Comments on the draft Unmanned Aircraft System Rules, 2020

The Internet Democracy Project welcomes the consultation by the Ministry of Civil Aviation, Government of India, on the draft Unmanned Aircraft System Rules, 2020. We would like to thank you for this opportunity to present our comments on this important policy document. In the interest of a transparent process, we hope that all responses will be made public.

At the Internet Democracy Project (https://internetdemocracy.in/, http://genderingsurveillance.in) we work towards realising feminist visions of the digital in society, by researching and analysing power imbalances in the areas of norms, governance and infrastructure in India and beyond, and by providing proposals for alternatives, based on this research, that can lead to a more equal digital society for all.

Unmanned aircraft systems, colloquially known as drones, can be equipped with devices[1] such as cameras, GPS trackers, sensors and facial recognition technologies, among others, and can be used by operators to locate people or objects, intercept phone calls, patrol areas and gather information, etc.[2] In India, the deployment of drones to patrol is not a recent practice: the Delhi government, for example, has been using it for over five years.[3] In the last few months, drones with thermal cameras have also been extensively deployed to ensure lockdown measures during Covid 19.

Drones are capable of appropriating a large amount of personal data of individuals without their knowledge. For example, while protests against the citizenship amendment bill were carried out in UP, the police of the state were conducting aerial surveys with the help of drones to keep track of the movements of alleged 'anti-social' elements. Among other things, they captured images of houses where bricks and stones are kept on the terraces. Terraces are a part of the house of a person, and as the Supreme Court in the Puttaswamy Judgement recognised houses as private

[1] Diaz, Angel. (2019). New York City Police Department Surveillance Technology. *Brennan Centre for Justice*. https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology
[2] EFF, (2017). Street-Level Surveillance. *Electronic Frontier Foundation*. https://www.eff.org/pages/dronesunmanned-aerial-vehicles
[3] Gill, Prabhjote. (2019). Police using drones to identify key protestors — and it may lead to harassment in the future. *Business Insider*. https://www.businessinsider.in/india/news/delhi-police-using-drones-to-track-down-protestors/articleshow/72902707.cms

spaces, are protected by the right to privacy. The State cannot hover over terraces using privacy invasive technologies unless there are exceptional circumstances..[45] As this example illustrates, the use of drone technology poses severe risks to the fundamental right of privacy of individuals in India.

Additionally, if drones become a part of everyday life of an individual in the country, this may lead to a chilling effect on the freedom of speech and expression of individuals. Studies highlight that the chances are high that people's behaviour will change with deployment of drones, as they will feel that they are under constant surveillance.[6]

The use of drones also may exacerbate instances of discrimination, as operators of drones in law enforcement agencies suffer from personal biases, which in turn may lead to further isolation and harassment of already marginalised communities.

For these reasons, in this submission we will comment on and make recommendations in particular to address privacy, freedom of speech and discrimination concerns arising from the Unmanned Aircraft System Rules, 202, so that this technology can be used to benefit the society.

We would like to draw your attention towards our detailed comments as follows:

Rules hardly mention or address privacy concerns

The draft Rules fail to account for the privacy implications that can be encountered by the usage of unmanned aircraft systems. Only rule 35 of the current draft Rules takes into consideration issues related to privacy. This rule states: 'imagery may be captured by an unmanned aircraft except in the non permissible area after ensuring the privacy of an individual and his property'. No other rule in the current draft deals with data privacy practices. In fact, the Rules also fail to delineate how the privacy of an individual and their property can be ensured while capturing images from unmanned aircrafts, a requirement in rule 35. Insufficient safeguards to protect the privacy of individuals is problematic and may encourage mass surveillance by the government and surveillance capitalism by private sector entities.

