Recommendations and Suggestions on the NITI Aayog Discussion Paper titled 'Responsible AI for All: Adopting the Framework- A Use Case Approach on Facial Recognition Technology'

(December 2022)

Prepared by the Study Group on Artificial Intelligence and Facial Recognition Technology (FRT), Centre for the Study of Law and Governance, Jawaharlal Nehru University, New Delhi

Study Group participants:

1. Anuradha Singh
2. Deepa Kansra
3. Jaivir Singh
4. Madhavi Shukla
5. Nupur Chowdhury
6. P. Puneeth
7. Prabhat Mishra, *convenor* (exalt@jnu.ac.in / prabhat0104@gmail.com)

We sincerely appreciate the efforts of NITI Aayog to formulate policy frameworks and seek public feedback on specific use cases of artificial intelligence, as reflected in the discussion paper titled 'Responsible AI for All: Adopting the Framework- A Use Case Approach on Facial Recognition Technology'. In this document, we propose a set of recommendations on the development and deployment of FRT systems in India. Our recommendations are listed below, followed by a brief discussion on the same in the subsequent section.

I. RECOMMENDATIONS:

1. A statutory framework to authorise the development and deployment of FRT systems for whatsoever purposes be put in place.
2. A nation-wide moratorium on usage of FRT for all purposes be declared till a statutory framework is in place.
3. A nation-wide moratorium on law enforcement uses of FRT systems till they are advanced enough to exhibit 100 percent accuracy.
4. New categorisation for the use of FRT systems needed.
5. Access to public goods and services shall not be denied based solely on automated data processing by FRT systems.
6. Risks related to design, development, testing, deployment, procurement, and use of FRT technology need to be individually and collectively addressed.
7. Need to adequately define the term *'constitutional morality'* and its linkage with the Responsible Artificial Intelligence (RAI) principles.
8. Application of the four-pronged test laid down by the majority in *K. S. Puttaswamy* as the threshold criteria for examining rights-based challenges to FRT.
9. Consent-based regulatory framework is inadequate and requires rethinking.
10. Measures to protect individuals' rights under the proposed DPDP Bill are inadequate, especially with regard to FRT.
11. Limitations on data collection and clear prohibition of repurposing of data without free, prior, informed consent.
12. Establishment of an effective grievance redressal mechanism.
13. Clear provisions for imposing penalties/sanctions for breaches and compensation for the persons aggrieved.
14. Fair and comprehensive assessment of FRT to determine whether it can be used in a manner that is consistent with human dignity.
15. Prohibition on the use of junk science to justify the development and deployment of FRT.

16. National standards need to be developed to ensure the quality and efficacy of FRT systems.
17. Auditing as a regulatory principle governing the use of FRT requires better enunciation.
18. Development and deployment of FRT systems should be in conformity with international Human Rights principles.

II. DISCUSSION:

1. *A statutory framework to authorise the development and deployment of FRT systems for whatsoever purposes be put in place.*

   FRT as a technology has various benefits and risks associated with it. Although, it is supposed to be widely applicable to various social contexts to authenticate the identity of individuals, it is also riddled with serious pitfalls and risks, as pointed out in the discussion paper. Presently, there is no law authorising the use of FRT in India and a national data protection legislation is only being envisaged by our legislature currently, we propose that no use of FRT be made for whatsoever purposes. Without legal authorisation, FRT-like privacy-intrusive technologies can throw serious challenges which would then be difficult to mitigate retrospectively. In this regard, **we suggest that every use-case of FRT shall be legally authorised. Therefore, a separate legislation for FRT is needed, emphasising the lawful usage of FRT with adequate safeguards**. The regulations governing FRT should clearly reflect the fact that there are inherent inaccuracies in FRT outcomes. Robust regulatory frameworks should be established to approve specific use cases of FRT, encompassing all kinds of FRT systems.

2. *A nation-wide moratorium on usage of FRT for all purposes be declared till a statutory framework is in place.*

   It draws from the first recommendation above that **the use of FRT in the absence of legal and regulatory frameworks is not to be allowed**. As the discussion paper points out, there are grave risks associated with the unregulated use of FRT which may cause irreparable damage to individuals and groups, more so the marginalised sections of society. Until such time that the contours of lawful use of FRT are defined through statutory means, a nation-wide moratorium shall be declared on the use of FRT.

