñez, Jamie Morgenstern, and Joy Buolamwini May 29, 2020,

independent body charged with certifying policing technologies before they are deployed.[73] In Canada, the Office of the Privacy Commissioner of Canada has issued regulatory guidance on police use of FRT, but this guidance is not legally enforceable.[74] Similarly, the Office of the Australian Information Commissioner (OAIC) is the main regulatory body with privacy-related jurisdiction at Federal level in Australia. Each State and Territory also has its own body responsible for privacy regulation. The OAIC has the power to conduct investigations into acts or practices that may breach the Privacy Act and to conduct privacy assessments to determine whether entities are maintaining and handling personal information in accordance with the Privacy Act. But the OAIC has moderate efficacy in upholding the rights engaged by FRT.

37. Should a law enforcement authority be permitted, by law, to use FRT, they must uphold the principles of transparency and accountability to safeguard people's right to protection of personal data.

38. An obvious transparency issue concerning FRT is the secret or opaque nature of how the algorithms underpinning a specifically used FRT system work, and how, in the main, members of the public and, more egregiously, the very communities disproportionately affected by the error-prone tech, are not consulted in a transparent manner about the tech, how it works, how it impacts the criminal justice system and people's lives and fundamental rights.

39. Another significant transparency issue is around members of the public simply not knowing that FRT is being used against them, in either a live or retrospective setting. For example, in the UK, when live FRT is being used the police are supposed to alert the public to their use. However, this often happens via Twitter[75] which is not a sufficient way of alerting the public considering many people are not on Twitter and those who are may not have seen the respective tweet. The police are also supposed to mark out the physical area where live FRT is being used so the public can avoid the area should they not wish for the biometric data to be processed. However, signs

https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf

[73] Friedman, Barry and Heydari, Farhang and Isaacs, Max and Kinsey, Katie, Policing Police Tech: A Soft Law Solution (June 1, 2022). Berkeley Technology Law Journal, Vol. 37, 2022, Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4095484

[74] Privacy regulators call for legal framework limiting police use of facial recognition technology, Office of the Privacy Commissioner in Canada, May 2022, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220502/

[75] See Metropolitan Police https://twitter.com/metpoliceuk/status/1226918678014431233?t=W_ejR-0D-qc4jW32I-QNFg&s=19

are usually placed too close to the area that it is often too late, or too cumbersome, to avoid the area. The issue of the public not knowing FRT is being used against them is hugely significant when FRT is used retrospectively and covertly, as it is near impossible for a person to know they have been involved in an FRT search.

40. A further transparency and accountability issue strongly emerging in the US is FRT being used in investigations leading to people's arrest and when they find themselves before the courts, their defense teams are denied access to any information about how that system worked, its propensity for error or bias, or even the name of the system itself.[76]

41. To help ensure some of the fundamental data protection principles - transparency and accountability - are upheld, an independent FRT oversight body must be established before any deployment of FRT by a law enforcement authority to assess the use of FRT and its compliance, or otherwise, with fundamental rights; and the applicable regulation. This body must:
    - Be established and regulated by law;
    - Be separate to the executive authority or respective government;
    - Have the necessary funds, skills, expertise, staff, legal and technological, to fulfill their responsibilities;
    - Have free and immediate access to the necessary information it needs to carry out its work;
    - Report annually to the public about its work and findings; and
    - Report annually to the respective parliament.

42. This independent FRT oversight body must publish annual reports which would include, but not be limited to, all of the written assessments mentioned in this submission, and:
    - A detailed assessment of, and comment on, the law enforcement's stated legal basis for the use of FRT;
    - Number of individual probe images used in FRT searches;
    - Number of images used in databases against which searches have been conducted;
    - Number of true positives and false positives per deployment;
    - Number of arrests per deployment;

[76] New Jersey Appellate Division One of First Courts in Country to Rule on Constitutional Rights Related to Facial Recognition Technologies, ACLU, June 2023, https://www.aclu-nj.org/en/press-releases/new-jersey-appellate-division-one-first-courts-country-rule-constitutional-rights

- The total number of FRT search requests made;
- The total number of FRT searches performed;
- The number of requests made or searches performed pursuant to judicial authorisation;
- The number of emergency requests made or searches performed;
- The reasons for requesting the search, including, but not limited to, any underlying suspected crime.

