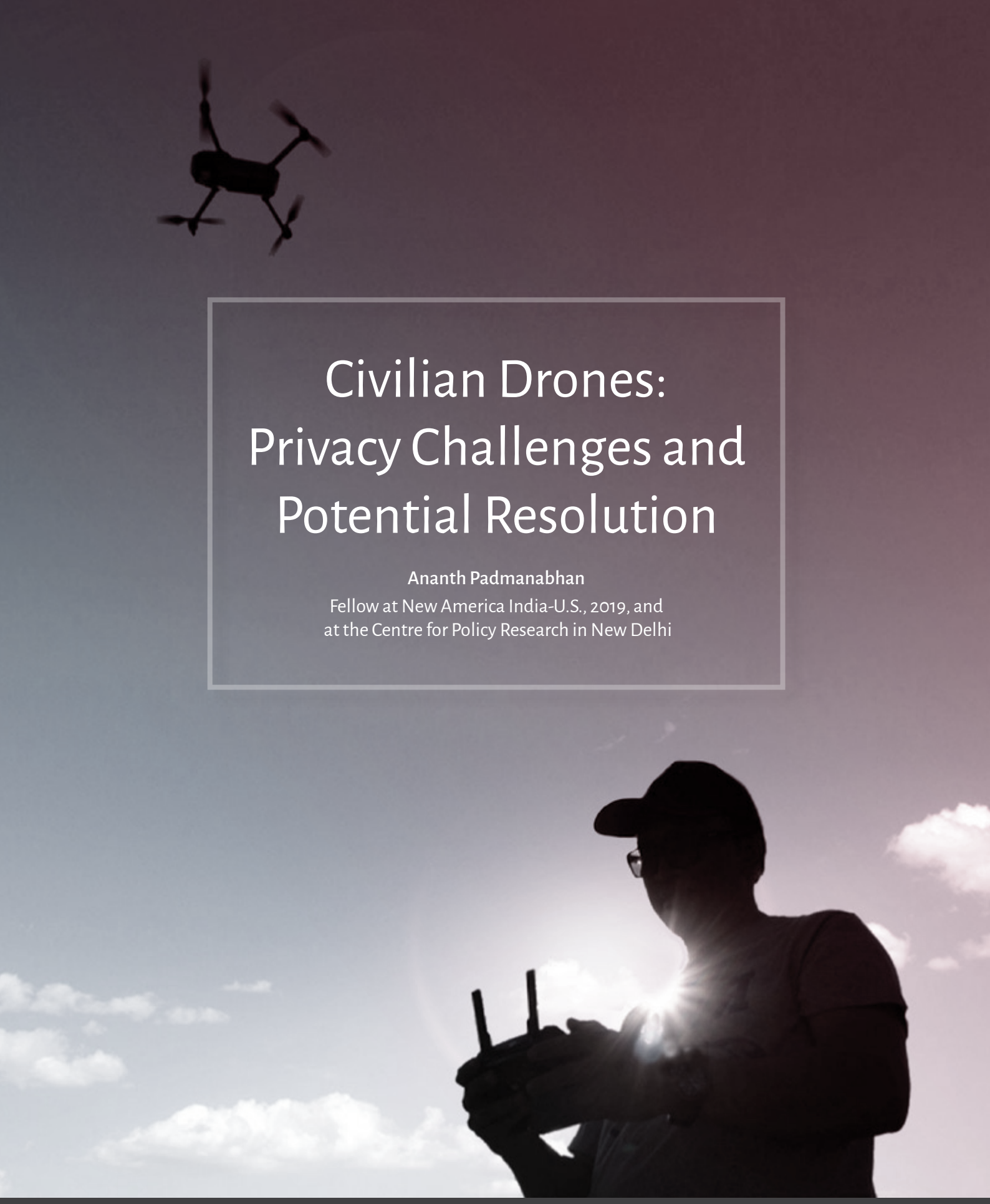
Civilian Drones: Privacy Challenges and Potential Resolution

September 2019

Ananth Padmanabhan

WORKING PAPER

CENTRE FOR POLICY RESEARCH



Civilian Drones: Privacy Challenges and Potential Resolution

Ananth Padmanabhan
Fellow at New America India-U.S., 2019, and
at the Centre for Policy Research in New Delhi

ACKNOWLEDGEMENTS:

The author extends heartfelt gratitude to Peter Singer, Arthur Holland Michel, Rachel Stohl, Anand Murali, John Livingstone, Mugilan T. Ramasamy, and Anirudh Rastogi for sharing their insights.