3. *A nation-wide moratorium on law enforcement uses of FRT systems till they are advanced enough to exhibit 100 percent accuracy.*

   Whenever laws on FRT are made, specific provisions regarding **a time-based moratorium to be declared** on use of FRT for predictive policing should be included. Similar conditions for other 'security related uses' like mass-monitoring, surveillance and any other law-enforcement purposes like identification of suspects/accused.

4. *New categorisation for the use of FRT systems.*

   The broad categorisation of FRT usage into security and non-security categories is inaccurate. In our view, the **c**riterion of categorisation should be determined by the nature of injury and liability. As different FRT systems would have different natures of injury and harm, permissibility standards should also differ accordingly.

   We suggest the following categories instead:

   i) Commercial Use (Public or Private, uses involving data sharing with private entities, PPPs etc.),
   ii) Public Service Delivery Use (PDS, taxation, other government services, etc.), and
   iii) Law Enforcement Use (policing etc.)

   Categorisation of FRT systems based on their use is important because the categorisation of FRT into only security and non-security uses does not adequately highlight the use of FRT for purely commercial uses/purposes, while also conflating the binary of public and private entities. It is especially crucial in the light of ever expanding uses of FRT for commercial purposes such as targeted delivery, improving customer experiences and so on to name a few. The categorisation suggested here would better enable fixing proportional legal liabilities and setting varied degrees of permissibility standards and regulatory measures.

   A distinction between different kinds of FRT systems in various other jurisdictions as well. The European Union, UK, USA, Canada and many other countries either have

different legislations pertaining to commercial and law enforcement purposes or more nuanced and clearly defined categories of FRT in their respective legislations.

For example, the EU member countries are governed by the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) which clearly distinguishes between security and commercial uses while also fostering a comprehensive privacy and data protection framework. The EU is also contemplating a proposal for harmonising rules on artificial intelligence.

Post-Brexit, the European data privacy framework does not apply in the UK, however, the Data Protection Act, 2018 regulates personal data while also regulating data uses for organisations, businesses and the government differently.

USA, being a federal republic, is governed by regulations at state, local and federal levels while also demanding a federal level legislation for FRT uses. The State of Illinois' Biometric Information Privacy Act (BIPA), Washington Privacy Act and other legislations provide for regulation of private entities' uses of FRT. Since 2019, FRT uses of various kinds have been banned at different levels. Multiple bills are in the pipeline which deal with the security, non-security and commercial uses of FRT differently.

Similarly, Canada has a comprehensive regime for the collection, use and disclosure of personal information for private, public and health sectors. Many countries are pondering over legislations and bans pertaining to invasive yet expansive uses of FRT.

5. *DigiYatra shall be categorised as commercial use.*

As the discussion paper points out, "the varied applications of FRT require a nuanced and measured approach towards its regulation, as opposed to a framework that treats all FRT alike, without considering the potential risks and benefits of each kind of application on its own merits" (page 12) In accordance with the typology suggested above, **the use-case of Digiyatra shall be listed as a commercial use of FRT.** It heavily engages in procurement of datasets with no legal liability. One of the many risks involves the purpose of data collection being breached owing to the absence of a data protection regime. Self-regulation safeguards, as promised by DigiYatra, without legislative backing

is only a myth. Additionally, the security, privacy and data-protection measures applicable to commercial uses of FRT shall be adhered to.

6. *Access to public goods and services shall not be denied based solely on automated data processing by FRT systems.*

   FRT-based processing shall not be the sole method for accessing public goods or services. Not only should FRT systems be voluntary, but also one among multiple methods for authentication. Commercial uses of FRT-based authentication should not be the sole option for accessing services and facilities by individuals. Moreover, in the case of FRT systems, there should be no denial of service to individuals. For commercial uses like the case of contactless onboarding at airports that Digiyatra targets, it should not be portrayed as the only option available to travellers.

7. *Risks related to design, development, testing, deployment, procurement, and use of FRT technology need to be individually and collectively addressed.*

   FRTs pose at least three kinds of risks:

   i) **Design-based risks** (algorithmic bias, non-availability of requisite material for design,deployment safeguards etc.)

   ii) **Procurement risks** (non-compliance with statutory rules/regulations, compromise in the choice of technology, etc.), and

   iii) **Deployment-based risks** (use of FRTs in poor settings or environments, by any actor, affecting accuracy levels, non-alignment with the core goals of the deployer, non-compliance with existing laws and privacy safeguard, unfettered use by state and private actors for mass surveillance, policing, and other activities, etc.).