43. Law enforcement authorities must also use the tools available to them to make public details of how probe images are used in an FRT operation in a clear, intelligible and understandable manner, online and offline and in such a way that are accessible to everyone. These details must identify, but will not be limited to:
    - The criteria necessary for a person's image to become a probe image;
    - The source of the probe image;
    - The length of time such probe images are retained before they are destroyed;
    - The legal basis for obtaining, retaining and processing the probe image; and
    - The contact details for an independent oversight body appointed to safeguard the fundamental rights of people whose images are used in a FRT search.

44. Before any deployment of FRT, the law enforcement authority must make public details of the technical specifications of any FRT system it is using in a clear, intelligible and understandable manner. These details must include, but will not be limited to:
    - The name and manufacturer of each FRT software used, each algorithm version number and each year they were developed;
    - The source code for each algorithm used;
    - A list of what measurements, nodal points, or other unique identifying marks are used by the system in creating facial feature vectors including, if those marks are weighted differently, the scores given to each respective mark;
    - The error rates for the FRT system used, including false positive and false negative rates, as well as documentation as to how the error rates were calculated, including whether they reflect test (laboratory) or operational conditions reflecting the demographic make-up of where the FRT use is being deployed;
    - A list of the parameters of the reference database used, including:
        1. How many images are in the database;
        2. How are the images obtained;
        3. How long the images are stored;
        4. How often the database is purged;

5. What the process is for getting photographs removed from the database;
6. Who has access to the database;
7. How the database is maintained;
8. The identity of the person/unit who is responsible for the maintenance and oversight of the database; and
9. The privacy and data protection policy for the database.

45. A police officer must not be permitted to conduct an FRT search unless:

- There is prior judicial authorisation for such use, except in duly justified urgent cases, whereby a higher-ranking officer must give approval. In such exceptional cases, the judicial authorization must still be requested without undue delay and no later than 48 hours after the search;
- The police officer conducting the FRT search is independent of the investigation of the offense; and
- The police officer conducting the FRT search has completed training, which will be updated annually, on how to use the relevant system, on the human rights impacts of the system, and how to determine whether there is an appropriate legal basis for the FRT search.

46. Law enforcement authorities must document each FRT search performed and provide this documentation to the independent oversight body every quarter. This documentation must include:

- A copy of any written request made for an FRT search, which must include:
    - The date and time of the request;
    - The name and position of the requesting individual officer and the police unit they are attached to;
    - Details of how the request was necessary and proportionate;
    - The reason for the request, including, but not limited to, any underlying suspected crime;
    - The judicial authoriser to whom the request was made and, in exceptionally urgent circumstances, the higher-ranking officer who gave the temporary authorization;
    - The outcome of the request;
    - If the request was granted, the composition/make-up of the database searched;
- The name and position of the individual officer who carried out the search;
- Information provided to the oversight body will also include aggregate information on the use of FRT, including:
    - The total number of FRT search requests;

    - The total number of FRT search requests that generated leads;
    - The number of FRT searches whereby an arrest or charges followed;
    - The number of FRT misidentifications* which preceded an action taken against those persons;
    - The number of individuals who appeared as a possible match in the FRT search and who were subsequently questioned, arrested and/or charged;
    - The demographic breakdown of individuals in probe photos by race and sex; and
    - Information about the FRT system and algorithm(s) used, including vendor, version, similarity threshold and if the similarity threshold was adjusted for the specific search.
- In addition to the above, every database of images used by a law enforcement authority for an FRT search must be audited at least annually to ensure that it does not contain images that are no longer legally permitted to be retained; that it does not contain wrong information; and that it is not being accessed or used inappropriately or unlawfully. These audits must also be provided to the oversight body.

Any other information requested by the oversight body to fulfil their legal obligations must also be provided by the law enforcement authority in a reasonable time.

47. Law enforcement authorities must disclose to persons detained, questioned, arrested, charged, or prosecuted subsequent to an FRT search, and their legal representative (if any), without restriction, details of the FRT operation applied to them and the technical specifications of the system involved in the investigation or procedure applied. These must include all of the details listed at paragraph 45 and:
    - The original copy of the probe image used;
    - Any/all information associated with the probe image, including metadata, that was in the possession of, or made available to, the person conducting the FRT search;
    - Details of the FRT system's threshold value fixed by the manufacturer, and/or by law enforcement authority if they changed the value, to determine when the respective software indicates that a potential match has occurred;
    - Any or all edited copies of the probe image used, noting if applicable, which edited copy produced the candidate list that the defendant was in, and a list of edits, filters, or any other modifications made to that image;

- A copy of the database image matched to the probe image and the rank number and similarity score assigned to the image by the FRT system in the candidate list;
- A list or description of the rank number and similarity scores produced by the FRT system, including the scale on which the system is based;
- A copy of the complete candidate list returned by the FRT system, in rank order and including the similarity score assigned to each image by the FRT system;
- The written report produced by the person who ran the FRT search, including the date, time of the search, and any notes made about the possible match relative to any other individuals on the candidate list; and
- The name and training, certifications, or qualifications of the person who ran the probe image in an FRT search.