INTRODUCTION

From being a technology used predominantly by the military for years, unmanned aerial vehicles (hereinafter referred to interchangeably as UAV, UAS, or drones) have gradually moved into the public sphere by offering versatile civilian uses. This is due to converging technological advances such as hardware miniaturization, sophisticated software functionalities, and advanced sensors.[1] While several countries have seen this explosion of drone innovation in the civilian airspace, China stands out with the dominance of Da-Jiang Innovations (DJI) as the market leader.[2] The United States has seen the rise and fall of many drone start-ups, alongside a realization on the part of leading aircraft manufacturers about the immense potential of the technology.[3] U.S. dominance in adjacent fields – artificial intelligence, robotics, and 3-D printing, to list some here – is significant, making it a force to contend with in this sector. India has primarily witnessed the proliferation of drone service companies that offer solutions across a range of areas, from agriculture to event photography. But Indian companies have not yet made a mark globally when it comes to the manufacture of drones or supporting hardware elements.[4] In short, the innovation landscape and relative strengths and weaknesses are significantly varied across countries.

The regulatory landscape is similarly incongruent across jurisdictions.[5] In an earlier report, I examined this issue, comparing the regulatory responses across key jurisdictions to the civilian use of this technology.[6] This work arose in the context of India's initial regulatory responses, wherein the Ministry of Civil Aviation (MCA) first declared, in 2014, a complete ban on civilian drone operations and followed by a set of draft regulations that failed to support the full potential of this technology when it came to commercial uses. As that report argued, the fledgling industry could be permanently crippled under the weight of security apprehensions that permeated that set of draft regulations. At the same time, the draft had not considered several aspects of drone operations that demanded regulatory attention,

In short, the innovation landscape and relative strengths and weaknesses are significantly varied across countries.

including property protections and safety concerns. It was thus both over- and under-inclusive. But in an optimistic turn, the new regulations that came into effect in December 2018 took a more progressive stance, earning a dial-down of some of the earlier criticisms.[7]

The newest set of regulations take seriously the challenges of compliance arising from a licensing regime. They propose a reg-tech (regulatory technology) solution to these challenges, namely Digital Sky, which operates as a platform for convenient filing of paperwork to obtain unique identification numbers and operators' permits.[8] These identification numbers and permits are a prerequisite for most remotely piloted aircraft (RPA) operations under the regulations. Appropriately titled Regulations 1.0, these regulations also present a window for future innovation in this sector, including testbed locations for experimental projects.[9] Though delivery drones may presently appear a distant use case, considering all operations must have a remote pilot operator for each RPA and be within visual-line-of-sight (VLOS), there is a distinct possibility that the sector would expand with time to accommodate fully autonomous, self-controlling drones that operate without the presence of any manual operator and beyond VLOS.[10] The safety of drone operations has also merited significant attention, including insistence on geo-fencing technological capabilities beyond a certain height and for most weight categories, and the requirement of drone operator insurance to compensate for any losses incurred because of commercial operations.[11]

However, despite privacy (of individuals, communities, and personal data) being a critical concern, solutions have not found a place in the regulatory narrative even as civilian use grows. Drone operators have also flagged concerns regarding confidentiality of their operations but those are outside the scope of this paper. Here, the focus is on end-user concerns, with the argument being advanced that the challenges in this regard are common to the United States and India. These challenges can be further subdivided into two sets, categorized here as "traditional privacy challenges" and "big data privacy challenges." These challenges are explained more fully in the next section. On both counts, legal and regulatory responses have been far from satisfactory. The aim of this paper is threefold: *descriptive* for clearly identifying these challenges; *explanatory* for demonstrating why they remain unresolved; and *reformative* to advance better regulation in this area.

The discussion proceeds in three segments. The first segment captures the present regulatory landscape in India on this issue and argues that privacy concerns have been mostly ignored or at least unaddressed in any meaningful way. The second segment discusses "traditional privacy challenges" and the limitations of the law, including constitutionally guaranteed rights when it comes to civilian drones and possible high-level responses. The third segment discusses "big data privacy challenges," current legal and regulatory limitations, and possible high-level strategies and responses. A short conclusion follows.

THE PRIVACY CHALLENGE AND BROAD REGULATORY BRUSHSTROKES

The present Indian regulations only require that RPA operators be "liable to ensure that privacy norms of any entity are not compromised in any manner," with nothing more by way of guidance on achieving this outcome.[12] The RPAS Guidance Manual accompanying these regulations, issued by the Directorate General of Civil Aviation (DGCA), simply restates this liability.[13] Additionally, no technological requirements have found mention in the regulations, unlike with safety concerns through the presence of geo-fencing and detect-and-avoid systems. A supplementary document accompanying the regulations places full responsibility on the RPA operator to come up with standard operating procedures (SOP), including to protect the privacy of persons, without any baseline that such SOP must meet in this regard.[14]

Public documents on the Digital Sky project do not consider privacy an important enough concern to be addressed through this reg-tech solution. The public tender for this digital platform contains Annexure No. 8, which outlines its technology architecture. It merely states that the "privacy of data should be fundamental in the design of the system without sacrificing the utility of the state procurement system" and reiterates that the handling of sensitive and critical data must not remain an afterthought in a system of this scale. It also references the IndiaStack – a system of Application Programming Interfaces built on top of India's centralized digital identities database, Aadhaar – as a model stack with privacy-protected data sharing.[15] This reference disregards the fact that the kind of data gathering and processing that is facilitated by drones is far removed from the use cases of personal data processing that IndiaStack can potentially resolve.

