
# Technology Policy

Conference Material

**India Habitat Centre**
**4-6th December 2017**
**New Delhi, India**

Institute for
**New Economic Thinking**

**The Economics of Releasing the V-band and and E-band Spectrum in India** **5**

**Open data and digital identity: Lessons for Aadhaar** **49**

**An analysis of Puttaswamy: the Supreme Court's privacy verdict** **69**

**Why Having a Single Regulator Would Upset Indias Game of Drones** **73**

**Building blocks of Jio's predatory pricing analysis** **81**

**Predatory pricing and the telecom sector** **85**

**Emerging themes around privacy and data protection** **87**

**Competition issues in India's online economy** **91**

**TRAI's consultation towards a net neutrality framework in India** **95**

**India needs drones** **98**

**Towards a privacy framework for India in the age of the internet** **105**

# The Economics of Releasing the V-band and E-band Spectrum in India

December 2, 2017

**Suyash Rai**

**Dhiraj Muttreja**

**Sudipto Banerjee**

**Mayank Mishra**

National Institute of Public Finance and Policy, New Delhi

Broadband internet access in India is mainly mobile-based. This constrains the quality of access in terms of consistency, reliability and speed. Mobile broadband networks in dense urban environments are increasingly getting congested due to shortage of backhaul spectrum and challenges of laying fiber for backhaul. V-band and E-band spectrum can help partially overcome these problems. In this paper, we identify the main types of use cases for this spectrum, and estimate the potential scale of these uses in an optimised scenario. We also map these uses to the types of economic benefits that may flow from them. We recommend approaches to releasing the spectrum that enable widespread usage, and maximise the benefit to the society. We caution against approaches that front-load government revenue, but may impede usage, especially for innovative and risky applications.

# Contents


**1 Introduction** **2**

**2 Band characteristics** **2**
2.1 V-band spectrum . . . . . 2
2.2 E-band spectrum . . . . . 3

**3 Licensing approaches: international experience** **4**
3.1 Legal position on release of spectrum . . . . . 6
3.2 International experience for V-Band . . . . . 7
3.3 International experience for E-band . . . . . 8
3.4 Federal Communications Commission - USA . . . . . 9
3.5 Office of Communications (Ofcom) - UK . . . . . 11

**4 The present policy stance on E-band and V-band in India** **13**

**5 Unlicensed spectrum bands in India** **15**

**6 Research on economic impact of Internet and unlicensed spectrum** **16**
6.1 Economic impact of Internet in India . . . . . 16
6.2 Economic benefits of unlicensed spectrum . . . . . 18

**7 Broadband Internet in India** **21**

**8 Identifying the potential uses of V-band and E-band in India** **23**
8.1 Case study on use of the bands for improving connectivity . . . . 24
8.2 Proliferation of commercial Wi-Fi and Wi-Gig hotspots . . . . . 25
8.2.1 Deployment of commercial Wi-Gig hotspots . . . . . 28
8.3 Proliferation of fixed broadband connections . . . . . 28
8.4 Backhaul for mobile broadband . . . . . 31
8.5 Improvements in the quality of Internet access . . . . . 32
8.6 Other potential benefits . . . . . 34
8.6.1 Extension of local area networks between buildings . . . 35
8.6.2 Internet of Things . . . . . 35
8.6.3 Vehicle to vehicle communication . . . . . 36
8.6.4 Augmented Reality (AR)/Virtual Reality (VR) Systems . . 37

**9 Mapping the economic benefits arising from the use cases** **37**

**10 Conclusion** **41**

# 1 Introduction

Broadband internet users in India have been on the rise over the last decade and currently stand at more than 290 million subscribers.[1] As this number continues to increase, it is imperative for the supply side to be able to match consumer expectations. It is also important to ensure optimal usage of the spectrum to maximise economic benefits of this natural resource. So, as the government decides to release the presently unreleased spectrum, it should consider the overall economic impacts of the alternative strategies for releasing the spectrum. In this note, we consider the potential uses of both V-band (57 GHz - 64 GHz) and E-band (71 GHz - 86 GHz), as well as the economic benefits that may accrue from these uses. This analysis can help the government choose a suitable strategy for releasing spectrum in these bands.

This note begins with a brief overview of the characteristics of the bands. After that, we present a review of the approaches different countries have taken while releasing this spectrum, and a section on the present policy stance in India. This is followed by a section on policy thinking on unlicensed spectrum bands. After that, we delve into the economic aspects of this issue, beginning with an overview of studies on how internet has impacted the Indian economy, and studies from other countries on the economic benefits of unlicensed spectrum bands. This is followed by an analysis of the potential uses of the bands in India. We attempt to quantify the scale of these uses to the extent possible, based on benchmarking with global standards. In the penultimate section, we attempt to map the economic benefits that can accrue from different uses of these bands. The note concludes with a few key insights.

# 2 Band characteristics

## 2.1 V-band spectrum

Spectrum in the V-band (57 GHz - 64 GHz) can be used for high capacity transmissions over short distances. Using point-to-point or mesh topologies, the spectrum can be put to a variety of backhaul and access uses. The large bandwidth (7 GHz) in the band allows for wide channels in which data can be transmitted at high speeds. Further, since its propagation characteristics, especially high oxygen

[1] TRAI Press Release on Telecom Subscription Data (May 31, 2017). Available at: http://www.trai.gov.in/sites/default/files/Press_Release_No50_Eng_13072017.pdf

absorption, mitigate the level of interference, there is lesser need for active interference management. As the typical antenna beam-widths in this spectrum are less than five degrees, many links can be put in the same area just by having them point in slightly different directions. These features of the band were highlighted by TRAI in their recommendations on the allocation of these bands.

Since many countries have released this spectrum, there is now significant progress on development of technical standards, and manufacturing and sale of devices. The last few years have seen strong global momentum behind the IEEE 802.11 ad, or WiGig standard which also uses 60 GHz and is making available very low cost semiconductors and system solutions. More recently, a new standard 802.11ay has been defined, with specifications that can enable 100 Gbps communications through a number of technical advancements. Experience on usage of this spectrum in a variety of contexts is gradually accumulating. This is the right time for India to consider releasing this spectrum.

## 2.2 E-band spectrum

Like V-band, the E-band has large bandwidth (10 GHz) capabilities allowing transmission of high speed data over short distances (2 to 3 kms). E-band's frequencies are point to point and line of sight radio waves. These unique transmission properties of very high frequency millimeter waves enable simpler frequency coordination, interference mitigation and path planning compared to lower frequency bands.[2]

E-band uses antennas which are highly directional and this coupled with the propagation limitations allows for highly focussed point to point "pencil-beam" links allowing for much higher frequency reuse in a given area. As of August 2014, more than 40 countries have come up with license plans for E-band.[3] There are some licensing exceptions, but most of the world follows a lightly licensed regime for E-band.

Although the E-band does not have the oxygen absorption characteristics of V-band, the availability of large spectrum allows for wider channels that can have potential uses in last mile connectivity. This spectrum band has a longer distance range as well as better weather characteristics, which make it a good frequency for backhaul usage. Both the ITU and CEPT have provided detailed channel plans

[2] TRAI, Recommendations on Allocation and Pricing of Microwave Access (MWA) and Microwave Backbone (MWB) RF carriers, 29th August 2014.

[3] Ibid

| Individual authorisation (Individual rights of use) | | General authorisation (No individual rights of use) | |
|---|---|---|---|
| **Individual licence** | **Light-licensing** | | **Licence-exempt** |
| Individual frequency planning / coordination<br>Traditional procedure for issuing licences | Individual frequency planning / coordination<br>Simplified procedure compared to traditional procedure for issuing licences<br>With limitations in the number of users | No individual frequency planning / coordination<br>Registration and/or notification<br>No limitations in the number of users nor need for coordination | No individual frequency planning / coordination<br>No registration nor notification |

**Figure 1:** Regulatory options for spectrum licensing
Source: ECC Report 132

for this band and its use has also been considered in India's National Frequency Allocation Table (NFAP) 2011.[4]

# 3 Licensing approaches: international experience

Before diving into the types of license regimes followed, it is important to understand the difference between individual and general authorisation.

As per the ECC report 132 (Article 5.1 of the Authorisation Directive), usage of radio frequencies where risk of harmful interference is negligible, should not be subject to grant of individual rights of use, and should instead have conditions of usage under general authorisation. This means that general authorisation should be used as the overarching framework, when coordination between users is not necessary. The license structures under the two types of authorisation is presented in figure 1.

1. *Individual licensing* - This is the conventional link-by-link coordination, usually made under an administration's responsibility; sometimes, the administration delegates this task to the operators, but it keeps control of the national and cross-border interference situation.[5] The likelihood of significant interference with the use of both these bands would be low and as such individual licensing or link-by-link coordination may not be the

[4]TRAI, Recommendations on Allocation and Pricing of Microwave Access (MWA) and Microwave Backbone (MWB) RF carriers, 29th August 2014.

[5]ETSI, E-Band and V-band - Survey on status of worldwide regulation, June 2015

best approach going forward.

2. *Light licensing* - It is a combination of license-exempt use and protection of users of spectrum. This model typically has a 'first come first served' feature where the user notifies the regulator with the position and characteristics of the stations. The database of installed stations containing appropriate technical parameters is publicly available and should thus be consulted before installing new stations.[6] Figure 1 shows how light licensing is different under an individual authorisation structure and a general authorisation structure, with no individual coordination required under the latter. In practice, the general features of light licensing can be enumerated as follows:
   (a) For installing a new link, the regulator must be informed. There is generally a database available to view all installed links.
   (b) Licensing fees tend to be low.
   (c) Provides a first come first serve protection, in the sense that if two links are installed in one location, and there is interference between the two, in such a case the link installed first is protected and the second link will be reconfigured or removed to prevent interference.
3. *License exempt* - This method offers the most flexible and low cost usage, and is more popular in specific bands (e.g. 2.4 and 5.8 GHz) where short range devices are allocated, but fixed service applications may also be accommodated. Although this does not guarantee any interference protection by the regulator, it should be noted that alternate interference management techniques are available today to deal with the issue. Some of these include cloud based routing through mesh, single frequency network, listen-before-talk and multi-antenna signal processing.
4. *Block assignment regimes* - Under this regime, assignment is made through renewable licensing or through permanent public auctions, or through other allocation mechanism. This is most common when fixed wireless access (point to multi-point) is concerned and the user is usually free to use the block in the best possible way to deploy its network. For some frequency bands this method is considered the best compromise between efficient spectrum usage and flexibility for the user.[7] The deployment of E-band and V-band is likely to see more P-MP links.

Different countries evaluate their markets and eco-systems differently and there is no uniform licensing approach towards spectrum. In the following sections, we review the general licensing framework implemented globally under both of these bands. However, a question that needs to be addressed in India's context is: does

[6] As defined by the ECC Report 80(25)

[7] ETSI, E-Band and V-band - Survey on status of worldwide regulation, June 2015

the legal framework allow any approach other than auctioning the spectrum?