---

[4] K.S. Puttaswamy v Union of India, (2019) 1 SCC 1

[5] Tripathi, Swapnil. (Jan, 2020). UP Police's Drone Surveillance: A Step Towards 'Orwellian' State?. *The Quint*. https://www.thequint.com/voices/opinion/uttar-pradesh-police-drone-surveillance-of-houses-right-to-privacy-security-law-constitution

[6] M. Ryan Calo. People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship. Penn State Law Review. Vol. 114:3 http://www.pennstatelawreview.org/articles/114/114%20Penn%20St.%20L.%20Rev.%20809.pdf

For example, if a private entity, say an online e-commerce platform, starts targeted advertising on the basis of GPS tracking and images captured by drones deployed in residential areas of India, people will lose their right to privacy and choice, because individuals mostly do not have knowledge about who is collecting the data, for what purpose, how long and where to seek answer for all these questions, in fact they don't even have means to consent to it or refuse such consent.

Thus, it is recommended that unless there's a comprehensive personal data protection framework, usage of drones by private and public entities should be minimised to security of the state and public health emergencies or natural disasters. In addition, in the absence of a data protection regime, the rules themselves should delineate certain privacy standards and obligations upon drone operators.

Exemptions (Rule 29 and 57) are too broad, and lack sufficient transparency and accountability

While it is the sovereign function of the State to ensure the security of the State, it is imperative to note that in a democracy, this goal cannot be achieved by rolling out mechanisms for mass surveillance. In fact, the Rules must uphold the fundamental right to privacy of citizens and must provide strong safeguards against mass surveillance.

Contrarily, **Rule 29** of the current draft allows the Central Government to exempt any Central and State Government or any agency thereof from requirements to obtain an Unmanned Aircraft Systems (UAS) operator permit in the interest of the security of India or in the national interest. This rule is disconcerting for various reasons.

Firstly, one of the grounds for granting exemption under this rule is 'national interest', a word that has not been defined in any statute and can be interpreted in many ways, including to enable mass surveillance. As this blanket exemption rule may enable mass surveillance, it is violative of the right to privacy judgment, which lays down that any privacy infringing provision must be lawfully passed and must be necessary and proportionate.

Secondly, this rule empowers any agency of the government to seek exemption in the interest of the security of India. This has the potential to massively increase the number of government agencies that can effectively conduct surveillance of citizens in the name of security concerns, beyond existing agencies that have this explicitly in their mandate. Further, such blanket exemptions in the absence of robust surveillance laws may prove dangerous as most intelligence agencies lack statutory backing, and there is often no parliamentary or judicial oversight over the

decisions of intelligence agencies. Therefore, this provision can be misused by those in power: it may normalise the practice of conducting mass surveillance and may be used to contain protests that are not aligned with the government's ideology, among other problematic activities.

In addition, **Rule 57** of the Unmanned Aircraft System Rules, 2020, is a step ahead of exemptions granted under Rule 29: it allows the Central and State Governments to exempt any UAS or class of UAS or any person or class of persons from **the operation of these rules, either wholly or partially**.

These exemptions are too wide, as they allow Central and State governments to exempt any person, *any* UAS, class of UAS, person or class of persons from all or any of the rules. Thus, this rule allows the government to outsource certain essential functions of the state to non-state actors, such as maintenance of law and order. Delegation of such essential functions of the state to private actors may affect the basic rights of the citizens and is an unbecoming approach in a democratic country.

In addition, this provision would allow for exemption from even rule 35, the only rule in the current draft that addresses privacy concerns, leaving citizens without protections from surveillance even vis-à-vis private actors. Where the rule is severely misused, the implications may affect even the right to life and liberty of citizens. For example, if a rogue UAS operator is exempted from the rules 36-39 by the government, the operator may misuse the exemption and would be empowered to drop harmful payload or bullets upon citizens of the country.

Moreover, both the exemption Rules, 29 and 57, lay down no obligation upon the Central Government to notify the public about the agency, UAS or person that the Central Government is exempting under these Rules. Thus, in the absence of information or accountability, there lies a constant potential threat of misuse of these exemptions, posing an imminent threat to the fundamental rights such as right to privacy, right to equality and freedom of speech and expression of citizens of India.