The vision for Digital Sky – no permission, no take-off (NPNT) – envisages setting "rights for airspace permission access at a fine-tuned level (for example, the ability to choose a polygon area of airspace at a particular altitude and for a particular date and time) and … enforced digitally through … generation of verifiable flight telemetry."[16] The DGCA will grant a "permission artefact" in the form of a digitally signed XML format file that specifies the geographic area and time of operations, and the identification details of the remote pilot. The RPAs are meant to carry firmware that can authenticate these artefacts and confirm that the flight parameters of the mission match those contained in the artefact. Thus, to be NPNT compliant, any flight module must carry three important features: a unique identifier to allow the end-to-end traceability of a flight module, a system to obtain and verify a permission artefact, and the elimination of any synthetic flight logs or external systems to provide simulated logs.[17]

Compared with these elaborate specifications for regulatory compliance, the Digital Sky Technology Standards go easy on privacy concerns. The primary response is through an articulation of "privacy-by-design (PbD)." This is included as a guiding design principle in the Standards, with its four key features being: a) proactive, not reactive, and preventative, not remedial; b) privacy as the default setting; c) visibility and transparency; and d) respect for privacy, of all stakeholders.[18] But there is no concrete direction, unlike with aspects such as key management and identification of registered flight modules that find more extensive detailing in the Standards. More recently, the MCA issued a Drone Ecosystem Policy Roadmap, where it is reiterated that "for privacy, we require manufacturers to adhere to a privacy by design standard, eliminating risks of future privacy

harms by operators." Though not a legally binding document, the roadmap captures the MCA's vision for civilian drone businesses and their regulation through Digital Sky and other means. Discussing fully autonomous drone operations, an area identified as the next frontier of innovation in this technology domain, the roadmap merely notes that "use of algorithms for piloting may be permitted, but only if adequate safety, security and privacy principles are demonstrated in the design of operations."[19] PbD is identified as an area to which airworthiness standards for drone design could potentially extend, such that privacy principles can be "embedded into the functional design … by introducing technical measures that enable *privacy as the default setting*."[20] In addition to these recommendations, the roadmap also envisages drone service providers including "technical and organizational measures designed to implement data-protection principles as part of any UAS operation that collects personal data, and to integrate the necessary safeguards to protect the rights of data principals" and "feedback and review mechanisms including requests to access, anonymize, or erase the data of the data principal." Remote pilot operators are also expected to be trained in applicable privacy and data protection laws of India before being approved to handle RPA operations.[21]

The reference to PbD in the standards and roadmap is also relevant because India's newly proposed Personal Data Protection Bill, 2018 emphasizes reliance on this concept. This bill resulted from extensive deliberations by an Expert Committee of the Ministry of Electronics and Information Technology headed by retired Justice B.N. Srikrishna (hereafter "Srikrishna Committee"). In relevant part, it states that data fiduciaries shall implement managerial and organizational policies, business practices, and technical systems that anticipate, identify, and avoid harm to the data principal and ensure that the interests of the data principle is accounted for at every stage of personal data processing.[22] This provision must be read in the light of deliberations by the Srikrishna Committee leading up to this bill, captured in an initial white paper that was circulated for public comments in November 2017. Here the committee has noted difficulties when operationalizing the notice and consent framework for the internet of things (IoT) and IoT-enabled applications that gather data ubiquitously. These technologies do not present individuals with the opportunity to evaluate privacy harms associated with specific use cases, and based on such evaluations, to either accept or reject such instances and applications of personal data collection and processing. Manufacturers of several "smart devices" used at homes and in personal settings decouple privacy notices from such devices and make them available instead on their respective websites. However, the Committee observed that this is not a very effective method to inform users about the data collection and use practices of such devices. The Committee therefore insisted upon the need to develop better notice design or whether such notices are the right solution for the privacy harms arising from the use of these "smart devices." The Committee also noted that standard responses such as de-identification techniques do not work very well in many such cases. As an example, the white paper cited gait analysis based on data processing by a wearable activity tracker, where no amount of possible de-identification could secure foolproof privacy protection.[23]

At present, there are no straightforward responses to the new kinds of privacy challenges posed by a combination of ubiquitous data gathering and advanced data analytics. Drone operations can potentially gather significant amounts of personal data, including facial images and location coordinates of individuals, and analyze them to granular detail. These activities pose great risk to both individual and community privacy, including re-identification of anonymized datasets and extensive profiling. The "big data privacy challenges" arising from these activities are discussed in Part III of this paper. Additionally, civilian drones offer the capability to commit more traditional forms of privacy violations, including intrusions upon spatial privacy and unlawful surveillance. The present regulatory response in India needs to evolve to address these concerns in a stronger way, as detailed in the following section.