## 3.1 Legal position on release of spectrum

It is relevant for our paper to discuss the impact of the 2G case[8] which would be considered by the Government, whenever it decides to release spectrum. In this case, the Supreme quashed several spectrum licenses granted to telecom service providers due to irregularities in the manner of allocation of spectrum to licensees on first-come-first-served basis. The Court observed that a duly publicised auction, conducted fairly and impartially, is perhaps the best method for discharging the burden of alienating scarce public resources like spectrum, etc as opposed to first-come-first-served basis which is likely to be misused. The Court was of the view that while transferring or alienating the natural resources, the State is duty-bound to adopt the method of auction by giving wide publicity so that all eligible persons can participate in the process.[9]

The Central Government filed a review petition that was later withdrawn. Thereafter, the Government moved the Supreme Court with a Presidential Reference[10] for its opinion on issues arising out of its 2G case. The clarification was sought, inter alia, on: whether auction is the only methodology to be adopted by the Government for alienation of all public resources in the country. The Supreme Court exercised its advisory jurisdiction and clarified that the law laid down in 2G case was limited to the facts of that case i.e., distribution of spectrum where the "Court evaluated the validity of the methods adopted in the distribution of spectrum from September 2007 to March 2008". The Court further observed, "Auction as a mode cannot be conferred the status of a constitutional principle. Alienation of natural resources is a policy decision, and the means adopted for the same are thus, executive prerogatives....However, when such a policy decision is not backed by a social or welfare purpose, and precious and scarce natural resources are alienated for commercial pursuits of profit maximising private entrepreneurs, adoption of means other than those that are competitive and [will] maximise revenue may be arbitrary and may face the wrath of Article 14 [equality before law]"

On the methodology, the Supreme Court noted, "...is clearly an economic policy. It entails intricate economic choices and the court lacks the necessary expertise to make them. It cannot, and shall not, be the endeavour of this court to evaluate

[8] See, Centre for Public Interest Litigation and Others. V. Union of India (2012) 3 SCC 1.
[9] Ibid.
[10] Re: Special Reference No. 1 of 2012.

the efficacy of auction vis-a-vis other methods. The court cannot mandate one method to be followed in all facts and circumstances. Therefore, auction, an economic choice of disposal of natural resources, is not a constitutional mandate."

The court in its opinion also stated that auction method may also suffer from problems and mere likelihood of abuse of any alienation method does not vitiate it unless there are actual problems. It was clarified that it is the prerogative of the Government to decide the methodology of alienation of other public resources, provided the method is transparent, fair and backed by social or welfare purpose. The Court also discussed about revenue maximisation theory and stated that this need not be the sole objective while alienation public resources and in fact this is subservient to the goal of serving common good of the society.

Auction is not the only option to alienate all public resources of the country. The key is to ensure that the method spectrum release should have a social or welfare purpose, and should not arbitrarily benefit certain parties.

As far as the question of releasing the V-band and E-band spectrum is concerned, the Government in the past has unlicensed spectrum (Wi-fi frequency) which yielded several benefits for the Indian economy. Moreover, globally the microwave bands like V-band and E-band have been either delicensed or subjected to light touch licensing. As long as it is clear that a given method of releasing the spectrum would maximise social benefits, and would not arbitrarily benefit anyone, it will probably withstand judicial scrutiny.

## 3.2 International experience for V-Band

A number of countries all over the world have adopted license free-frameworks for adopting the 60 GHz band. Table 1 indicates some of these along with the year in which they were adopted.[11]

These countries have seen benefits in going for a license free regime and the fact that the license structure has not changed in recent times seems to be a sign of the existing structure working. While both the European Commission and the Federal Communications Commission (FCC) have made recent policy changes in the power level ranges for short-range devices (applicable to V-band), the overall license free structure has been maintained.

Singapore, is an example of a country with a licensed 60 GHz regulatory environment, for outdoor links. The rationale for such decision is based on the concern

[11]The database reporting this information is available at http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp9_e_band_and_v_band_survey_database.zip

**Table 1:** Timeline V-band adoption

| Country | Year of adoption |
|---|---|
| Belgium | 2014 |
| Canada | 2010 |
| China | 2015 |
| Japan | 2014 |
| Korea | 2013 |
| Malaysia | 2015 |
| Philippines | 2016 |
| Poland | 2014 |
| Slovakia | 2015 |
| Switzerland | 2011 |
| UK | 2010 |
| US | 2010 |

that being a highly dense urban environment, it was prudent to regulate the location of high powered links to ensure that there is no interference between band receivers. No licensing restrictions have been placed on low power band devices, which are more suitable for indoor environments.

## 3.3 International experience for E-band

Many countries have decided to open up the 71-76 and 81-86 GHz ITU frequencies for ultra high capacity point to point communications. Countries have recognised that licensing fees based on the amount of data transmission or bandwidth usage may result in extremely high tariffs that can have a detrimental effect on the adoption of these bands. As such, most regulators have decided to adopt the "light license" approach when regulating this band. Some of the countries that have opened up this spectrum are represented in table 2.[12]

Both the FCC in the United States and the OfCOM in the United Kingdom were among the early adopters of these bands. In the following section, we take a deeper look at the respective approaches taken towards regulating the use of these bands.

[12]E-band communications, Licensing and License Fee Considerations for E-band 71-76 GHz and 81-86 GHz Wireless Systems

**Table 2:** E-band adoption and price

| Country | License structure | License fee |
|---|---|---|
| USA | Online light license | $75 - 10 year license |
| UK | Light license | 50 pounds per year |
| Czech Republic | Unlicensed | Free of charge |
| Russia | Light license | Minimal registration fee |
| Australia | Light license | AU$187 per year |
| UAE | Traditional PTP | 4,500 Dirhams per year |
| Ireland | Traditional PTP | 952.30 Euros per year |
| Jordan | Traditional PTP | JD200 per year |
| Bahrain | Traditional PTP | 1% of generated link revenue |

## 3.4 Federal Communications Commission - USA

### V-band

FCC has been working to delicense spectrum to promote wireless connectivity and other innovative uses (like RFID) which can have industrial, scientific and medical applications. Users can operate without an FCC license, any spectrum designated as "unlicensed" or "license-exempt". The Commission permits the operation of radio frequency (RF) devices within the band of (57 GHz - 71 GHz) without an individual license from the Commission or the need for frequency coordination.[13] This exemption, is however, not applicable if the equipment is being used on aircrafts or satellites, field disturbance sensors, including vehicle radar systems, unless the field disturbance sensors are employed for fixed operation, or used as short-range devices for interactive motion sensing. Further, the operators must use certified radio equipment and comply with the technical requirements, including power limits, limits on spurious emissions, etc. as stated in FCC's Part 15 Rules. Users of the license-exempt bands do not have exclusive use of the spectrum and are subject to interference. The technical standards for Part 15 are designed to ensure that there is a low probability that these devices will cause harmful interference to other users of the spectrum.[14]

The primary operating conditions are that the operator of a device must accept whatever interference is received and must correct whatever harmful interference is caused. Should harmful interference occur, the operator is required to

[13] 47 C.F.R. part 15 "Radio Frequency Devices" (15.255). Available at https://www.law.cornell.edu/cfr/text/47/15.255

[14] FCC, Notice of Inquiry, In the Matter of Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Systems, August 20, 1998.

immediately correct the interference problem, even if correction of the problem requires ceasing operation of equipment causing interference.[15]

In the US, WirelessHD and WiGig commonly use the 60 GHz unlicensed band to achieve multi-gigabit data transfer over the range of a few meters. Applications of these technologies include home entertainment, data networking and wireless docking.[16] In the US, an interesting study was conducted that dispelled some common myths on 60 GHz outdoor mobile communication, to establish that outdoor 60 GHz picocells[17] can augment existing cellular networks and have the potential to deliver orders of magnitude increase in network capacity.[18]

### E-band

On October 16, 2003, the FCC adopted a Report and issued an Order establishing service rules to promote the private sector development and use of the spectrum in the 71-76 GHz, 81-86 GHz,(E-band frequencies) and 92-95 GHz bands.[19] In 2005, this order was subsequently modified by the Memorandum Opinion and Order issued by FCC.[20] FCC adopted a *light licensing* framework for the E-band that does not require separate FCC license applications for most links or traditional frequency coordination among non-Federal Government users. A license to operate a link in the E-band spectrum consists of two parts - *a non-exclusive nationwide license combined with registration of each link.*[21]

First, an interested party has to obtain nation wide non-exclusive license from the FCC. Once approved, the licensee can register for any number of individual

[15] 47 C.F.R. § 15.5 General conditions of operation. Available athttps://www.law.cornell.edu/cfr/text/47/15.5

[16] Milgrom et al, The Case for Unlicensed Spectrum, 2011. Available at https://web.stanford.edu/~jdlevin/Papers/UnlicensedSpectrum.pdf

[17] A picocell is a small cellular base station typically covering a small area, such as in-building (offices, shopping malls, train stations, stock exchanges, etc.), or more recently in-aircraft. In cellular networks, picocells are typically used to extend coverage to indoor areas where outdoor signals do not reach well, or to add network capacity in areas with very dense phone usage, such as train stations or stadiums.

[18] Zhu et al, Demystifying 60GHz Outdoor Picocells. Available at https://www.cs.ucsb.edu/~ravenben/publications/pdf/60pico-mobicom14.pdf

[19] Federal Communication Commission, Millimeter Wave 70/80/90 GHz Service. Available at https://www.fcc.gov/wireless/bureau-divisions/broadband-division/millimeter-wave-708090-ghz-service

[20] Federal Communication Commission, Memorandum Opinion and Order, March 3, 2005. Available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-05-45A1.pdf

[21] Federal Communication Commission, Millimeter Wave 70/80/90 GHz Service. Available at https://www.fcc.gov/wireless/bureau-divisions/broadband-division/millimeter-wave-708090-ghz-service

E-band links in the US and its territories. The non-exclusive nationwide license does not authorise operation until the link is registered as an approved link in the *Link Registration System* which is administered by three FCC-selected third party database managers. The band manager then undertakes a four-step automated analysis of the link. The licensee may use the E-band for any point-to-point, non-broadcast service. There is no limit to the number of non-exclusive nationwide licenses that may be granted for this band. The license term is ten years, beginning on the date of the initial authorisation (nationwide license) grant. Registering links will not change the overall renewal period of the license. License fee is USD 75 for a 10 year license.[22]

The applicant has to provide interference analysis to the third-party database manager to establish that the potential for harmful interference to or from all previously registered non-government links has been analysed according to the prescribed standards in the Code of Federal Regulations and generally accepted good engineering practice.[23] Further, the analysis must show that the proposed non-government link will not cause harmful interference.[24]

Further, since the 70/80/90 GHz bands are allocated on a shared basis with Federal Government users, each link must be coordinated with the National Telecommunications and Information Administration (NTIA) with respect to Federal Government operations as part of the registration process.[25]

## 3.5 Office of Communications (Ofcom) - UK

### V-band

Ofcom has opened the spectrum in the 59-64 GHz band for fixed point to point wireless systems (FWS) and combined this with the 57-59 GHz band under one overall licence exempt authorisation approach for FWS. This decision created one contiguous and flexible block of spectrum providing 6.8 GHz of available bandwidth (57.1-63.9 GHz) taking into account two 100 MHz guard bands.[26] The

[22] See, US Title 47, CFR Part 101. 1501 Chapter 1, available at https://www.gpo.gov/fdsys/pkg/CFR-2013-title47-vol5/pdf/CFR-2013-title47-vol5-part101-subpartQ.pdf

[23] Ibid.

[24] Ibid.

[25] Federal Communication Commission, Millimeter Wave 70/80/90 GHz Service. Available at https://www.fcc.gov/wireless/bureau-divisions/broadband-division/millimeter-wave-708090-ghz-service

[26] Release of the 59 – 64 GHz band, December 11, 2009. Available at https://www.ofcom.org.uk/consultations-and-statements/category-1/59_64ghz/statement

60 GHz band has been available for FWS on a licence exempt basis across the UK, with the exception of three small geographical areas to protect Ministry of Defence radio location systems against likely harmful interference.