   For technology-based risks, in general, international human rights law holds States responsible to conduct human rights due diligence systematically, including regular comprehensive human rights impact assessments, when designing, developing, purchasing, deploying, and operating surveillance systems.

8. *Need to adequately define the term 'constitutional morality' and its linkage with the RAI principles.*

The present discussion paper (like the previous ones published by the NITI Aayog) repeatedly invokes 'constitutional morality' as a cornerstone to develop principles for governing AI including FRT in India. Neither the present discussion paper nor the previous ones actually elaborate on what constitutes 'constitutional morality' and how exactly seven RAI principles were culled out from it.

Though, in India, the concept of 'constitutional morality' was invoked in the Constituent Assembly itself and later by the Supreme Court in a number of cases starting from Kesavananda Bharati (1973) and more recently and emphatically in Naz Foundation and Navtej Johar, etc., it has not been succinctly explained. It remains very abstract and means different things to different people. All that can be gathered from the discussion papers is that 'constitutional morality' is distinct from 'social morality' and in case of conflict the former must prevail over the latter. Further that constitutional morality "extends beyond the mere text of the Constitution to encompass the values of a diverse and inclusive society while remaining faithful to other constitutional principles". This articulation seems to have limited the meaning of 'constitutional morality', which is all encompassing and includes within it all the principles and values enshrined in the Constitution either explicitly or implicitly.

The term 'constitutional morality' also embodies human rights principles and standards provided in the core human rights treaties, to which India is a party. **It cannot be said that seven RAI principles identified in these documents capture the principles of constitutional morality fully well.** Many more can be added to the list**,** most importantly, the "principle of executive non-interference with the rights and liberties of the citizens without the sanction of law that is consistent with the Constitution"; and the right of the aggrieved person to seek appropriate remedy. These principles have their roots in the constitutional ethos and it is very much relevant to be reiterated in the context of AI and FRT particularly because of the fact that current deployments of FRT, either for (new categories), do not have any legislative backing. If use of FRT impinges constitutionally guaranteed rights, most importantly right to privacy, as explicitly

acknowledged in these documents, then it is important to point out that current usage is not consistent with the principles of constitutional morality.

9. *Application of the four-pronged test laid down by the majority in* K. S. Puttaswamy *as the threshold criteria for examining rights-based challenges to FRT.*

The present discussion paper suggests a three-pronged test laid down in K. S. Puttaswamy shall be adopted for examining right based challenges to use of FRT in India. On a careful reading of **K.S. Puttaswamy**, it appears that **the Supreme Court has in fact laid down a four-pronged test.** They are:

i. Existence of a valid law
ii. Legitimate/compelling state interests
iii. Proportionality
    a) Legitimate goal,
    b) Suitable means of furthering that goal,
    c) Least restrictive alternative , and
    d) No disproportionate impact on rights
iv. Procedural safeguards

It is important to include the fourth test as well for testing the validity of state measure that impinges the right to privacy. The same four-pronged test can be adopted for examining the challenges based on other fundamental rights as well.

As regards rights guaranteed under article 19 (1) of the Constitution, it is important to mention that what constitutes 'legitimate/compelling state interest' are explicitly enumerated in clauses (2) to (6) of article 19. Unless the law authorising use of FRT has rational nexus with any one of those enumerated compelling state interests, such law cannot pass the constitutional test.

10. *Consent-based regulatory framework is inadequate and requires rethinking.*

    i). The conceptualization of consent as something intrinsically connected with the expectation of no harm is also an important principle. This destabilises the straitjacket idea that consent should be the only formal prism to justify even highly unequal and harmful contractual relationships. The idea of consent is of course an expression of autonomy. However, **circumstances under which consent is given and the potential harm which may result from that consent, provide a moral ground for not relying on formal consent as a category for legitimising deeply unequal and flawed relationships that require the taking of personal data from an unwilling or more pertinently unknowing (in terms of the potential harm that can result from takings of personal data) individual**.

    ii). Continued emphasis on individual consent as the fundamental principle for allowing for privacy intrusions, when in fact individuals have little knowledge, information or agency in negotiating such acts of sharing of privacy is of concern .The principle of no harm is of import in the context of the internet. In most cases, formal consent or even tacit consent is considered to be adequate in providing legitimacy and or legality to activities online. However, this exercise of consent should also be accompanied by the principle of no harm should result from this consent. This would provide an obligation on the consent taker to ensure no harm results and much beyond the current practices of due diligence obligation under the IT Act or as envisaged under the DPDB, 2022.