TRADITIONAL PRIVACY CHALLENGES AND RESPONSES

In the U.S., the Electronic Privacy Information Center (EPIC, a non-profit research center) petitioned the Federal Aviation Administration during the rule-making process for civilian UAS operations, providing an overview of traditional privacy challenges.[24] EPIC highlighted the increased capacity for domestic surveillance offered by drones through high-definition cameras, real-time video streams, a massive geographical sweep, heat and motion sensors, automated text and facial recognition technologies, and the ability to operate undetected. It also raised concerns regarding incentives for various kinds of businesses to develop and deploy drones for a wide range of data gathering purposes, including 'paparazzi drones' to track and photograph celebrities, street-level drones to enhance satellite imagery, and drones offered as market solutions for private detectives. The FAA refused to consider these issues, leaving it to states to respond appropriately to the various privacy concerns, resulting in a "patchwork" of privacy protection.[25] The FAA reaffirmed this stance in February, 2019, as part of a fresh rule-making exercise.[26]

Similarly, in the Indian context, the privacy jurisprudence does not offer clear principles to adjudicate claims against private violators. The primary reason for this – disproportionate focus on constitutional principles that are better addressed to tackle privacy violations by the State, rather than the organic evolution of privacy through tort law (as has happened in the United States) – and other reasons, such as a weak civil justice system with long-pending cases and minimal judicial guidance on evaluating and apportioning damages for tortious claims, have been elaborated in my earlier report.[27]

The "patchwork" in the U.S., which is comprised of not only state laws but also a wide range of local ordinances, makes it difficult to pinpoint any legislation as the ideal. At the same time, certain principles and regulatory approaches stand out. Commonly restricted conduct includes operations over public property and critical infrastructure; over private property without the owner's consent; in parks; and at large events.[28] Criminal law and high monetary penalties are relied upon to address intrusive behavior that makes use of drones, with the ability to factor in the intent of the perpetrator when deciding on questions of guilt and punishment. For instance, North Carolina prohibits using drones to photograph a person with the intent to publish or distribute the photo, but exempts "newsgathering, newsworthy events, or events or places to which the general public is invited." Similarly, Arkansas law criminalizes the use of drones for video voyeurism, Indiana addresses "remote aerial harassment" and "remote aerial voyeurism," and the Californian legislation is targeted towards individuals who knowingly enter air columns immediately above private property for taking pictures or videos. South Dakota prohibits using a drone with a camera to take photos of private property or a person on private property when the person has a reasonable expectation of privacy.[29]

Through all of these examples, an attempt to balance multiple values emerges: the prospect of innovation using this new technology, the reasonable expectation of privacy in certain settings, and fairness of criminal action. The American Legislative Exchange Council has put out an easily comprehensible and consistent model law in this regard, primarily focusing on harassment and stalking activities that are met with criminal penalties of the same nature as "a misdemeanor punishable by imprisonment for not more than 90 days or a fine of not more than $500.00, or both." The model law also proposes penalizing the knowing and intentional operation of drones to "capture photographs, video, or audio recordings of an individual in a manner that invades the individual's reasonable expectation of privacy."[30] Indian lawmakers could benefit from these insights while avoiding the patchwork in the US, intervening at this early stage to come out with drone legislation that sets the balance between criminal offenses and civil liabilities, and

clearly spells out different kinds of conduct to which they apply.

The Indian legal system has also not been responsive to mass surveillance, partly because, for several years, the status of privacy as a fundamental right in India was ambivalent at best. But also, mass surveillance has not run into effective legal and constitutional challenges because Indian courts have analyzed State surveillance within the factual context of individual, rather than systemic, surveillance. In fact, many of the contested instances involve individuals who found their way into "history sheets" maintained by the police for reasons justifiable or otherwise. Upon constitutional challenges against police action, the Supreme Court has balanced out individual rights with social goals, such as maintenance of public order, often prioritizing the latter. Even in cases that apparently address systemic flaws, such as unauthorized telephone tapping, the technical capabilities of the executive and the intent behind the contested State action were both limited towards a subset of individuals. Therefore, the court laid down procedural and substantive restrictions on the authority of the State to carry out surveillance, which would operate on a case-by-case basis. The court's detailed directives against telephone tapping demanded specificity of State action in the communications and persons and addresses intercepted; the exhausting of alternate and less intrusive ways to acquire the information before activating interception; or the limiting of intercepted material to the necessary minimum. However, these directives are not adequate safeguards against mass surveillance as they fail to conduct a robust review of the technology architecture in place to gather and process data.[31]

Shifting from this context to one of mass surveillance where technical capabilities permit non-targeted gathering and processing of data without further action from the political executive has been a steep learning curve for the Apex court. The 2018 verdict in *Justice Puttaswamy v. Union of India* shows the challenges when adjudicating the legality of such measures.[32] This case involved an omnibus constitutional challenge to Aadhaar, India's biometric identities project aimed primarily at de-duplication of identities to ensure that welfare benefits from the State reach their rightful beneficiaries. Among the various grounds of the challenge was a novel one that attacked the excessive seeding of Aadhaar numbers in multiple databases, such as a pension, education, banking, and telecom databases. The petitioners argued that this exercise would, in effect, present the State with a mass surveillance tool. Additionally, they also pointed out that various state resident data hubs (SRDHs) helped to offer a 360-degree view of residents, as publicly acknowledged by the State governments – Haryana, Andhra Pradesh, Tamil Nadu, Madhya Pradesh, and others – instituting them. These SRDHs used the Aadhaar identity as their foundation without incorporating the protections under the Aadhaar Act in respect to data security or privacy. Thus, the SRDHs made it evident that the aggregation of data from different silos, profiling, and consequential surveillance of residents was no longer in the realm of conjecture; it had become reality. The Aadhaar numbers made finding information much more convenient by serving as a unifying link across various government departments and between their respective databases.