The UK has one of the highest densities of Wi-Fi networks in the world. A 2012 survey by Strategy Analytics found that 73.3% of UK households have a home Wi-Fi network, a proportion second only to South Korea. The UK also leads Europe in the deployment of public Wi-Fi hotspots. This goes on to define the market for license exempt radio devices in the U.K. The IEEE 802.11ad standard, sometimes referred to as Wi-Gig, effectively caters for Wi-Fi type deployments in this band and has recently been formally adopted by the Wi-Fi Alliance, with suggested applications including cable replacement for displays, wireless docking between devices like laptops and tablets, instant data synchronisation and backup and simultaneous streaming of multiple, ultra-high definition and 4K videos.[27] There have been reported utilisations of 63-64 GHz band in road traffic communication.[28] Further, UK has explored use of V-band for vehicle to vehicle communication links.[29]

## E-band

In March, 2007 after substantial public consultation, Ofcom allowed a new class of license 'Self Coordinate Links' for operation in E-band frequencies. Similar to US, UK has also adopted a *light licensing* approach for E-band spectrum which can be used for point to point wireless communications. The licence fee is £50 Pounds which includes the charge for registration of the first link for the first year of the licence. Any further links registered by the licensee is charged at £50 Pounds per link per year. An applicant has to first obtain non-exclusive national licences. Thereafter, a licensee may register point to point fixed wireless links in the UK, through a link registration process administered by Ofcom.[30]

Ofcom follows a *first come first served basis* wherein it provides date and time

[27]UK Spectrum Policy Forum, Future use of Licence Exempt Radio Spectrum. Available at http://www.plumconsulting.co.uk/pdfs/Plum_July_2015_Future_use_of_Licence_Exempt_Radio_Spectrum.pdf

[28]Radio Systems at 60GHz and Above, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0018/44811/radio60ghzreport.pdf

[29]Vehicle to vehicle communication outage and its impact on convoy driving. Available at https://eprints.soton.ac.uk/75222/

[30]See, Ofcom, Guidance Notes for Self Co-ordinated Licence and Interim Link Registration Process in the 64-66 GHz, 73.375-75.875 GHz and 83.375-85.875 GHz bands. Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0021/84018/ofw_369_guidance_notes_65_70-80ghz_final.pdf

record to each link on the register. This record is used to establish priority within the band for interference purposes. A link with a date time record will have priority over links registered later. If a new link is likely to cause interference to an existing link, the licensee of the new link should coordinate with the existing licensee in order to avoid interference. In the event where this is not possible, the new link should not be registered. If the link is registered, the later link will be removed from the register if an interference complaint is received by Ofcom. The interference assessment between registered links and new links is the responsibility of the licensees. Ofcom does not conduct interference assessments.[31]

In 2013, after extensive stakeholder engagement, Ofcom adopted a new licensing approach with respect to E-band frequencies. The consultation process revealed growing perception among stakeholders that current self-coordinated approach did not offer the certainty required for the high availability (above 99.99%) applications, specifically for supporting 4G networks. Therefore, Ofcom decided to change the former regime on management and authorisation approach with respect to E-band frequencies to provide a balance between the different user communities and sufficient interference management assurance for those stakeholders wishing to deploy high availability.[32] The current position is a double regime where the band is sub-divided into two parts, the lower segment of 2 GHz regulated as fully Ofcom coordinated (link-by-link) and the upper segment of 2.5 GHz part remains self-coordinated (light licensing) as per the previous policy.[33]

# 4 The present policy stance on E-band and V-band in India

The TRAI has been exploring the use of millimeter wave bands such as E-Band and V-band since 2014. In its recommendations on *Allocation and Pricing of Microwave Access (MWA) and Microwave Backbone (MWB) RF carriers* dated 29th August 2014, TRAI recommended that:

- *...in order to increase broadband penetration in India, the usage of high capacity backhaul E-band (71-76 / 81-86 GHz) and V-band (57-64MHz) may be explored for allocation to the telecom service providers.*

[31] Ibid.

[32] Ofcom Consultation on the future management approach for the 70 / 80 GHz bands, August 2013. Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0029/46775/condoc.pdf

[33] Ofcom, Review of the Spectrum Management Approach in the 71-76 GHz and 81-86 GHz bands, August 2013. Available at, https://www.ofcom.org.uk/consultations-and-statements/category-2/70-80ghz-review

- *... both E-band and V-band should be opened with 'light touch regulation' and allotment should be on a 'link to link basis'. The responsibility for registration and database management should lie with WPC wing of DoT. For this purpose, WPC should make necessary arrangements for an online registration process by developing a suitable web portal. Responsibility for interference analysis should rest with the licensee, who needs to check the WPC link database prior to link registration (links should be protected on a "first come, first served" basis). WPC can also maintain a waiting list for the same spot.*

Subsequently, in its recommendations on *Delivering broadband quickly: What do we need to do?* on 7th April 2015, TRAI stated that most countries have already de-licensed the 60 GHz band(V-band or WiGig band using 802.11ad) and this band has a good device ecosystem; India should also de-license the 60 GHz band immediately and make it available for consumers.

In October 2015, the Department of Telecommunications (DoT) asked for some clarity on the licensing as well as prices recommended by TRAI in its recommendations on *Allocation and Pricing of Microwave Access (MWA) and Microwave Backbone (MWB) RF carriers*. TRAI issued a response to DOT's reference in November 2015, wherein TRAI specified that for V-band a light touch regulation may only be required for backhaul applications, also stating that the V-band be unlicensed for both indoor and outdoor access applications. The Authority recognised the importance of both bands in the proliferation of broadband through Government/Public Private Partnerships (PPP) enabled hotspots in public spaces. The Authority also cited the congestion of the existing Wi-Fi bands as one of the reasons for the need to explore alternatives.

While access applications need not be monitored, the Authority said that for V-band, light touch regulation should be in place for backhaul applications, mainly for the purpose of interference management. Such management would lie in the hands of the licensee who would need to verify the existing databases before setting up a backhaul link in this frequency. The Authority also made reference to stakeholder comments during the consultation process, which said that a number of countries world over have liberalised sections of the V-band in an unlicensed manner for both access and backhaul, and that India should follow suit.

In its recent recommendations on *Proliferation of broadband through public wi-fi networks* dated 9th March 2017, the Authority has reiterated its previous recommendations asking for the Government to expedite the process of allocating E-band and V-band in India.

# 5 Unlicensed spectrum bands in India

It is often assumed that licensing the spectrum, especially through an auction process, helps allocate the spectrum to those who are most likely to use the spectrum efficiently. This argument underpins the auction-based approach to spectrum allocation in India and other countries. However, in most countries, it has been acknowledged that certain spectrum bands are best left unlicensed, or may be subjected to a "light touch" licensing regime, with minimal regulation. The International Telecommunication Union (ITU), European Union telecom regulatory bodies, as well as leading state telecom policy makers and regulators such as the FCC and Ofcom have recognised that the optimal use of radio spectrum is dependent on flexible spectrum management policies and the multi-time sharing of this precious resource.

As of now, a number of spectrum bands are in unlicensed in India. These include: 2.4 GHz and 5.8 GHz spectrum bands used for Wi-Fi access; 865 MHz - 867 MHz band used by RFID devices; 402 MHz - 405 MHz spectrum band used for medical wireless devices; 335 MHz for remote control of cranes; and so on. In the National Telecom Policy, 2012, one of the strategies for spectrum management is:

> *....To identify additional frequency bands periodically, for exempting them from licensing requirements for operation of low power devices for public use.*

The experience of unlicensed spectrum bands suggests that it is difficult to predict in advance what kinds of applications the spectrum will be used for. For example, RFID spectrum has generated huge economic benefits in the retail sector - the scale of which could not have been predicted in advance. Later in this note, we present findings from some studies that show the scale of economic benefits from unlicensed spectrum.

One of the major concerns around use of unlicensed spectrum tends to be interference management, and a possible solution here tends to be the use of interference free spectrum which drives short range connectivity. Technological advancements such as Wireless Local Area Network (WLAN), Ultra Wide Band (UWB), Radio Frequency Identification (RFID), Near-Field Communication (NFC) systems, and others have demonstrated that when an opportunity for cost-efficient and flexible spectrum usage is presented in the form of unlicensed spectrum, the market is likely to respond through innovation and expansion.[34] Further, because of development of technological solutions for interference management, the regulatory role in this has been reduced. Still, it is important for regulators to specify and

[34]CIS, Unlicensed Spectrum Policy Brief for Government of India. Available at http://cis-india.org/telecom/unlicensed-spectrum-brief.pdf

enforce technical standards to ensure that devices used are not leading to unfair interference.

In a country like India, unlicensed spectrum can play a big role in bridging the digital divide. However, the country is still behind when compared to unlicensed spectrum availability in the U.S. and UK which have already integrated innovative spectrum management techniques in their telecom policies. These policies aim to create a flexible, market-driven approach to spectrum regulation and management through integrating spectrum sharing techniques and meeting the industry demand for unlicensed spectrum.

# 6 Research on economic impact of Internet and unlicensed spectrum

The strategy for releasing a spectrum band should comprehensively consider the consequences of the alternative approaches. To understand the potential economic impact of these spectrum bands in India, we can draw lessons from two types of studies. First, since one of the main impacts of these bands is improved access to high speed Internet (discussed later), studies on economic impact of Internet are useful. Even if precise monetary value of such impact is difficult to estimate, these studies can help give an understanding of the range of such impact. Second, there are studies on economic impact of unlicensed spectrum that can help understand how leaving a spectrum unlicensed or lightly licensed can lead to economic benefits that might not have accrued had the spectrum been more strictly licensed.

## 6.1 Economic impact of Internet in India

Two types of studies on the economic impact of Internet in India have been conducted.

- *Studies on the economic impact of marginal increase in Internet penetration:* Typically, such studies estimate the percentage impact on GDP growth resulting from marginal increase in the number of subscribers. This impact includes not just the increase in the Internet economy, but also the externalities of Internet.
  A 2012 study by ITU presented an overview of the variety of impacts of

broadband deployment.[35] For India, the study found that every 10 percent increase in broadband penetration was leading to 0.31 percent increase in the GDP of the respective region.[36] A 2012 study published by Kathuria et al from Indian Council for Research on International Economic Relations (ICRIER) estimated that every 10 percent increase in the number of Internet subscribers was leading to 1.08 percent increase in a state's GDP.[37]
In a similar study published in 2016, Kathuria et al use a modified growth multiplier method to estimate the economic impact of Internet.[38] They find that a 10 percent increase in Internet subscribers results in an increase of 2.4 percent in the growth of state's per capita GDP. The most recent study, published in 2017, found that 10 percent increase in India's total Internet traffic delivers on average a 3.3 percent increase in India's GDP.[39]
Usually, the rising penetration of Internet enables its application to an increasing variety of services. This is consistent with the intuition of network economics, which suggests that as the economy gets better networked, the economic benefits from access to Internet should increase. The famous Metcalfe's Law proposes that the value of a network is proportional to the square of the number of users. So, each additional user adds higher value than the previous user. This might be the reason why more recent studies find greater economic impact of marginal increase in internet penetration. These studies suggest that the marginal economic impact of increased Internet access is accelerating. This is also consistent with the finding presented in various studies, including the ITU study referenced above, that the economic impact of marginal increase in Internet access is higher for countries that are already well-networked.

- *Studies on the contribution of the Internet to the economy:* Such studies estimate the contribution of Internet to India's GDP. These studies usually include only the direct contribution of the internet. McKinsey and Company, 2012 estimated that the Internet contributed about 1.6 percent to India's GDP.[40] They contrasted this with the average contribution of the Internet in

[35]Katz, Raul. "The impact of broadband on the economy: Research to date and policy issues." Broadband Series. 2012. Available at: https://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf

[36]It is worth noting that although the study found the coefficient to be statistically significant, there is a risk of potential endogeneity, which means that it is possible that the causal relationship between broadband penetration and GDP growth runs in both directions. The study's methodology may not have sufficiently overcome this problem.

[37]Kathuria, Rajat, and Mansi Kedia-Jaju. India, the Impact of Internet. ICRIER, 2012.

[38]Kathuria, Rajat, et al. "Quantifying the Value of an Open Internet for India." ICRIER. 2016.

[39]Kathuria, Rajat, Mansi Kedia, Gangesh Sreekumar Varma, and Kaushambi Bagchi. "Estimating the Value of New Generation Internet Based Applications in India." 2017.

[40]Gnanasambandam, Chandra, et al. "Online and upcoming: The Internet's impact on India."

developed countries, which was estimated to be 3.4 percent. The study used data from 2010. A 2015 report by the Boston Consulting Group estimated that in 2013, the Internet contributed 2.7 percent to India's GDP.[41] The report projected that this contribution would grow to 4 percent of the GDP by 2020.

Kathuria et al, 2016, use national accounts (expenditure) data as well as growth multiplier method to estimate the economic value of Internet for India.[42] They estimate the aggregate expenditure on the Internet in India to be between 2.2 percent and 4.8 percent of GDP. The upper bound is the estimate if both connectivity and the Internet are considered. Using the growth multiplier method, the study estimates the value of the Internet to be 3.38 percent of the nominal GDP.