    iii). Thus, **we need statutory intervention in ensuring that consent is exercised in a manner which is prior, free, informed and is accompanied by an obligation on the consent taker of ensuring that no-harm results from the giving of consent.**

11. *Measures to protect individuals' rights under the proposed DPDP Bill are inadequate, especially with regard to FRT.*

    The Digital Personal Data Protection Bill, 2022 was analysed with specific reference to biometric data (images) collected and deployed for the purpose of Facial Recognition

Technology (FRT). The following aspects are highlighted as discrepancies which requires amendment:

i. There should be **collection limitations for sensitive data like facial images and it should be collected only by the State and only when "necessary" for a public purpose**, which the DPDP fails to do.

ii. Clause 10 which defines "harm" should explicitly include "loss of access to goods and service" and "failure of the data principal to meet legitimate expectations." These harms can be anticipated specifically if access to public goods and services delivery is conditioned on the collection of biometric information and deployment of FRT.

iii. The only mention of profiling is in Clause 4(2). **Profiling of persons needs to be prohibited as it presumes access to personal information and repurposing of data without consent.**

iv. Clause 7 defines "consent" but does not include "prior". Consent needs to be taken before the collection of data from the data principal.

v. **Deemed consent provisions, governed on the standard of reasonable expectation, should only be applicable for State uses and be strictly limited to a limited number of instances like disaster management**.

vi. Specifically in the context of FRT, which we know has a propensity of producing errors as false negatives, **the right to not be subjected to decisions governing access to public goods and services based solely on automated data processing should be explicitly recognized**.

12. *Limitations on data collection and clear prohibition of repurposing of data without free, prior, informed consent.*

The data collected by several public cameras and other surveillance systems may be used for purposes beyond which the initial systems were installed. Researchers have pointed out this phenomenon, known as 'function creep', to be especially worrisome in the case of FRT. To ensure that there is no misuse of data, the kinds of data that are to be

collected, stored, processed, shared, and so on, shall be explicitly mentioned at the outset in various policy documents and frameworks regulating the use of individual's data for specific FRT systems. **Guidelines shall be put in place that put limitations on data collection and explicitly prohibit repurposing of datasets to ensure that data is used for pre-specified functions and purposes.**

13. *Establishment of an effective grievance redressal mechanism.*

States, under international and constitutional law, are mandated to provide remedies to redress acts constituting a violation of human rights. Remedies, as defined in international and constitutional law, must be effective, accessible, available, and affordable.

Under the Guiding Principles on Business and Human Rights (2011), the right to remedy is recognized as a foundational principle in the regulation of business for human rights. States, as part of their duty to protect against business-related human rights abuse, must take appropriate steps to ensure, through judicial, administrative, legislative, or other appropriate means, that when such abuses occur within their territory and/or jurisdiction those affected have access to an effective remedy. (UN Guiding Principles 2011). Industry, multi-stakeholder, and other collaborative initiatives should ensure that effective grievance mechanisms are available.

In the context of FRTs, a right to remedy is recognized as an integral part of the regulatory framework that governs them. Evidence of legislative, administrative, and judicial interventions across jurisdictions, highlight the value of a right to remedy for persons disproportionately affected by the use of FRTs. In such cases, constitutional remedies, like the remedy of *habeas* data, are tacitly and expressly recognized in personal data protection frameworks to ensure that data subjects have access to their personal data and can request the correction or deletion of data that either are inaccurate or are used for discriminatory purposes. (Special Rapporteur on Right to Privacy, 2022).

In India, a challenge to the State deployment of FRT was raised in a Public Interest Litigation, filed under Article 226 of the Indian Constitution before the High Court of

Telangana (2021). The petition raised several concerns including "the lack of procedural safeguards to prevent disproportionate harm to certain minorities and vulnerable persons", who are at higher risk of being profiled on the lines of caste, gender, religion, and sexuality. It was also submitted that there are no remedies available "to request access to data held about them, and to request its deletion, or to register their grievance in case of data theft or data breach" (para 40).