To articulate this threat in legal terms, the petitioners relied on important decisions of the European Court of Justice that treated mass surveillance as a separate category when up for judicial review. These cases focused on the structural and architectural aspects of the respective surveillance programs. But the Indian Supreme Court followed a more conservative approach, narrowly balancing immediate individual harms and long-standing social goals rather than assessing medium and long-term consequences of such unified databases. While the majority opinion suggested several quick fixes for any immediate harms from the workings of Aadhaar, they hardly addressed the long-term consequences of SRDHs and other potential applications of Aadhaar for big data analytics and profiling. In fact, the majority did not even reference SRDHs despite the petitioners pointing out that, when combined with multiple databases, the view that Aadhaar offered on citizens could

be extremely invasive. The majority observed that the averment of "a surveillance state created by the Aadhaar project is not well founded, and in any case, is taken care of by the diffluence exercise carried out with the striking down certain offending provisions in their present form."[33]

For reasons best known to the State, it extensively relied during the hearing on a powerpoint presentation by the Chief Executive Officer of the Unique Identification Authority of India (UIDAI). This presentation mostly focused on the security architecture in place to prevent data leaks and did not address the surveillance threat or refer to the SRDHs. Yet, the majority verdict endorsed these claims that were, at best, irrelevant to the surveillance challenge. This is particularly disconcerting because secure systems can simultaneously be extremely sophisticated surveillance machines. Instead, the majority would have done well to follow the various European court decisions that consistently opposed state-of-the-art mass surveillance architectures because their long-term consequences, while not fully ascertainable, made them even more worrisome and intrusive. All this goes to establish the case here that Indian courts have an extremely limited vocabulary to address questions of mass surveillance. Because of the widespread use of civilian drones in governance is a distinct possibility, it is important that such vocabulary be developed immediately in order to address concerns that are more architectural in nature. Digital Sky or enhanced security systems cannot substitute the need for the same as their primary focus is on ease of regulatory compliance and safety of drone operations.

The court could look to the "chilling effects" doctrine as developed by U.S. courts as a possible solution here. It has, in fact, done so previously in a different setting. In Shreya Singhal v. Union of India,[34] a case dealing with free speech, the police had invoked section 66-A of the Information Technology Act, 2000 against some Facebook users for expressing their displeasure at a city-wide shutdown in Mumbai in the wake of Shiv Sena supremo Bal Thackeray's death. Striking down this provision as being unconstitutional for its chilling effects on the freedom of speech and expression, the court opened doors to the possibility of evaluating structural power imbalances brought on by vaguely-worded criminal offenses. Chilling effects can occur when a citizen apprehends that the State is watching their activities and alters their behavior based on this belief. While immediate criminal consequences may not necessarily follow, the mere existence of vague and overreaching criminal liabilities could restrain individuals from expressing themselves due to the fear of such consequences. As the court reasoned, "Section 66-A is cast so wide that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net. Such is the reach of this section and if it is to withstand the test of constitutionality, the chilling effect on free speech would be total."[35]

While this doctrine is not a perfect mechanism to scope out the limits of state authority when undertaking mass surveillance, and can even be a conversation-stopper in this context, the verdict in *Shreya Singhal* demonstrates the need to evaluate possible long-term consequences of state action. To do so, the judiciary must go beyond immediate cases of rights infractions to a critical scrutiny of the architecture of data collection put in place, be it legal or technological. This is not a point limited to rights reviews. Even cases involving the dilution of judicial independence through the formation of tribunals, for instance, demand a similar outlook – as do instances such as circumventing legislative scrutiny through frequent resort to executive ordinances. In all these situations, the State's usual defense – that the scope for abuse is not grounds for striking down an executive or legislative action – is weakened. These are all architectural questions, ones that have a bearing on even the basic structure of the Constitution, but not in the same way that surveillance orders against repeat offenders or individual instances of telephone tapping impinge on individual rights.

BIG DATA PRIVACY CHALLENGES AND SOME RESPONSES

Besides their low-altitude operations, with direct spatial privacy and surveillance concerns, drones also gather considerable amount of data. Drone platforms – often consisting of in-flight software to help command the aircraft, high-resolution Light Detection and Ranging (LiDAR) imagery solutions, digital orthomosaic technology to stitch together varied images and present a composite picture, photogrammetry to calculate distance and volume measurements, and data analytics solutions – offer critical actionable insights to several industries today. This capability has resulted in business models where such platforms are offered as services.[36] In addition to the new kinds of sensors and data that drones can gather, they also transmit the standard types of data that any internet-of-things solution can potentially channel to a central server—- mobile phone data, radio frequency identification data, location, weather and temperature data.