These studies cannot be directly compared, because they use different methodologies. However, if their conclusions are considered chronologically, they suggest that the direct contribution of Internet to the economy has been growing.

To the extent the use of V-band and E-band leads to cheaper, broader and better quality access to Internet, it could lead to acceleration in GDP growth, and also increase the GDP contribution of the Internet. The pathways and scale of these impacts depend on the specific uses of the spectrum, which are discussed later. The key findings from the studies on the economic impact of Internet in India are summarised below.

## 6.2 Economic benefits of unlicensed spectrum

Although there are no studies estimating the economic benefits of unlicensed spectrum bands in India, studies have been conducted in other jurisdictions. Here, we have focused on studies in one country - the United States of America - for ease of comparability across studies. The studies are:

- *Thanki, 2009:*[43] this study estimated the benefits from residential Wi-Fi, hospital Wi-Fi and RFID technology.

Technology, Media and Telecom Practice,Mc Kinsey and Company (2012).

[41] Shah, Alpesh, Nimisha Jain, and Shweta Bajpai. "India@ digital." Bharat Creating a USD 200 billion Internet economy. BCG Group publication, AIMAI. 2015. Available at:http://company.mig.me/wp-content/uploads/2015/09/bcg-report-on-Indian-Internet.pdf

[42] Kathuria, Rajat, et al. "Quantifying the Value of an Open Internet for India." (2016). Available at http://icrier.org/pdf/open_Internet.pdf

[43] Thanki, Richard. "The economic value generated by current and future allocations of unlicensed spectrum." Perspective Associates. 2009.

- *Milgrom et al, 2011:*[44] this study estimated the benefits from mobile offloading, residential Wi-Fi, and Wi-Fi tablets. However, in estimating the benefits from mobile offloading, it only included consumer surplus and benefits from higher speed. It did not consider producer surplus and benefits that may emerge from new business revenue.
- *Cooper, 2012:*[45] this study focused on benefits from mobile offloading, and use of residential Wi-Fi. Contrary to Milgrom et al, 2011, while estimating the benefits of mobile offloading, this study only includes producer surplus, and leaves out consumer surplus, benefits from higher speed, and other benefits.
- *Thanki, 2012:*[46] this study estimates benefits from mobile offloading and use of residential Wi-Fi.
- *Katz, 2014:*[47] this is the most comprehensive study. It focuses on public Wi-Fi, residential Wi-Fi, mobile offloading, Wi-Fi tablets, RFID technology, and innovative business models, such as bluetooth products.

Understanding the different types of impact of unlicensed spectrum bands from these studies can help us identify the pathways of economic benefit from V-band and E-band. Table 3 summarises the findings of these studies (we have adjusted the estimates for inflation for the time since the studies were conducted).

An interesting insight from these studies is that some of the biggest economic benefits of unlicensed spectrum may come from real economy uses that are difficult to predict in advance. The use of RFID in clothing and healthcare sectors contributes more than half of the estimated economic benefits of unlicensed spectrum in USA. These sectors have used this spectrum to improve their processes, and this has yielded rich returns.

There are no similar studies on V-band or E-band spectrum. So, the methodological choices must be made with little support from existing studies. Also, since the deployments of these bands in other countries are still small in scale, there is not enough experience to learn from. So, our focus is on identifying the categories of benefits, and quantifying them. For the most part, we desist from monetising the benefits. We leave that to a later date, when more experience has accumulated, and data availability is less constrained.

[44] Milgrom, Paul R., Jonathan Levin, and Assaf Eilat. "The case for unlicensed spectrum." 2011.

[45] Cooper, Mark. "Efficiency gains and consumer benefits of unlicensed access to the public airwaves." 2012.

[46] Thanki, Richard. "The economic significance of licence-exempt spectrum to the future of the Internet." White Paper. 2012.

[47] Katz, Raul L. "Assessment of Current and Future Economic Value of Unlicensed Spectrum in the United States." 2014.

**Table 3:** Economic benefits of unlicensed spectrum in USA (figures in USD Billion)

| Benefit | Thanki (2009) | Milgrom et al (2011) | Thanki (2012) | Cooper (2012) | Katz (2014) |
|---|---|---|---|---|---|
| Wi-Fi mobile offloading | NA | 39.6 | 8.9 | 48.4 | 16.3 |
| Residential Wi-Fi | 4.81 - 14.1 | 13.5 | 16.3 | 40 | 37.31 |
| Wi-Fi only tablets | NA | 16 | NA | NA | 44.4 |
| Hospital Wi-Fi | 10.7 - 18 | NA | NA | NA | NA |
| Clothing RFID | 2.24 - 9.1 | NA | NA | NA | 98.25 |
| Wireless Internet service providers | NA | NA | NA | NA | 1.5 |
| Wireless personal area networks | NA | NA | NA | NA | 2.25 |
| Health care RFID | NA | NA | NA | NA | 37.3 |
| Total | 17.75 - 41.2 | 69.1 | 26.2 | 88.4 | 237.31 |

# 7 Broadband Internet in India

The context of broadband Internet in India will determine the kinds of benefits that India can get from V-band and E-band. The following are a few key facts about broadband Internet in India.

- *Reliance on mobile broadband:* In India, most users access broadband Internet through mobile broadband. As on May 31, 2017, wired connections comprised only 6.3 percent of the broadband connections. The trend also seems to be towards greater reliance on mobile broadband. The density of wired broadband connections in India is 1.4, while the average for OECD countries is 29.8.[48] World average is about 11.6 fixed broadband subscriptions per 100 inhabitants.
  This shows how much India deviates from the global norms in terms of its reliance on mobile broadband. Many other countries also rely significantly on mobile broadband, but almost all of these countries have much lower population density and fewer densely populated urban areas. This may be the reason why wired connections are considered less feasible in those countries. So, India's disproportionate reliance on wireless connections is unique when compared to countries with similar population density.
  Although India has managed to rapidly expand access to broadband using mobile broadband, this approach has certain limitations:
  - *Mobile broadband congestion:* In densely populated areas, as more people get on to wireless broadband, the mobile spectrum bands may get congested. This was experienced in the 3G spectrum bands - as more people started using the spectrum band, congestion increased. This necessitates more cell sites and higher backhaul speeds.
  - *Constraints on speed and consistency of connection:* Compared to wired connections, especially fiber optic connections, mobile broadband provides lower speeds and less consistent connectivity. High speed, consistent connectivity is crucial for high quality usage at homes and offices. Wireless Internet on mobile devices is necessary only while using Internet in transit and outdoors.
  - *Low potential for community hotspots:* If density of wired connections remains low, this will constrain the potential of developing community hotspots, where residential or business hotspots are made available for use by other users of the network. The proliferation of such hotspots is one of the most remarkable stories in the growth of Internet in recent years. Globally, community hotspots have grown from 19.38

[48] This is available at: http://www.oecd.org/sti/broadband/oecdbroadbandportal.htm

million in 2013 to 251 million in 2017. Such hotspots provide high speed, consistent connectivity, while offloading from mobile networks - a benefit that India will not be able to realise without proliferation of fixed broadband connections.

Since India is already making considerable progress on mobile broadband, it is worth considering how it could expand access to high speed fixed broadband Internet, which complements mobile broadband.

- *Relatively lower use of higher speed fixed broadband connections:* A negligible percentage of the fixed broadband connections are fibre optic-based. Most of the wired connections use DSL, Dial-up, or Ethernet, all of which offer potentially lower speeds than fibre optic. This situation is very different from what is seen in developed countries, and also in comparable developing countries. From the fixed Internet connections in India, about 62 percent are DSL-based; 14.7 percent are dial-up connections; 13.96 percent are Ethernet/LAN connections, and 6.9 percent are cable modem connections. Only 1.8 percent of the connections are fiber optic connections. Leased lines comprise a negligible percentage.
- *Low density of commercial Wi-Fi hotspots:* Commercial Wi-Fi hotspots, whether offered for a fee or made available for free through third-party financing, can help augment the mobile broadband and private residential and commercial hotspots as well as mobile broadband. They are an important part of the broadband infrastructure in a country. In many other countries, there is much greater availability of such hotspots. Use of public Wi-Fi can help offer consistent, reliable and high speed Internet to users, while decongesting mobile broadband. India has only about 32,800 public Wi-Fi hotspots.[49] The total number of public Wi-Fi hotspots in the world is over 11 million.[50]

Given this context, we take the key intermediate goals for broadband Internet India to be: expanding access to fixed broadband; decongesting mobile broadband in dense urban environments; proliferating commercial Wi-Fi hotspots; and improving the quality of Internet access. If these goals are achieved, India's performance on quality and quantity of internet access would improve. It is also crucial for India to ensure that it does not miss the bus with the new spectrum-based technologies and business models being developed, especially those that will rely on spectrum bands such as V-band and E-band.

[49] See: https://www.ipass.com/wifi-growth-map/
[50] Ibid.

# 8 Identifying the potential uses of V-band and E-band in India

The scale and nature of economic benefits from these bands may depend on: the variety of use cases for the spectrum; the potential scale of each use case; the value of economic activity supported by the spectrum; and so on. Based on stakeholder consultations, literature review, and above analysis of broadband Internet in India, we have identified the following key uses of the V-band and E-band spectrum:

- *Support proliferation of commercial Wi-Fi and Wi-Gig hotspots:* these bands can help backhaul the commercial Wi-Fi infrastructure in a cheaper and quicker manner, especially in dense urban locations.
- *Support expansion of fixed broadband Internet in urban areas:* these bands can help solve the last mile problems of getting high speed wired broadband Internet into dense urban locations.
- *Backhaul for mobile broadband:* these bands can provide higher capacity backhaul for mobile broadband, thereby easing congestion
- *Other uses:* these bands can be put to a variety of other uses. These, inter alia, include: extension of local area networks between buildings within a building complex; Internet of Things; Vehicle to vehicle communication; Augmented Reality (AR)/Virtual Reality (VR) Systems; and so on.

Most of the benefits discussed in this section depend not just on release of the spectrum, but also on other enabling conditions. This raises the question: *what do we assume about the policy environment in the next few years?* For the purpose of our analysis, we assume an optimised policy environment, which means that we expect that the other necessary steps will be taken, and no further impediments will be created. The benchmarks we are proposing are not ambitious but in line with the performance that can be expected in India in an optimal scenario.

Our analysis is for the five-year period between 2017 and 2022. This seems to be a reasonable time period, because a longer period would render the conclusions inutile, given the rapid changes in technology, and any short period may lead to under-estimation of benefits, as benefits are expected to accrue over a few years.

To understand the specific types of benefits from these bands, it is useful to think about a specific densely built urban habitat. It may comprise residential, recreational as well as commercial places. To help identify the benefits, we have developed a hypothetical case of a dense urban area to see the benefits that are likely to accrue to producers and consumers.

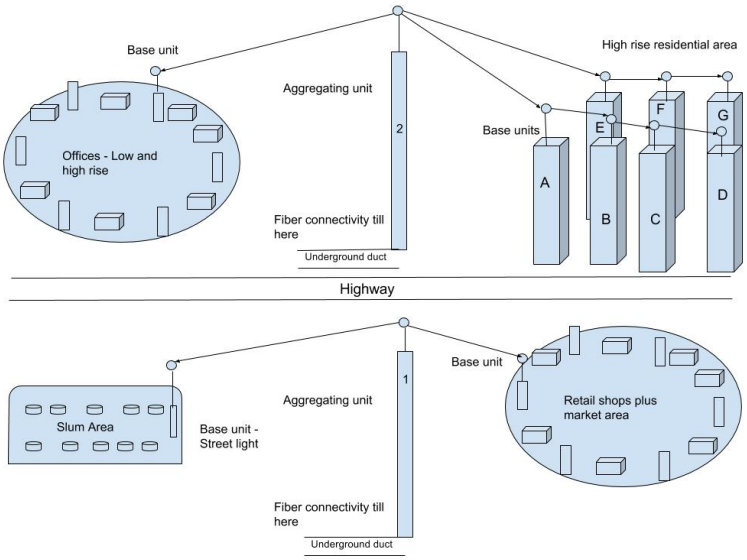



**Figure 2:** Case Study of a Dense Urban Environment

## 8.1 Case study on use of the bands for improving connectivity

In this hypothetical example, we consider the usage of this band for last-mile connectivity. We assume that fiber connectivity is available upto aggregate sites, beyond which fiber becomes impractical to use due to a number of reasons. We also assume that backhaul from this base site is extended using these bands, which will cater to a market area (eg. inner circle of Connaught Place in Delhi), high rise residential area, slum area and office complex.