In the light of the above, the following is recommended:

- **Only intelligence agencies that are statutorily backed should be considered eligible to avail of the exemption of security of India under rule 29,** because security of the state and national security are functions of certain specific agencies of the State, and should not be performed by any other agency, person or class of persons. Further, national interest as a qualifier should be removed and should be replaced with

exceptional circumstances such as public health emergencies and natural disasters should be qualifiers for other state agencies to claim exemption if necessary and proportionate.

- **Intelligence agencies and other central government ministries** should be considered eligible to avail of the exemption of security of India under **rule 57,** only in exceptional circumstances such as public health emergency, natural disasters and to ensure security of the state.
- **Robust surveillance reforms** such as statutory backing of all intelligence agencies, with these agencies only conducting activities as prescribed by the statute, and parliamentary and/or judicial oversight of all surveillance agencies and activities, among others, should be introduced and implemented prior to granting any exemptions to any UAS.
- The **Central Government may exempt** certain agencies (backed by statute) from application **of certain rules** (such as requirement for licenses or allow photography in restricted areas) but ***not*** **all the rules. No agency should be exempted from the following rules: 15, 19, 32, 35, 36, 37, 38, 39, 41, 43, 45, 58, 60, 65**
- The Central Government may exempt any agency under either of these rules only if it is satisfied that it is necessary and proportionate.
- There must be an order for an exemption, which shall be made available to the public if it affects public interest, and reasons for such an order are to be recorded in writing.
- **Each of these orders should be subject to judicial oversight**, as recommended by the Supreme Court in the Aadhaar judgment:[7] judicial officers shall examine the validity of the order and prima facie case against the data principal.
- Further, if drones are being used in a certain area on a regular basis, for example during the time of Covid 19, when states across the country have deployed drones to ensure quarantine measures, in such cases the state should ensure that the people that are affected or may be impacted should be informed about the nature, purpose and implications of the use of this technology.

Adherence to existing draft policies

The current draft of the Rules is not just deprived of new rules and recommendations to address privacy risks but also fails to acknowledge the privacy practices prescribed by the draft Drone Policy 2.0.

The draft Policy 2.0 emphasises the need for strict compliance of privacy by design standards for the manufacturers of unmanned aircrafts. The Rules, in contrast, do not mention privacy by design standards anywhere. Additionally, the draft Drone Policy 2.0 provides that unmanned aircraft service providers must establish feedback and review mechanisms, including requests to

[7] K.S. Puttaswamy v Union of India, (2019) 1 SCC 1, para 447.

access, anonymise, or erase the personal data of the data principal. However the draft Rules 2020 fail to accommodate these recommendations in the text.

Thus, it is recommended that the Rules **should acknowledge and adopt the best practices with respect to privacy in existing draft and notified government policies.** The new Rules must prescribe **strict compliance of privacy by design standards for the manufacturers** of unmanned aircrafts. Further, the rules should obligate unmanned aircraft service providers to establish feedback and review mechanisms, including requests to access, anonymise, or erase the personal data of the data principal

Miscellaneous Recommendations:

Ideally, the Personal Data Protection framework of India should ensure privacy and security of personal data of individuals. In the absence of a robust overarching framework, apart from the recommendations made above, following are other recommendations that will need to be implemented to uphold fundamental rights to privacy, equality and free speech;

- **Autonomous decision making:** Images, videos, GPS data, among other personal data collected by drones, should not be used for any autonomous decision making purposes such as serving personalised ads, as discussed above, and policing, among others.
- **Data retention policy**: Data collected by drones such as images, videos, GPS data, among other personal data, should not be retained unless there exists prima facie evidence that the data collected will ensure security of the state or national interest. Neither should the data accumulated be allowed to be shared or sold to any third party unless it is to ensure security of the state.
- **Audits and expenditures on drones**: To ensure transparency and accountability, all the expenditures made towards deployment of drone technology and the benefits of the deployment should be made public. If drones are used in national interest and for the public good, the information should be in the public domain. This practice would also ensure that the technology is not being misused and overused.