A significant part of such data would fall within the legal definition of sensitive personal information. No special case needs to be made here for the privacy risks associated with such data, evident as they are from the strict legal mandate that prior written consent of the data-holder is required to collect and process the same Apart from the stand-alone risks of such data in the hands of private entities, these pieces of data are often combined with personal data categories – social media behavior, biometric information, financial data – gathered from other sources, to heighten the risk.[37] These "big data privacy challenges" are however less obvious as compared with risks highlighted in the previous section, and we remain relatively underinformed about them even in settings outside of the civilian drone context.

Often, the challenges there are not with the gathering of data, but rather with how it is processed and the associated risks. As digital activities grow exponentially, so do the electronic tracks left behind by individuals. The semantic web and other data analytic solutions permit such crumbs to be aggregated by intelligent machines and algorithms to provide a comprehensive picture of an individual's preferences, personality traits, and values, as well as predict her next move and suggest specific, relevant choices. Yet such practices run the risk of being reductive, incomplete, and often divorced from the context in which the data was originally gathered.[38] Because of the efficiency involved in algorithmic perception, prediction, and suggestion, and the recombinant nature of data, private actor incentives are aligned towards the unhindered amassing and processing of huge swaths of personal data, often for purposes unidentifiable at the time of the original transaction or data exchange. As noted by the Indian Supreme Court, these privacy invasions often go undetected because of the non-rivalrous and invisible nature of data access, storage, and transfer.[39]

Unstructured streaming data presents new challenges for state-of-the-art anonymization strategies developed to deal with static, structured, and well-defined datasets.[40] Re-identification techniques have evolved in parallel, combining multiple Personally Identifiable Information (PII)-excluded databases to arrive at near identical results as those emerging from the processing of a PII-inclusive database.[41] The newly created database can then be linked with other databases, even PII-excluded ones, to compromise anonymity. These techniques present a cautionary tale: against the ubiquity of "data fingerprints" left by individuals, and the excessive linking of multiple databases, PII protection can do much less than before. Therefore, the legal mandate on big data handlers must go beyond anonymization and de-identification strategies that exclude PII.

Finally, much like the issue with surveillance identified in the previous section , i.e. refocusing attention from targeted to mass surveillance, big data processing demands refocusing attention from individual to group privacy and the simultaneous development of policy positions on handling community data. Individuals, while not personally

identifiable in many such cases, may still be "reachable" on account of being within a group targeted for prejudicial action based on data-driven inference and prediction.[42] To illustrate, individuals practicing a certain faith can be targeted either by identifying them individually or through a larger group consisting of several individuals practicing this faith. In the latter scenario, while the individual remains unidentified, she is vulnerable to any action taken against the group. Often, individuals are even unaware of such memberships because the aggregated datasets and groups emerging therefrom do not perfectly align with pre-existing real-world groupings, constructed as they are by algorithmic black boxes.[43] The excessive linking of multiple datasets also enables group profiling without any personally identifiable information being breached.[44] Of particular concern is the possibility of constructing "demographically identifiable information," which then enables the classification, identification, and/or tracking of a specific categorization based on ethnicity, religion, gender, age, health condition, location, or any other demographically defining factor.[45] Though aware of these risks, the Srikrishna Committee did not propose any immediate solutions for community data protection, perhaps because it did not strictly fall within its mandate.[46] Noting the need for a "principled basis for according protection to an identifiable community," "class action remedies for certain kinds of data breaches involving community data," and "tools like group communication and sanction," the Committee strongly recommended that the Government of India address them through appropriate legislation.[47]

Many of the solutions to these threats are within the ambit of personal data protection and regulations thereof, but it is unclear how effective they could be in balancing the multiple values at stake. With new modes of gathering and processing data, such as internet-of-things and remote cloud servers, privacy notices that are predominantly available on websites and mobile apps are fast losing their relevance.[48] The pervasiveness of digital technologies and applications has also resulted in "consent fatigue" due to the increasingly large number of requests for consent and the disproportionate time required to meaningfully assess such requests by the user on a routine basis.[49] Meaningful consent is further vitiated by a substantial number of companies adopting a "take it or leave it" approach to privacy notices, with no room for negotiation.[50] Privacy notices also often suffer from verbosity and dense legalese.[51] Moreover, the draft bill proposed by the Srikrishna Committee does not address many situations where it is difficult to register consent because of technological or interface limitations. Consequently, the notice-and-consent foundations of this bill can diminish the flexibility needed for new data technologies to scale and grow.[52]