In figure 2, we have drawn out a hypothetical dense urban environment. It is comprised of a slum, market area, an office complex and a residential area. If a service provider wants to extend Internet services from the aggregating unit to any of these areas, they can use these bands to extend the backbone. We make the following assumptions respectively for the commercial and residential area:

- *Residential area*
  - This consists of a number of high rise buildings.
  - Each building in the residential area will have a cell at the top and using ethernet and existing utility ducts, Internet can be made available to each home.
- *Market area*

  - This is a busy marketplace of the kind that is seen in every city.
  - It has a high daily average footfall of, say, 100,000 people.
- *Office Area*
  - Several high rise buildings and low rise buildings in the office area.
  - The high rise buildings would have more bandwidth requirement than low rise buildings.
- *Slum area*
  - This is a habitation comprising of low rise temporary and semi-permanent constructions that are densely packed in a small area.

We work with the assumption that the bands have a radius which allows connection to a respective base station in all four areas, with one or more hops. As the aggregation sites are connected using fiber, the bandwidth they can carry is assumed to be very high. These base units would then connect to other cells (within line of sight) to ensure adequate coverage of each area. The use of these bands will ensure high throughput as compared to the existing licensed microwave bands such as 13, 15 18 and 21 GHz.

The office buildings will require high speed Internet to be made available to employees. Such buildings may require multiple cells to be placed on each of them. The residential buildings may have lower requirements, and one cell per building may suffice, and the distribution within the building may be done using DSL, ethernet or any other solution. For the slum area, the service provider may situate towers in strategic locations, from which it could distribute within the area. The market place is a suitable location for commercial Wi-Fi hotspots. A mesh of Wi-Fi hotspots backhauled using these bands can provide high speed connectivity in the market place, while helping decongest the mobile network.

This illustrates how these bands can be deployed to improve connectivity in dense urban environments where laying cables is expensive and time consuming, and may even be infeasible in certain locations.[51] These bands can enable quicker and cheaper backhaul solutions in such contexts.

Considering this, we have identified the key economic benefits expected from use of V-band and E-band in India.

## 8.2 Proliferation of commercial Wi-Fi and Wi-Gig hotspots

At present, service providers offering commercial Wi-Fi hotspots must mainly rely on wired backhaul. In urban areas, establishing wired backhaul is expensive,

[51] This point was made repeatedly in consultations with stakeholders.

time-consuming, and, in some places, even infeasible. As discussed earlier, this problem can be potentially overcome by the use of V-band and E-band. India has about 25 commercial Wi-Fi hotspots for every 1 million inhabitants, while the global average is 1470.[52] In 2013, the global average was about 1000, while in India this was about 22.[53] So, in spite of the low base, the pace of proliferation in India is low. For our analysis, we assume that the government and TRAI will take the necessary measures to help proliferate commercial Wi-Fi hotspots in India. To estimate the number of public Wi-Fi hotspots that will use these bands for backhaul, we first need to establish a reasonable benchmark for the density of such hotspots that India could achieve in the next five years.

Since the use of these bands for backhauling Wi-Fi hotspots is primarily in densely populated urban areas, we need to find a relevant benchmark for such areas in India. In 2016, the per capita income in India in purchasing power parity (PPP) terms was about 40 percent of the average per capita income in the world.[54] According to government's estimates, per capita income in urban India is about 2.5 times of that in rural areas.[55] From this, we can derive that, in 2016, per capita income in urban India was about 68 percent of the average per capita income of the world. Assuming that the rate of growth in per capita income between 2011 and 2016 will persist between 2016 and 2022, this will be 84 percent in 2022. However, given the low density of hotspots in India, it might take a few years for the proliferation to take place. Hence, we propose benchmarking the density of commercial Wi-Fi hotspots in urban India at 60 percent of the average density in the world by 2022.

Beginning with the present global benchmark, we project the proliferation of commercial Wi-Fi hotspots in the next 5 years. For this, we assume that the present rate of growth in population and number of commercial Wi-Fi hotspots will continue.[56] This yields a global benchmark of 2267 hotspots for every 1 million inhabitants in 2022. Sixty percent of this is 1360 - this is the density we expect to see in urban India by 2022.

About 75 percent of broadband subscribers are in urban areas.[57] Since we do not

[52] Based on the number of hotspots reported on https://www.ipass.com/wifi-growth-map/

[53] Ibid.

[54] See this World Bank database on per capital income in India and the World in PPP terms: http://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD

[55] See this report on urban and rural per capita incomes: http://bit.ly/2wlJI9Z

[56] For rate of growth in commercial Wi-Fi hotspots, we consider the rate between 2014 and 2017. The rate of proliferation of public Wi-Fi hotspots globally decelerated from 15 percent in 2013-14 to 10 percent 2014-15, but it has been the same since then.

[57] TRAI. The Indian Telecom Services Performance Indicator Report January - March, 2017. Available at: http://www.trai.gov.in/sites/default/files/Indicator_Reports_050720174.pdf

**Table 4:** Projected public Wi-Fi hotspots in urban areas in India: 2017 to 2022

| Year | Population projection for urban India (millions) | Commercial Wi-Fi hotspots in urban India | Density (hotspots per million) |
|---|---|---|---|
| 2017 | 432 | 24600 | 57 |
| 2018 | 442 | 47471 | 107 |
| 2019 | 452 | 91604 | 203 |
| 2020 | 462 | 176768 | 382 |
| 2021 | 473 | 341110 | 721 |
| 2022 | 484 | 658240 | 1360 |

have information about urban-rural distribution of commercial Wi-Fi hotspots, we assume that 75 percent of commercial Wi-Fi hotspots are in urban areas. So, about 24,600 hotspots are estimated to be in urban areas - about 57 hotspots per million inhabitants.[58] Table 4 presents our projections of the number and density of commercial Wi-Fi hotspots. The yearly projections are based on the compounded annual growth rate required to go from the present density to the benchmark density in 2022. Although the annual rate of growth required may appear to be high, this is consistent with the rate at which hotspots have proliferated in other countries.

So, we project about 6,33,640 new commercial Wi-Fi hotspots to be established in urban areas during the next five years, if all the necessary steps, including release of these spectrum bands, are taken. Now, to estimate the number of these hotspots that will need to use V-band and E-band for backhaul, we consider it important to distinguish between the top 15 most populated cities[59] and the other urban areas. The top 15 cities have the highest right of way costs, labour costs, and other difficulties in laying wired backhaul network. We assume that 35 percent of the total public Wi-Fi hotspots in India are in these 15 cities.[60] So, we expect about 2,95,699 new commercial Wi-Fi hotspots to come up in the top 15 cities.

Given the challenges of alternative backhaul options, we expect that, if these bands

[58]Using the urban population in 2011 (377 million) as the base, and applying the annual growth rate in urban population in India (2.3 percent), we estimate the population in 2017 to be 432 million.

[59]These cities, which have been selected on the basis of population in 2011 census, are: Delhi, Mumbai, Bangalore, Kolkata, Hyderabad, Chennai, Ahmedabad, Surat, Jaipur, Pune, Kanpur, Nagpur, Indore, Thane.

[60]This assumption is based on our estimate that about 35 percent of broadband subscribers are in these 15 cities.

are released, about 40 percent of the new commercial Wi-Fi hotspots established in the top 15 cities will use them for backhaul, while only 20 percent will do so in other urban areas. Further, we expect that about 10 percent of the hotspots in the top 15 cities and 5 percent in the other urban areas cannot be established without these bands or any similar backhaul spectrum, because of infeasible backhaul costs. The benefits from these hotspots can be fully attributed to these bands, while those from other hotspots that use this band for backhaul can only be partly attributed. So, according to our estimates, about 46,467 commercial Wi-Fi hotspots in India would not come up unless these spectrum bands are made available. Further, we expect 1,39,401 other commercial Wi-Fi hotspots to use these spectrum bands for backhaul even though they could have been established otherwise, but at a higher cost and with significant delays.

### 8.2.1 Deployment of commercial Wi-Gig hotspots

Wi-Gig can offer multi-gigabit data transfer rates to users. Since the technology is in early stages of adoption, it is difficult to project the scale of its proliferation. Wi-Gig hotspots are expected to be about 10 percent of the Wi-Fi hotspots by 2020.[61] For our analysis, we expect that Wi-Gig hotspots in India will be about 10 percent of the hotspots in urban locations by 2022. We expect about 65,000 commercial Wi-Gig hotspots to be deployed by 2022 in urban locations in India. Although all these hotspots may not use V-band or E-band for backhaul, since all of them will use V-band for access, the economic benefits arising from them can be fully attributed to these spectrum bands.

## 8.3 Proliferation of fixed broadband connections

In densely populated urban areas, because of the existing built-up area, it is expensive and often very difficult to take wired Internet to homes and offices. Even if wired network can be taken into certain locations, extending it to adjacent areas can be challenging because of difficulties of obtaining right of way permissions, or the physical obstructions on the way. These observations were made by the stakeholders we held discussions with. TRAI also observed in its "Recommendations on Delivering Broadband Quickly: what do we need to do (2015)", the following:

> ....Fibre to the Home (FTTH) or Fibre to the curb (FTTC) networks require installation of a new fibre link from the local exchange (central office) directly to or closer

[61] See, for instance: http://bit.ly/2vhSVCK

> to the subscriber. Even though fibre is known to offer the ultimate in BB bandwidth capability and is not very expensive, installation costs of such networks (cost of fibre and Right of Way (RoW)) have, up till recently, been prohibitively high.

Some stakeholders indicated to us that the fibre breakage rates in India are much higher than those seen in other countries.

V-band and E-band can be used along with fibre optic cables to create a high speed wired Internet network, which can help improve consistency of Internet connectivity in India, and get FTTH and FTTC networks in locations where they are not present currently. This spectrum can also be used to reduce the cost of improving bandwidth availability in locations where wired broadband is already available. The use cases of this spectrum is most obvious in densely populated urban areas, but may also extend to suburban areas and residential clusters in rural areas.

There are about 18.23 million fixed/wired broadband subscribers in India.[62] These include residential as well as commercial locations. This translates to a wired broadband density of 1.4 per 100 inhabitants. Assuming that the share of urban subscribers in the fixed broadband subscriber base is the same as their share in total broadband Internet subscriber base (for which this rural-urban disaggregation is available), we estimate about 13.5 million fixed broadband subscribers in urban India.[63] Based on the estimated urban population for 2017 (432 million), the density of fixed broadband connections in urban areas is estimated to be about 3.13. Further, based on their estimated share in the broadband Internet subscriber base, we estimate about 6.3 million of these connections to be in the top 15 cities.

As discussed earlier, the average density of fixed broadband connections in the world was about 11.6 (per 100 inhabitants) in 2015, up from 9.04 in 2011. Assuming that the rate of growth between 2011 and 2014 continues, the density of fixed broadband connections in the world in 2022 would be about 18. Adjusting for differences in incomes, as discussed earlier, the density for urban India should be about 15 in the year 2022. However, for the purpose of our analysis, the benchmark we are proposing for density of fixed broadband connections in urban India in 2022 is 12. This downward adjustment is driven by our judgment that, given the heavy reliance on mobile broadband in India, it is not likely that we in India will be able to make a rapid shift to meet the global benchmark in the near future.

[62] Data available at: http://www.trai.gov.in/sites/default/files/Press_Release_No50_Eng_13072017.pdf

[63] About 74.3 percent of the total number of broadband subscribers, which include fixed as well as wireless connections, are in urban areas.