14. *Clear provisions for imposing penalties/sanctions for breaches and compensation for the persons aggrieved.*

The discussion paper mentions 'harm' (pages 19, 39, 47, 65, 66, 67)**, 'legal liability'** (pages 19 and 62) **and has an annexure dedicated to 'rights-based risks'** (page 64-68), **without making provisions for remedies for aggrieved persons**. Furthermore, the right to seek remedies in cases of violations, injury, or infringements, is sacrosanct in international human rights law and constitutional law. The State is duty-bound to make provisions for aggrieved persons to allege injury at the hands of State and private players. Additionally, a provision for remedies is mandated to be safeguarded in constitutional law, statutory law, or/and administrative law.

There are laws in other jurisdictions pertaining to the use of penalties by enforcement agencies in cases of infringement of data protection and technological misuse. The UK Information Commissioner's Office (ICO) recently served an Enforcement Notice and fine to Clearview AI Inc. for infringement of the UK GDPR and for using images of people in the UK, and elsewhere, to create a global online database that could be used for facial recognition (2022). The ICO found that Clearview AI Inc. had failed to use the information of people in the UK in a way that is fair and transparent, given that individuals are not made aware or would not reasonably expect their personal data to be used in this way; failing to have a lawful reason for collecting people's information; failing to have a process in place to stop the data being retained indefinitely, etc.

The on-going deliberations on a legally binding international framework to Regulate, in international human rights law, the Activities of Transnational Corporations and Other

Business Enterprises, are moving in favour of creating mandates for States to "adopt legal and other measures necessary to ensure that their domestic jurisdiction provides for effective, proportionate, and dissuasive criminal, civil and/or administrative sanctions were legal or natural persons conducting business activities have caused or contributed to human rights abuses." (Third Draft, 2021)

15. *Fair and comprehensive assessment of FRT to determine whether it can be used in a manner that is consistent with human dignity.*

    Studies regarding use of FRT have demonstrated how social dynamics and technology can manufacture unequal outcomes. To illustrate, an analysis of FRT algorithms developed by IBM, Microsoft and Face++ by digital activist Joy Buolamwini (2018) revealed that the software had higher inaccuracy rates while trying to recognize women, individuals of colour, and young people. Within the Indian context, according to a report published by the Centre for the Internet and Society (2021), the populations that have been historically marginalised such as Muslims, Scheduled Castes and Scheduled Tribes risk further discrimination through FRT. Another paper released by Vidhi Centre for Legal Policy (2021) did an empirical study of the usage of FRT by Delhi police that showed how the algorithm could potentially discriminate against those belonging to the minority sections in the city.

    Since the facial image is demonstrated in likeness of personhood, the enumeration of citizen-portraits as visual data through FRT by effacing social realities poses particular vulnerabilities. Unlike any personal information like social security number or bank password the loss of personal image entails serious risks as one's face cannot be changed. Visuality additionally exacerbates risks for women whose pictures would be ostensibly handled by male personnel at various levels of operation, and without relevant legislation pertaining to sensitive data management, the proposed gallery/database is likely to become a repository for voyeuristic gazing.

    Thus, **the discussion paper in descriptions of 'user'** (pages 32, 33, 36 and 46) **reduces and objectifies a citizen in the form of data in a visual format, and the process in**

decontextualizing an individual from its social context thereby further impinges upon its individual and collective rights. Given the public nature of the dataset that is tasked for production of digital citizens, the objectification inherent to the FRT mechanism causes biases against those historically persecuted within a society; a veritable reality that challenges all assumptions regarding 'responsible AI'. The end process of creating the virtual portraits thus reflects and reifies social hierarchies as gender, sexuality, religion, caste, class and ethnicity, which further endangers the subjects of the database in real time. **Faced with the enormity of harm that is likely to be caused by deployment of FRT, there cannot be any "acceptable error rate" (page 43) that justifies threat to personal and civil liberties and therefore it requires to be banned.**

16. *Prohibition on the use of junk science to justify the development and deployment of FRT.*

    As the discussion paper points out, there are multiple risks associated with use of FRT. One of the most important ones among them is **the harm caused to individuals and their rights by inaccurate probabilistic profiling of their behaviour.** This takes shape in various ways, **ranging from claims to recognise emotions through photographs, to predicting criminality, sexual orientation, propensity to illegal activities, and various other uses** that are not backed by science, and may be called as 'junk-science' applications. The report should highlight such applications of up and coming AI systems and ensure that no such systems are allowed.