Therefore, solutions on offer at present, especially the idea of privacy self-management, need to be customized to the specific context of civilian drone use. Here, responses could include integrating a notice dashboard as part of Digital Sky. The public then can access information about the geographic locations and purposes served by drone operations, the sensing and data gathering technologies onboard the unmanned system, the kinds of data potentially captured, and technical specifications relating to the granularity and accuracy of the data collected and processed, from such dashboard. By providing this option, the DGCA can effectively compel drone operators to carry out privacy impact assessments and publicize them before undertaking such operations. Data minimization can also be achieved because these assessments and disclosures make it possible to evaluate whether the data operations are proportionate with the stated purposes, thereby disincentivizing drone operators to gather or process disproportionate amounts or types of data.[53] Many of these recommendations are reflected in a set of voluntary best practices that the National Telecommunications and Information Administration (NTIA) released in 2016.[54]

CONCLUDING REMARKS

The traditional privacy challenges raised by drone technology – fitting drones with devices that can capture personal and private information at very close range, using the technology for mass surveillance, causing discomfort to human beings through their intrusive nature – are concerns totally ignored by the present regulatory response in India, except to place liability on drone operators for any such harms. Criminal law responses similar to those present in many of the state legislations in the U.S. need to be introduced to penalize rogue actors with wrongful intent to intrude upon privacy. In parallel, strengthening the civil tort of privacy through clear delineation of principles for quantification of damages, and the constitutional tort of privacy through appropriate legal standards to restrain mass surveillance projects, is required to safeguard individual interests against such traditional privacy harms.

The Indian State must also move ahead to create appropriate personal and community data protection regimes that place limits on the processing of such data using drone technology. This framework should make use of a co-regulation framework that incentivizes private actors to adopt voluntary codes of conduct and places responsibility on appropriate state authorities to evaluate such codes, suggest suitable modifications, and monitor compliance with the same. The Digital Sky platform, a state-of-the-art solution for regulatory compliance as well as drone tracking, should be expanded to publicize privacy impact assessments carried out by drone operators. These are basic steps that must be implemented soon to keep pace in an area where law and technology will continue to evolve.

These are basic steps that must be implemented soon to keep pace in an area where law and technology will continue to evolve.

END NOTES

1. Bart Elias, Unmanned Aircraft Operations in Domestic Airspace: U.S. Policy Perspectives and the Regulatory Landscape (Washington, D.C.: Congressional Research Service, 2016)
2. Tom Hancock and Wang Xueqiao, "China's DJI targets agriculture as consumer drone sales slow," Financial Times, March 25, 2019
3. Richard Levick, "Drone Industry Just Beginning To Take Off," Forbes, May 15, 2018
4. Ujjwal Bakshi and Manash Neog, "Much to Drone About," Economic Times, April 4, 2019
5. Therese Jones, International Commercial Drone Regulation and Drone Delivery Services (Santa Monica: RAND Corporation, 2017)
6. Ananth Padmanabhan, Civilian Drones and India's Regulatory Response (New Delhi: Carnegie India, 2017)
7. Somya Lohia, "Drone Regulations 1.0 Can Fetch India Major Slice of $100 Billion Industry," Money Control, January 9, 2019
8. Civil Aviation Requirements Series X Part I Issue I: Requirements for Operation of Civil Remotely Piloted Aircraft System (RPAS), F. No. 05-13/2014-AED Vol. IV (New Delhi: Directorate General of Civil Aviation, 2018)

9. Ibid., Reg. 14.2.
10. Ibid., Reg. 12.14 & 12.2.
11. Ibid., Reg. 11.2 & 17.1.
12. Ibid, Reg. 12.21.
13. DGCA RPAS Guidance Manual (New Delhi: Directorate General of Civil Aviation, 2018)
14. Procedures for Operation of Civil Remotely Piloted Aircraft Systems (RPAS) in Indian Airspace, AIP Supplement 164/2018 AAI/ATM/AIS/09-09/2018 (New Delhi: Airports Authority of India, 2018),
15. Tender Document: Development, Hosting and Maintenance of Digital Sky Platform for Ministry of Civil Aviation IT-11042/1/2018-DIRECTORATE OF IT (New Delhi: Airports Authority of India, 2018)
16. DGCA RPAS Guidance Manual (New Delhi: Directorate General of Civil Aviation, 2018)
17. Ibid
18. Ibid.
19. Drone Ecosystem Policy Roadmap (New Delhi: Ministry of Civil Aviation, 2019),
20. Ibid, 7.
21. Ibid, 14.
22. The Personal Data Protection Bill, 2018 (New Delhi: Ministry of Electronics and Information Technology, 2018),
23. White Paper of the Committee of Experts on a Data Protection Framework for India (New Delhi: Ministry of Electronics and Information Technology, 2017),
24. Petition to the Federal Aviation Administration: Drones and Privacy (Washington, D.C.: Electronic Privacy Information Center, 2012),
25. Margot Kaminski, "Drone Federalism: Civilian Drones and the Things They Carry," California Law Review 4 (2013): 57–74.
26. Notice of Proposed Rulemaking: Operation of Small Unmanned Aircraft Systems Over People FAA–2018–1087 (Washington, D.C.: Federal Aviation Administration, 2019),
27. Ananth Padmanabhan, Civilian Drones and India's Regulatory Response (New Delhi: Carnegie India, 2017),
28. Arthur Holland Michel, Drones at Home: Local and State Drone Laws (New York: Center for the Study of the Drone, Bard College, 2017),
29. Amanda Essex, Taking Off: State Unmanned Aircraft Systems Policies (Denver, CO: National Conference of State Legislatures, 2016),
30. An Act Relating To Unmanned Aircraft Systems – Establishing Statewide Standards, Protecting Privacy, And Ensuring Public Safety (Virginia: American Legislative Exchange Council, 2017), https://www.alec.org/model-policy/an-act-relating-to-unmanned-aircraft-systems-establishing-statewide-standards-protecting-privacy-and-ensuring-public-safety/
31. Gautam Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography," National Law School of India Review 26 (2014): 127–158.
32. (2019) 1 SCC 1.
33. Ibid, 359.
34. (2015) 5 SCC 1.
35. Ibid, 167.
36. Colin Snow, "Drones Pose a Unique Big Data Challenge For Business Users," Forbes, February 6, 2019, https://www.forbes.com/sites/colinsnow/2019/02/06/what-every-cio-needs-to-know-about-commercial-drone-data/#3d477aff89ba; Michelle Chan, "What Businesses Need to Know About Drone Data," Techwire Asia, February 13, 2019, https://techwireasia.com/2019/02/what-businesses-need-to-know-about-drone-data/
37. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules ((New Delhi: Ministry of Electronics and Information Technology, 2011)," https://meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf, Ibid. ; Rachel Finn and Anna Donovan, "Big Data, Drone Data: Privacy and Ethical Impacts of the Intersection Between Big Data and Civil Drone Deployments," in The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives, ed. Bart Custers (The Hague: TMC Asser Press, 2016), 47-67.