**Table 5:** Projected fixed broadband connections in Urban India

| Year | Fixed broadband connections (in millions) |
|---|---|
| 2017 | 13.5 |
| 2018 | 18.1 |
| 2019 | 24.2 |
| 2020 | 32.3 |
| 2021 | 43.3 |
| 2022 | 57.9 |

To meet the benchmark of 12 fixed broadband connections per 100 inhabitants, India will need about 58 million fixed broadband subscribers in urban areas by 2022. So, 44.5 million more connections will be required in urban areas in the next five years. Assuming that their share in subscriber base remains constant, we estimate about 20.77 million of these new connections to come up in the top 15 cities. V-band and E-band can help in the expansion of the fixed broadband subscriber base in urban areas by making it easier and cheaper to backhaul these connections. Table 5 presents our projections of the number of fixed broadband connections in urban India. The yearly projections are based on the compounded annual growth rate required to go from the present density to the benchmark expected in 2022.

Consistent with the assumptions made regarding commercial Wi-Fi hotspots, we assume that V-band and E-band will be used for backhaul in 40 percent of connections in the top 15 cities, and 20 percent of connections in the other urban areas. Further, we assume that 10 percent of the connections in the top 15 cities and 5 percent of the connections in other urban areas would not come up without this spectrum. For the other new connections, using this spectrum for backhaul would lead to savings of time and money. So, about 3.26 million new fixed broadband connections would depend on the release of this spectrum, and their benefits can be fully attributed to it. Further, about 9.8 million of the additional fixed broadband connections may use this spectrum for backhaul, even though they could have come up using other backhaul solutions, albeit at a higher cost and with delays.

In the next few years, some of these fixed broadband connections may use Wi-Gig devices for access, instead of Wi-Fi or cable. As discussed earlier, such hotspots are expected to be 10 percent of total number of Wi-Fi hotspots in the world by 2020. We assume that, by the 2022, of all the fixed broadband connections, about 10 percent will use Wi-Gig standard devices for access. So, there will be about 5.8 million such connections in urban India in 2022. Their economic benefits can be

fully attributed to the availability of these spectrum bands.

## 8.4 Backhaul for mobile broadband

Only about 15 percent of cell sites in India are connected using fibre optics. The mobile backhaul infrastructure in urban environments suffers from similar problems as the infrastructure for wired broadband network. As TRAI had observed in its "Recommendations on Delivering Broadband Quickly: what do we need to do (2015)".

> ....Another major reason for the poor quality of wireless broadband is non-availability of adequate bandwidth in the backhaul. For 3G and 4G networks, in the absence of adequate fibre, availability of sufficient quantum of backhaul spectrum is a prerequisite.

In the same paper, TRAI had also discussed how the high Right of Way costs for establishing wireless access points of presence and backhaul facilities affected backhaul infrastructure.

Presently, 13/15/18/21 GHz Bands have been made available for backhaul usage. V-band and E-band can be used to augment and extend wired backhaul networks, and perhaps even to substantially replace use of wired backhaul infrastructure with a combination of hops. This would reduce the cost of mobile backhaul and also enable high speed backhaul in areas where high congestion is expected. Further, our discussions with stakeholders so far suggest that the use of V-band and E-band reduces the size of cells, including the base stations. This means that a base station would take smaller space and could be installed at a lower cost and lesser right of way problems. The lower cost of cells, along with higher backhaul capacity, could help potentially reduce congestion in mobile broadband access, and even allow more data to be made available at the same price.

V-band and E-band offer a larger backhaul capacity at short distances than the spectrum bands that have been made available for this purpose. The backhaul range for V-band and E-band can be increased by using multiple hops from one point to another. In dense urban environments, in sites that require high backhaul capacity, these spectrum bands can offer an effective backhaul solution. First, in such locations, laying underground cables is expensive, impossible or a cause for delay. Second, in such locations, there is greater likelihood of congestion of wireless backhaul using the presently available spectrum. With the rapid rollout of 4G, and the expected introduction of 5G, it is quite likely that many locations where backhauling is done using the wireless spectrum will face congestion.

It is difficult to project how many sites in India will face backhaul congestion. Our consultations did not yield a precise estimate. A report by Ericsson estimates that by 2021, the mobile broadband backhaul capacity required in 2021 may be much higher than that required at present.[64] Even with basic mobile broadband, about 20 percent of radio sites may require more than 150 Mbps of backhaul capacity, and a few may even require more than 300 Mbps. Further, the report estimates that with advanced mobile broadband (4G and higher), by 2021, the backhaul capacity required may rise to 1 Gbps for 20 percent of sites, and a few sites may even need 3-10 Gbps of backhaul capacity. For the sites that require high backhaul capacity, the presently available spectrum bands are not going to suffice, and since most of those sites are located in dense urban environments, it will be difficult to rely upon fiber optic cables.

We expect that the sites that face backhaul congestion with the presently available backhaul spectrum bands will comprise about 15 percent of total sites in India by 2022. This assumption is based on other assumptions discussed in this note. For instance, we assume that commercial Wi-Fi hotspots will develop rapidly, and fixed broadband connections will proliferate, thus decelerating the pace of mobile broadband congestion. Hence, we are proposing a modest assumption about the number of cell sites that will face congestion by 2022.

According to a report by the consulting firm Deloitte, the number of cell sites in India is expected to grow to about 1.5 million by 2020.[65] Assuming that the rate of growth in cell sites will reduce because of a shift to fixed broadband and proliferation of commercial hotspots, we assume that the number of cell sites required would rise to about 1.6 million by 2022. So, about 2,40,000 cell sites may need to use V-band and E-band, a similar spectrum band or wired backhaul solutions to meet the needs. We expect that about 50 percent of these would use V-band and E-band for backhaul. So, about 1,20,000 cell sites would rely on V-band and E-band for backhaul in 2022.

## 8.5 Improvements in the quality of Internet access

Use of V-band and E-band spectrum can, by enabling changes in the infrastructure for Internet, help improve the quality of Internet access in India. By helping expand the access to fixed broadband, by enabling proliferation of public Wi-Fi, by helping improve mobile backhaul capacity, and by allowing Wi-Gig connections to

[64] Report available at: https://www.ericsson.com/assets/local/microwave-outlook/documents/ericsson-microwave-outlook-report-2016.pdf

[65] Report is available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-indian-tower-industry-noexp.pdf

begin proliferation, these spectrum bands can help change the way users in India access the Internet. This can have a significant impact on the speed, consistency, and volume of Internet usage.

- *Speed of Internet access:* According to Akamai's State of the Internet Report, in the first quarter of 2017, among the 15 Asia-Pacific countries covered in the report, India has the second lowest average Internet speed, and the lowest average peak speed.[66] One of the reasons for this is that India relies disproportionately on technologies that allow lower speeds. As discussed earlier, most people in India access broadband Internet through mobile broadband, and even fixed broadband connections are mostly based on DSL and dial-up. This constrains the speed available to users. For instance, in Thailand, 72 percent connections are above 10 mbps, in India only 19 percent connections have this speed. Use of V-band and E-band for backhaul and, in some cases, for access can help improve the average Internet speed in India. If, by 2022, urban India has 58 million fixed broadband connections, 6,58,240 commercial Wi-Fi hotspots, and 65,000 Wi-Gig hotspots, the average and peak speeds could be much higher.
- *Consistency of Internet access:* At present, most users in India rely on mobile broadband for broadband Internet. With the advent of 4G, the speeds for mobile broadband are now much higher than they were with 3G. Mobile broadband has the advantage of offering mobility, but it faces constraints on consistency of connection, especially in locations with density of connections. Compared to mobile broadband, Wi-Fi offers a much better consistency of Internet access. As India is rapidly scaling up Internet access, it is equally important to ensure that the way in which people access Internet meets not just the requirements of mobility and speed, but also consistency of access. This can be done, inter alia, by use of V-band and E-band for improving access to fixed broadband and public Wi-Fi hotspots.
- *Volume of Internet usage:* According to forecasts by Cisco, mobile data usage in India is expected to be 2 Exabytes per month by 2021, up from 266 Petabytes in 2016. Based on population forecasts, this would mean that the volume of mobile data usage would increase from about 200 Megabyte per person per month to about 1.43 Gigabytes per person per month. For fixed connections, the usage is forecasted to grow from 1.5 Exabytes per month (1.13 Gigabytes per person) to 4.96 Exabytes per month (3.57 Gigabytes per person). The average total data usage per person per month is forecasted to increase from 1.33 Gigabytes to 5 Gigabytes. Mobile connections are forecasted to account for about 29 percent of total data usage in 2021,

[66] Available at: https://www.akamai.com/us/en/multimedia/documents/state-of-the-Internet/q1-2017-state-of-the-Internet-connectivity-report.pdf

up from 15 percent in 2016. The global forecast for mobile data usage is 49 Exabytes per month (6.36 Gigabytes per person) in 2021, up from 7.2 Exabytes per month in 2016 (about 0.98 Gigabytes per person). For fixed connections, the forecast is that data usage in 2021 will be 196 Exabytes per month (26.74 Gigabytes per person), up from 82.8 Exabytes per month (11.3 Gigabytes per person) in 2016. So, the average data usage per person month is forecasted to increase from 12.3 Gigabytes to 33.1 Gigabytes. Globally, the share of mobile connections in data usage is expected to increase from 8 percent in 2016 to 20 percent in 2021. The following table summarises the status in 2016 and forecasts for 2021.

**Table 6:** Internet usage forecasts

| | Aggregate data usage per month (in Exabytes) | | | Data usage per person per month (in Gigabytes) | | |
|---|---|---|---|---|---|---|
| | Mobile | Fixed | Total | Mobile | Fixed | Total |
| India | | | | | | |
| 2016 | 0.266 | 1.5 | 1.766 | 0.2 | 1.13 | 1.33 |
| 2021 | 2 | 4.96 | 6.96 | 1.43 | 3.57 | 5 |
| Global | | | | | | |
| 2016 | 7.2 | 82.8 | 90 | 0.98 | 11.3 | 12.28 |
| 2021 | 49 | 196 | 245 | 6.36 | 26.74 | 33.1 |

Aggregate data usage depends on various demand and supply factors. One of the supply-side factors is the proportion of mobile and fixed connections used for accessing Internet. Also, constraints on backhaul capacity may restrict the number of high speed connections, which may also affect the total usage. Further, as price elasticity studies from other countries and recent experience with increase in data usage with falling prices in India suggest, every unit decrease in price leads to a huge increase in volume of usage. So, to the extent that delicensed V-band and E-band will be able to ease the backhaul constraints, help improve access by deployment of Wi-Gig, and enable lowering the prices, there will be an impact on the volume of data usage in the coming years.

## 8.6 Other potential benefits

There are a variety of potential use cases of these spectrum bands that are under development. Although it is very difficult to quantify, let alone monetise, the benefits from these use cases, it is nonetheless important to consider them while

taking a decision about the release of these spectrum bands. Some of these use cases are summarised below.

### 8.6.1 Extension of local area networks between buildings

India has a large number of office, college, university, hospital and other complexes wherein multiple buildings are located in a contiguous area, with a local area network spanning the complex. V-band and E-band can help connect different buildings within such complexes using point-to-point cells, so that such connections do not require fibre optics or other cable-based solutions. This can help reduce the cost of networking without significant compromise in the quality of the network.

A typical scenario might involve a company in a high-rise office building that has opened a second office in an adjacent building. Both offices house employees who need to share data on the company's LAN or access databases in real time. This required connectivity could have been provided by the owners of the buildings if they had established a fibre-optic cable run between the two buildings. But often there is no such level of interconnectivity between buildings. So, a second option would be to run dark fibre (i.e., privately operated optical fibre) between the two offices. This type of installation requires a special contractor with high costs. That may be worth it in some cases, but there are other options that do not require such a high capital expenditure.

If the facilities are within line of sight of each other and within the range, the company can easily deploy a connection using these bands, and depending on other usage of the band in the location, it could get multi-gigabit of data transfer rates. After a relatively modest capital expenditure, the company will have a secure, reliable connection with low ongoing operating expenses.