17. *National standards need to be developed to ensure the quality and efficacy of FRT systems.*

    Several public agencies have issued tenders (Request for Proposals) for the procurement of FRT systems for various purposes. None of the tenders issued specify the standards, testing and quality certification which such FRT systems are supposed to conform with. Given that we know that in general FRT systems are not 100% accurate and can result in false positives and false negatives; **the lack of any standardisation criteria specified in**

such tender documents means that sub-optimal systems can be procured and deployed leading to grave consequences. Unlike in India, the NIST (National Institute of Standards and Technology) in the US (it is the equivalent of the BIS in India) has been conducting established the Face Recognition Vendor Testing Program (FRVT) in 2000 and has been undertaking periodic reviews of such FRT systems available on the market to test their robustness and efficacy. In the absence of any such equivalent initiatives in India, there should be an immediate moratorium on the procurement of FRT systems for public deployment.

18. *Auditing as a regulatory principle governing the use of FRT requires better enunciation.* The document mentions the term audit and describes an audit system to govern FRT a number of times (pages 33, 38, 43,44, 45,60, 62, 63). However this call, while welcome, in absence of a clear definition remains merely a token gesture. It needs to be realised that **auditing cannot be done in a vacuum and the term is of no consequential value without stating the relevant context**. To be clear about auditing we need to realise that the notion of auditing is not independent as to for whom and what purpose the audit is being performed. An auditor is typically present to mediate a principal-agent relationship. The principal has inadequate information about the agent and the auditor steps in to check if the information is accurate, verifiable and most importantly conforms to an acceptable standard.

    One of the first points to note here is that **for a proper audit system to be in place and identification of the principals and agents.** In the document there is no clear indication as to who the principal is—whether it is addressed to society at large concerned about use of data and dangers of technology, or the state as a user of the FRT remains unclear. Additionally, it does not list the goals of the auditing exercise on whether it is concerning the accuracy and reliability of the FRT technology or data breaches and the hazards thereupon.

    One key issue that immediately shows up is the issue of standards. The process of auditing demands verification of conformity to standards and requires them to be accordingly set. The only gesture towards realising this within the document is mentioned

in the constitution of an 'experts committee' (page 43) to set the standards and while a committee may - such standards and norms (as is generally argued over our submission) must be incorporated into a law or laws. Such law or laws are needed to join liability that arises in the event that standards are not met with suitable remedies.

Usually audits (in other contexts) are divided into internal and external audits. The document does not explicitly make this difference but on page 44 speaks of internal ethics committees and audits serving a 'self-regulatory, light touch measures' for internal governance. In reaction, as discussed elsewhere, the idea of self regulation in the context of AI is most unsuitable. Internal audits are inherently biased to protecting interests of internal members and are useful to the extent external audits are binding and vigilant. The interest served by internal audits is not the interests of the external audit.

Auditing is a costly exercise yet the document does not cover who bears the cost in this regard. It is **vital to explicitly state all the details of the financial expenditures incurred on account of the audits** which remain currently lacking in this paper.

19. *Development and deployment of FRT systems should be in conformity with international Human Rights principles.*

The unregulated or unfettered use of technology, including FRTs, poses a major threat to the human rights guaranteed under the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), Convention on the Elimination of Racial Discrimination (CERD), Convention on the Elimination, International Covenant on Economic Social and Cultural Rights, Convention on the Elimination of All Forms of Racial Discrimination, Convention Against Torture, Convention on the Elimination of Discrimination Against Women, Convention on the Rights of the Child, and Convention on the Rights of Persons with Disabilities. The use of FRTs also erodes the rule of law, civic spaces, and the foundations of vibrant and pluralistic democracies (OHCHR 2022).

The absence of legal frameworks and safeguards signals a serious lapse on the part of States and the international community. **There is international consensus that the**

human rights of individuals and groups are at the centre of all regulatory systems, and States are duty-bound to regulate technologies to minimise or eliminate the risks they pose to human rights.

Technologies, including FRTs, are posing discriminatory challenges on grounds of race, ethnicity, gender, religion, and sexuality, for which, international human rights law requires careful attention from government officials, the United Nations and other multilateral organisations, and the private sector, to these impacts of technologies (Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, 2020).

FRTs can pose a challenge to specific human rights including the enjoyment of human rights in peaceful assemblies (OHCHR, 2020), the right to privacy, the right to be presumed innocent, the right to a fair trial, the right to a fair and independent investigation, the right to information, the right against arbitrary arrest, the right to informed consent, the right to justice, the right to remedy for violations, etc.