38. As Solove remarks about the "Information Age:" "The data gathered about people is significantly more extensive, the process of combining it is much easier, and the computer technologies to analyze it are more sophisticated and powerful." See Daniel Solove, "A Taxonomy of Privacy," University of Pennsylvania Law Review 154 (2006): 477, 506 ; Ibid., 507–08.

39. Jordi Soria-Comas and Josep Domingo-Ferrer, "Big Data Privacy: Challenges to Privacy Principles and Models." Data Science and Engineering 1 (2016): 21, 22. ; Justice KS Puttaswamy v. Union of India, (2017) 10 SCC 1.

40. Guide to Basic Data Anonymisation Techniques (Singapore: Personal Data Protection Commission of Singapore, 2018), www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf.

41. For a particularly stark situation, where the de-identification was considered near foolproof and yet re-identified, see Jean Louis Raisaro et al., "Addressing Beacon Re-Identification Attacks: Quantification and Mitigation of Privacy Risks," Journal of the American Medical Informatics Association 24 (2017): 799, 800.

42. Solon Barocas and Helen Nissenbaum, "Big Data's End Run around Anonymity and Consent," in Privacy, Big Data, and the Public Good, eds. Julia Lane et al. (New York, NY: Cambridge University Press, 2014), 44–45.

43. Ira S Rubinstein, "Big Data: The End of Privacy or a New Beginning," International Data Privacy Law 3 (2013): 74, 77–78; Davide Castelvecchi, "Can We Open the Black Box of AI?" Nature 538, no. 7623 (2016): 20.

44. Mireille Hildebrandt, "Defining Profiling: A New Type of Knowledge?" in Profiling the European Citizen: Cross-Disciplinary Perspectives, eds. Mireille Hildebrandt and Serge Gutwirth (eBook: Springer, 2008), 17, 20.

45. Nathaniel A Raymond, "Beyond 'Do No Harm' and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society's Use of Data," in Group Privacy: New Challenges of Data Technologies, eds. Linnet Taylor, Luciano Floridi and Bart van der Sloot (eBook: Springer, 2017): 67, 75.

46. A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (New Delhi: Ministry of Electronics and Information Technology, 2018),

47. Ibid, 45–46.

48. Ananth Padmanabhan and Anirudh Rastogi, "Big Data," in Regulation in India: Design, Capacity, Performance, eds. Devesh Kapur and Madhav Khosla (London: Hart Publishing, 2019): 251, 262.

49. Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," I/S Journal of Law and Policy, 4 (2008): 543, 565.

50. Arthur Allen Leff, "Contract as Thing," American University Law Review 19 (1970): 131.

51. Nikhil Narendran, "Policy Framework for Protection of Big Data in State Possession," in Blockchain for Property: A Roll Out Road Map for India, eds. Baladevan Rangaraju and Vishnu Chandra (New Delhi: India Institute, 2017): 34, 40.

52. Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (Noida: Harper Collins, 2018): 167–171.

53. Carmine Cifaldi, "Unmanned Aircraft System Privacy and Data Protection," in Handbook of Unmanned Aerial Vehicles, eds. K.P. Valavanis and G.J. Vachtsevanos (eBook: Springer, 2018): 1–19.

54. Voluntary Best Practices for UAS Privacy, Transparency, and Accountability (Washington, D.C.: National Telecommunications and Information Administration, 2016).