Obligations of private actors and corporations

48. Private actors and corporations are both users and vendors or suppliers of these technologies. As users, their use of FRT raises the same human rights risks outlined in this submission and, therefore, must be obliged to comply with the same safeguards and within the same limitations.

49. As vendors, companies tend to present their systems packed into "global solutions" and are presented as "what is needed" without a clear explanation about how such a solution works and why the solution must be acquired as a whole. These practices can lead to a user or buyer becoming dependent on a vendor. For that reason, in addition to the assessments and measures outlined under Question 4 and 5, law enforcement authorities must not acquire or deploy any new FRT without a prior assessment of vendor lock-in risk, including, but not limited to:
    - An evaluation of the interoperability and compatibility with current existing systems;
    - A data ownership and portability assessment, evaluating the costs of migrating the data to a different vendor's system;
    - A comparison of the proprietary systems, components and algorithms with the existing open alternatives, should there be any; and
    - A strategy to change vendors if needed, including the foreseeable costs of such a change.

    The procurement of FRT systems should favor vendor offers that maximize open standards and interoperability and minimize proprietary components, while a duty must be placed on vendors to explain, in plain language, how a specific FRT system works, and a duty on law enforcement authorities to fully understand how the technology and the system work.

Lessons learned, both positive and negative

50. As stated above, attempts to ensure more diverse representation in training datasets will *not* eliminate the problem of racial and gender disparities in FRT false-match rates. As also stated above, this is just one of many reasons why FRT should not be used by law enforcement authorities.

Lack of redress mechanisms

51. In this submission, we have outlined the grave human rights risks and real-life impacts associated with the use of FRT by law enforcement, and how the impacts are just starting to emerge. As individuals in jurisdictions across the world are only just beginning to attempt to obtain redress for the harms caused to them via litigation, it is too soon to say what, if any, effective redress mechanisms exist for those negatively impacted by the use of this defective, deeply discriminatory but powerful technology. It is for this reason that we believe law enforcement authorities should not be deploying FRT at all and instead, follow the road of more than 20 jurisdictions in the U.S. —including Boston; Minneapolis; Pittsburgh; Jackson, Mississippi; San Francisco; King County, Washington; and the State of Vermont — who have passed legislation halting most or all law enforcement or government use of FRT.[77]

Public consultation

52. Before any law enforcement authority use of FRT, the authority must hold meaningful public consultations with members of the public; including members of the communities who will be disproportionately affected by the FRT use. This consultation must include the sharing of:
    - Details about how the technology and system works in an explainable and accessible manner;

[77] ACLU Comment re: Request for Comment on Law Enforcement Agencies' Use of Facial Recognition Technology, Other Technologies Using Biometric Information, and Predictive Algorithms (Exec. Order 14074, Section 13(e)), January, 2024, https://www.aclu.org/documents/aclu-comment-facial-recognition-and-biometric-technologies-eo-14074-13e

- Details about the parameters of the authorities’ expected use within the respective jurisdiction including the strict conditions under which the system is used;
- Details of the images used as probe images and any databases, when applicable;
- Demographic data of those who are expected to be subjected to the use of the system;
- All written impact assessments mentioned in this submission; and
- Details of the safeguards in place to prevent arbitrary use of the system.

Other relevant information

53. As stated above, INCLO members believe the twin dangers of highly consequential misidentifications and pervasive surveillance mean law enforcement authorities should not be deploying FRT at all. In jurisdictions where law enforcement authorities do use it, FRT must never be used on live or recorded moving images or video data, or to:
    - Identify whistleblowers, journalists or journalistic sources;
    - Identify people who have no evidentiary link, direct or indirect, to a crime;
    - Categorize people by a protected characteristic or for social scoring;
    - Infer the emotions or intentions of a person;
    - Try to predict the future actions of a person;
    - Identify protesters or to collect information on people attending peaceful assemblies; and
    - Identify people in or around polling stations.