### 8.6.2 Internet of Things

Internet of Things (IoT) devices can range from small sensors to large industrial equipment and may find usage across industries. IoT applications too are diverse. Consequently, the communications requirements for these applications are quite different. Depending on the intended usage, the application may require city-wide coverage or indoor coverage, or may require the capability to transfer large amounts of data. Certain IoT devices, such as sensors installed in remote areas, may also have low power requirements. Different wireless technologies address these different requirements.

The IEEE standard 802.11ad (WiGig) operates in the 60 GHz spectrum and supports very fast data transfers at a very low latency. These characteristics make WiGig a suitable choice for critical industrial applications where certainty of timely access is key, albeit over short ranges.[67] A typical use case for WiGig would be an industrial control and machine vision system used for robotic guidance. Another IoT use case for WiGig would be a 4K video camera security system with high bandwidth requirements. An example of an existing WiGig implementation is the prototype developed for use at the Tokyo-Narita airport. This system, which combines WiGig with Mobile Edge Computing (MEC) to enable ultra-high speed downloads with low latency, is expected to be used for the 2020 Summer Olympics.[68]

Some experts believe that WiGig is not suited for IoT since WiGig requires line of sight and can't penetrate even thin walls.[69] Another Wi-Fi technology, Wi-Fi HaLow is based on IEEE 802.11ah and operates in the sub 1 GHz spectrum. Longer range, lower power operation and lower throughput compared to other Wi-Fi technologies makes it more suitable for IoT devices distributed in larger areas.

### 8.6.3 Vehicle to vehicle communication

Vehicle to Vehicle (V2V) communication is another potential area of application for WiGig. Vehicles will increasingly utilise sensors, using technologies such as Light Detection and Ranging (LIDAR), to transmit large amounts of data in connected vehicle systems.[70] The data rate requirements for such systems are very high, especially for systems involving autonomous vehicles having enhanced sensing capabilities. WiGig is seen as a solution for these scenarios but challenges such as antenna placement and interference continue to persist.

[67] Internet of Things - New Vertical Value Chains and Interoperability, Wireless Broadband Alliance, 2017, available at http://www.wballiance.com/wp-content/uploads/2017/03/IoT-New-Vertical-Value-Chains-and-Interoperability-v1.00.pdf

[68] Sakaguchi, Kei, et al, Where, When, and How mmWave is Used in 5G and Beyond, available at https://arxiv.org/ftp/arxiv/papers/1704/1704.08131.pdf

[69] Will 60GHz be the new 2.4GHz Wi-Fi?, available at http://jbsystech.com/will-60ghz-next-2-4ghz-Wi-Fi/

[70] R. W. Heath, Vehicular Millimeter Wave Communications: Opportunities and Challenges, available at http://users.ece.utexas.edu/rheath/presentations/2015/DSTOPvehicularMmWave2015Heath.pdf

### 8.6.4 Augmented Reality (AR)/Virtual Reality (VR) Systems

The demand for AR/VR systems and the data usage by such systems is expected to increase significantly in the coming years. A recent study claims that data traffic for mobile VR applications is expected to grow by 950% between 2016 and 2021.[71] VR systems have high throughput and low power requirements. Current VR displays are wired peripherals though and manufacturers are looking to make them self-contained devices with processing capabilities built inside the device. Such VR headsets need to be lightweight and must ensure that they offer a natural immersive experience to users.[72] WiGig, with its gigabit speeds, low latency and low interference levels, is being seen as a solution to the aforementioned issues with VR systems. Manufacturers such as Intel are already working on employing WiGig for VR systems and such wireless headsets are expected to be more common in the coming years.[73]

# 9 Mapping the economic benefits arising from the use cases

In choosing a method for releasing this spectrum, the focus should be on generating the highest net benefits for the society as a whole. In this section, we present the key economic benefits that are expected to accrue from the uses of these spectrum bands. Given the paucity of relevant data and earlier studies, we are unable to reasonably monetise the economic value of these benefits.

If the V-band and E-band spectrum is delicensed or lightly licensed, the pass-through cost of this spectrum will be zero or very small, and only the installation costs incurred will be substantial. In a competitive market, ceteris paribus, reduction in costs will lead to lower prices for consumers. Given the price elasticity of demand for internet, and the rapid evolution of technology, this availability will lead to higher usage of broadband internet by consumers, allow new consumers to use broadband internet, and enable innovative business models and technologies.

Since the use of these spectrum bands will lead to a reduction in costs, and create opportunity to reach hitherto unreachable locations in dense urban environments

[71] CISCO Whitepaper, "CISCO Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021," Feb. 2017.

[72] IEEE 802.11ad (WiGig's) future in virtual reality (VR) systems, available at http://www.bluwirelesstechnology.com/ieee-802-11ad-wigigs-future-virtual-reality-vr-systems/

[73] Intel and HTC tease upcoming WiGig accessory to untether the Vive, available at http://newatlas.com/htc-vive-intel-wigig-wireless/49784/

with high speed Internet, it will be a shift in the supply curve, so that more quantity is made available at a given price. If the quality of Internet access improves, as is expected from the use of V-band and E-band, there may also be a shift in the demand curve, as users may be willing to pay more for the connection. Quality improvement also has larger economic benefits. For instance, if the speed of Internet usage increases, users will be able to put their connections to a wider variety of uses, especially in commercial contexts. Bohlin and Rohman, 2012, estimate that each doubling of broadband speed leads to 0.3 percent increase in GDP.[74]

Following is an overview of the key expected economic benefits arising from the uses of V-band and E-band spectrum. It should be noted that all these benefits cannot be fully attributed to these spectrum bands. Some of them, such as benefits from Wi-Gig devices, may be fully attributed to these spectrum bands, because they rely completely on the availability of this spectrum. Other benefits can be partially attributed to these bands.

- *Producer surplus due to offloading from mobile broadband:* Producer surplus is the difference between the price that a service provider charges, and the minimum price the provider will be willing to accept. Producer surplus usually increases if the cost somehow falls without change in price charged. It can also increase if the price increases without corresponding increase in costs. The use of these spectrum bands would enable offloading from mobile broadband which will generate producer surplus.
  - *Offloading by users:* Use of commercial Wi-Fi hotspots and fixed broadband would lead to offloading from mobile broadband. This would enable service providers to use the same infrastructure to give more services, especially in congested areas. The producer surplus would be equal to the total cost savings compared to developing the infrastructure for such access using only mobile broadband. Estimating the monetary value of this producer surplus requires information from service providers about the cost of developing backhaul infrastructure using different options - fibre, V-band, E-band.
  - *Offloading by service providers:* As some users allow their private Wi-Fi hotspots to double up as community hotspots - a common practice in many countries - this will enable mobile broadband providers to enter into agreements with fixed broadband providers to allow offloading to Wi-Fi hotspots as soon as a user comes within the range of a hotspot. This will create producer surplus, as it will reduce the infrastructure

[74] Bohlin, E. and Rohman, I. (2012). Does Broadband Speed Really Matter for Driving Economic Growth? Investigating OECD Countries? Available at SSRN: http://ssrn.com/abstract=2034284

cost. This surplus may accrue to providers of fixed broadband (as fees) as well as to mobile broadband service providers (as additional revenues or lower costs). The global average is one community hotspot per 30 persons.[75] There is a huge opportunity to create producer surplus by developing community hotspots in India, but that needs proliferation of fixed broadband connections.

- *Producer surplus from lower backhaul costs for mobile broadband:* Lower backhaul costs could lead to producer surplus for mobile broadband service providers. This can be calculated by comparing the costs of backhaul using V-band and E-band with the cost of establishing infrastructure for a similar quality of service using other backhaul solutions, such as fibre optic cables. Most of this surplus would arise in congested areas. As per analysis presented earlier, about 15 percent of cell sites may face this situation by the year 2022.
- *Consumer surplus from use of commercial Wi-Fi hotspots and fixed broadband:* Consumer surplus is the difference between the price consumers are willing to pay and the amount they actually pay for a given quality and amount of service. This is the benefit that consumer derive from use of a service or good. Consumer surplus can increase if consumers' willingness to pay for a unit of service increases, which usually happens with perceived improvements in quality. It can also increase if prices of a service fall. A variety of sources for consumer surplus can be identified on the basis of the uses of V-band and E-band presented in the previous section.
  - *Consumer surplus from commercial Wi-Fi in dense locations:* In a densely populated location (eg. market place, tourist spot), for a given level of quality (speed and consistency), commercial Wi-Fi hotspots may be able to provide Internet access at a lower unit cost than mobile broadband. This will produce consumer surplus, which can be calculated as the volume of usage multiplied into the difference between unit cost for a certain quality of mobile broadband use and the unit cost of commercial Wi-Fi use for the same quality of access.
  - *Consumer surplus from free Internet:* Many providers of commercial Wi-Fi hotspots may give a limited amount of Internet usage for free. The entire value of such access would be consumer surplus. This can also be facilitated by third-party financing by government or any other agency.
  - *Consumer surplus from greater use of Wi-Fi and Wi-Gig devices:* Whenever we purchase and use a device, some consumer surplus accrues to us, as the price we pay is lower than the benefit we get from the device.

[75] See this page for data on hotspots: https://www.ipass.com/wifi-growth-map/

Since greater availability of Wi-Fi and Wi-Gig for access may lead to higher usage of Wi-Fi and Wi-Gig devices, the consumer surplus from these devices can also be partially attributed to use of V-band and E-band, to the extent that this spectrum enables usage of these devices.

  - *Consumer surplus from indoor use of fixed broadband:* For a given level of quality, the per unit price for fixed broadband is usually lower than that of mobile broadband. The difference between the price paid for mobile broadband and that for fixed broadband per unit is consumer surplus arising from this proliferation.

- *GDP contributions:* In addition to consumer surplus and producer surplus, there are also GDP contributions that may arise from the use of this spectrum. These are mostly in terms of new or improved businesses and technologies that are enabled by this spectrum band.
  - *GDP contribution of commercial Wi-Fi and Wi-Gig hotspots:* Provision of commercial Wi-Fi in public locations is relatively sparse in India. If such hotspots proliferate, the value addition done by the service providers operating the hotspots with V-band and E-band for backhaul would be a contribution to India's GDP that could not have been made in the absence of this spectrum. The firms would use spectrum, their capital investments and operating expenditure as inputs, and charge fees from users. The difference would be the value addition that would contribute to India's GDP.
  - *GDP contribution due to Wi-Fi and Wi-Gig device sales:* The sale of Wi-Fi tablets in India has been falling in recent years.[76] Perhaps this is due to the poor Wi-Fi network in India. If the system of Internet access changes, so that there is better availability of Wi-Fi hotspots and Wi-Gig hotspots, this trend could reverse. The value addition from additional purchase of such devices would be a contribution to India's GDP.
  - *GDP contribution of higher speed:* Use of commercial Wi-Fi and Wi-Gig hotspots and proliferation of fixed broadband would lead to higher average speed of Internet usage. In aggregate, this would lead to increase in GDP. If, for example, use of V-band and E-band leads to 50 percent increase in average speeds overall, this may lead to a GDP increase of about 0.15 percent.[77]
  - *GDP contribution of new or modified businesses and technologies:* Most of the other uses of V-band and E-band discussed in this note would

[76] See this report: https://ultra.news/t-t/31689/india-tablet-sales-fall-16-4g-picks-jan-mar-2017
[77] Based on the nominal GDP for 2016-17.

lead to GDP contributions, just like the technological and business model innovations that followed liberalisation of other spectrum bands. For instance, when RFID was delicensed, its extensive use in retail establishments led to substantial contributions to the GDP.

Since most of these benefits will accrue to consumers and producers, this will also create potential for the government to extract part of this benefit as additional tax collection. For instance, sale of devices and provision of services will create opportunities for the government to collect taxes from these activities. Further, to the extent that these activities will lead to additional profits for service providers, part of that profit will be taxed by the government. The concern that government may lose out on some non-tax revenue if it chooses to delicense this spectrum may be overcome by these revenue opportunities. Further, in light licensing regimes, some fees may also be levied on the usage of the band. However, as discussed earlier, keeping the fees high may impede usage of these bands, and may discourage some types of usage that may generate significant economic benefits. The experience of wi-fi and RFID spectrum supports this contention.

# 10 Conclusion

We have attempted to quantify the scale of usage of both these bands, and mapped those uses with potential economic benefits that would accrue from them. The paucity of data and studies prevented us from monetising the value of economic benefits from V-band and E-band. A few key points takeaways from this analysis are worth noting.

First, while choosing a method for releasing this spectrum, the focus should be on ensuring maximum aggregate benefits for the society, and not short-term revenue maximisation for the Government. Among other things, this means that the potential of these bands to help improve India's overall system of broadband Internet access should be realised. There are inherent limitations in the present system of reliance on mobile broadband, near absence of commercial Wi-Fi hotspots, and low penetration of high speed fixed broadband. Some of these limitations could be partially overcome by use of these spectrum bands, along with other suitable policy measures.

Second, based on the analysis in this note, it is safe to say that the economic benefits of these spectrum bands are likely to be substantial. Studies on economic benefits of previously unlicensed spectrum bands suggest that the variety and scale of economic benefits may increase over a period of time. However, if

delicensing is not feasible, it will be better to release this spectrum using block licensing or node registration. Link-by-link registration/licensing may not be suitable for backhaul usage, as there will be multiple links between nodes in a given area. Such registration is more suitable for point-to-point networks, and not for mesh networks.

Third, as has happened with other unlicensed spectrum bands, innovation and competition may lead to many types of uses that are difficult to anticipate at present. Hence, it would make sense to liberalise the spectrum without any cumbersome procedures or fees. For instance, levying a fee or auctioning the spectrum may limit the potential uses of the spectrum, as it would have for Wi-Fi and RFID spectrum bands. Since many potential users of the spectrum may be individuals and organisations outside of the regulated telecom sector, placing licensing requirements on them may restrict innovative uses of this spectrum.

Fourth, many of the benefits are not realised by the service providers, and accrue in terms of consumer surplus and GDP contributions of businesses and technological innovations spurred by the availability of this spectrum. If government decides to target revenue maximisation while allocating the spectrum, it will only be able to extract part of the producer surplus. However this will have effect on proliferation and therefore on consumer surplus and GDP contributions. This may lead to significantly lower economic benefits of the spectrum for the economic as a whole. At the same time, government may extract revenue afterwards, which may be linked to the scale of usage.

Fifth, in thinking about the strategy to release the spectrum, it is important to align with global device ecosystems and standards, so that India can benefit from economies of scale in production of devices, and potentially become a manufacturing hub for the devices.

# Acknowledgements

A number of persons and organisations have provided us with valuable input and feedback along the way. We would like to thank the following for their contributions:

- Vishal Trehan - Consultant at the National Institute of Public Finance and Policy
- D. Manjunath - Professor at IIT Bombay
- Shyam Ponappa - The Centre of Internet and Society
- Abhay Karandikar - Professor at IIT Bombay
- Ericsson
- Facebook
- Broadband India Forum (BIF)
- Tejas Networks
- Qualcomm
- Cellular Operators Association of India
- Bharat Broadband Network Limited (BBNL)

# Open data and digital identity: Lessons for Aadhaar[1]

December 3, 2017

**Amba Kak**

Mozilla Foundation
ambakak@gmail.com

**Smriti Parsheera**

National Institute of Public Finance and Policy
smriti.parsheera@gmail.com

**Vinod Kotwal**

Department of Telecommunications
vinod.kotwal@gov.in

Aadhaar, the largest national biometric system in the world, has been lauded for its promise to bring e cies to government service delivery, and the stimulus to private sector innovation. Yet it is contested and criticised for the vulnerabilities created by biometric data, potential threats to privacy and exclusion. However, in all of this, there has been relatively less exploration of the pen data possibilities from the Aadhaar ecosystem.

Every day, large volumes of data are being generated through the use of Aadhaar-enabled authentication and eKYC systems, both by government and private entities. The challenge now is to nd ways to nudge the UIDAI and all users of Aadhaar towards greater sharing of data, in privacy-protecting ways that do not create risks for Aadhaar-number holders. We propose an implementation framework that can achieve these goals by leveraging the existing provisions of the Aadhaar Act to create an open data ecosystem that balances the needs of openness and privacy.

[1] An earlier version of this paper was presented at the International Telecommunication Union (ITU) Kaleidoscope Conference, 2017 held in Nanjing, China.

# Contents


**1 Introduction** **2**

**2 Sources and potential of Aadhaar data** **3**
- 2.1 Release of open data by UIDAI . . . . . 4
- 2.2 Data generated by Aadhaar users . . . . . 6

**3 Incentives to "open"** **8**
- 3.1 For public bodies . . . . . 8
- 3.2 For private bodies . . . . . 10

**4 Privacy and implementation framework** **13**
- 4.1 Privacy framework for open data . . . . . 13
- 4.2 Monitoring and enforcement framework . . . . . 15

# 1 Introduction

Aadhaar, meaning foundation, refers to a 12-digit random identification number issued by the Unique Identification Authority of India (UIDAI). Originally established under an executive order in January, 2009, UIDAI came to become a statutory body under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act"). The project currently holds a biometric database of more than 1.18 billion individuals. Covering over 85 percent of India's population, it is the largest national biometric database in the world.

From its inception, Aadhaar was a unique government project - in part due to its collaboration with technologists and entrepreneurs, and a focus on the potential applications or "use-cases" the Aadhaar could lend itself to. This is also reflected in its API-based architecture, that allows private companies to query the database for authenticating users.

Its ability to "uniquely" identify individuals based on their biometric / demographic information and Aadhaar numbers is the stated basis for the government's push to link Aadhaar across (and even beyond) government services. Over the years, the government has linked, and made mandatory, the use of Aadhaar numbers for various welfare schemes like the transfer of direct cash benefits under public distribution of food grains, employment guarantee benefits, mid-day meals in schools, LPG subsidies, etc. It is also increasingly used as identification proof for availing services like banking and finance, digital payments and utility connections, among others.

Despite this rapid proliferation, the goals and architecture of the project have met with growing resistance. The Supreme Court of India is currently hearing a series of petitions challenging the constitutionality of Aadhaar, its compulsory linkage for the delivery of government benefits, potential for exclusion of beneficiaries; and impact on privacy, among others. These hearings recently led to a pronouncement by a nine judge bench of the Indian Supreme Court that there exists a fundamental right to privacy in India, which cannot be denied except through a fair, just and reasonable procedure established by law. The Court also spoke of other tests to question the existence of a legitimate state aim and proportionality of the measure to achieve that aim (Bhandari et al, 2017 [20]). These tests will now be applied for testing the constitutionality of Aadhaar.

While the judicial determination of these issues remains pending, the Aadhaar database continues to grow as the focal point of a rapidly evolving digital ecosystem. Hence there is a need to examine the data emanating from the Aadhaar

system, and its varied uses. Aadhaar is a publicly funded resource, and as such, there is a strong case for promoting the disclosure of data points that can facilitate more informed research, policy making, business decisions, as well strengthen the accountability of the UIDAI itself.

In this paper, we (i) identify the various streams of data generated both by the Aadhaar system, as well as its varied applications across sectors; (ii) identify the existing incentives for public and private sector to create open data; and (iii) suggest privacy principles and an implementation framework to guide the release of more open data through Aadhaar.

## 2 Sources and potential of Aadhaar data

Open data is de ned as *data that can be freely used re used and redistributed by anyone subject only at most to the requirement to attribute and sharealike* . Therefore, the most important features of open data are - availability and access; re-use and redistribution; and universal participation (Open Knowledge International [9]). In case of Aadhaar, its open data potential is closely linked to its characteristic design, features and functionalities. We therefore begin by examining the architecture of the Aadhaar project and then proceed to identify the categories of data that can emanate from its di erent processes.

The UIDAI is tasked with three key functional processes: enrolment, identi cation and veri cation (MeitY, 2017 [14]) Through an extensive network of enrolment agencies, UIDAI collects the demographic (name, date of birth, gender, address) and biometric ( ngerprints, iris scan and photograph) information of individuals for the purposes of enrolling them into the Aadhaar system. All the collected information is housed in, and managed by, the UIDAI Central Identities Data Repository. The next step of identi cation refers to the de-duplication of biometric data in the UIDAI database. In this de-duplication process the Aadhaar system performs a check of the information collected for each new enrolment against all the enrolled data to ensure uniqueness This results in the issuance of a unique Aadhaar number to the individual, which is meant to be a random number with no built-in intelligence.

Finally, it is the veri cation process that is employed in a variety of use-cases. This veri cation can be of two kinds - authentication and eKYC. The authentication services respond with a yes or no answer to the Aadhaar number holder s claim of identity and no personal information is shared in the process with the querying entity. On the other hand, electronic know-your-customer functionality

or eKYC allows authorised users to seek a person's identity information (but not their biometric information) from the Aadhaar database. The UIDAI rules allow the authorised eKYC agencies to keep the collected data in their records and use it for the purpose of delivering their services.

The list of agencies that have already adopted Aadhaar-based authentication systems includes Government benefit transfers and e-governance initiatives, banks and financial service providers, telecom companies, and digital certifying agencies. As of mid November 2017, UIDAI reported over 13 billion cumulative authentication transactions and over 3.5 billion eKYC transactions. This represents a drastic increase over the 4.5 billion authentications and 665 million eKYCs reported as of December, 2016 (UIDAI [16]). A number of factors have contributed to this increase, particularly the encouragement of eKYC driven financial inclusion and its use by telecom service providers pursuant to directions issued by the Government.

As more and more Government and private agencies move towards Aadhaar-based authentication systems, we see two primary sources of data emanating from the Aadhaar ecosystem:

1. statistics of Aadhaar enrolment and usage of the database available with UIDAI; and
2. data generated through government and private uses of Aadhaar.

Each of these categories of data comes with a unique set of challenges pertaining to the ownership of the information, the extent to which it can and should be made public and the incentives that might drive such disclosure. Before turning to these issues in the next section, we first identify the types of information that can emerge from Aadhaar and its uses, and the potential value of such data.

## 2.1 Release of open data by UIDAI

The decision and the responsibility of creating open data vests upon the owner or manager of the database. This right is exercised within the bounds of legally permissible disclosures. We therefore begin this section by examining the extent to which the Aadhaar Act permits (or, at the least, does not prohibit) UIDAI from making any Aadhaar related data publicly available.

The Aadhaar Act does not expressly vest the ownership of the collected demographic and biometric data with the UIDAI. However, the UIDAI claims to hold the data pertaining to residents as a trustee/custodian. UIDAI's control over the collected data is also exemplified by the fact that the individual providing her

information does not have the option to exit from the system (although she can request access to her information).

Irrespective of the issue of ownership, the sensitivity of the information and scope for its misuse demands that UIDAI, as its custodian, deal with this data in a highly controlled manner. Privacy and data protection concerns demand that an individual's Aadhaar number; the demographic or biometric information collected during the enrollment process; or authentication records of a person should not be released publicly, by UIDAI, its enrolment partners or the authorised users of its authentication and eKYC systems.

Keeping this in mind, the Aadhaar Act casts an obligation on the UIDAI to ensure the confidentiality of the identity information and authentication records of individuals. Subject to certain exceptions, the law also specifically bars UIDAI from revealing any information stored in its database or authentication records to any person. The authority is also restricted from collecting or maintaining any information about the purpose of authentication. These provisions put some basic restrictions on the information that can legitimately and legally be released in the public domain by UIDAI. However, in discharge of its daily functions, the UIDAI also gains access to a number of other data points that would not be captured by the confidentiality restrictions in the Aadhaar Act. Many aspects of this information are already being released as open data.

For instance, the Authority currently maintains an online dashboard that offers data about the State-wise status of enrolments, including by age and gender and the entities involved in the process. Similarly, monthly information is also being made available regarding the usage of the UIDAI authentication / eKYC architecture by its approved agencies for the period post December, 2016. This is accompanied by daily transaction figures, name of the authorised entity making the request and type of authentication (biometric, demographic or using one-time password) for the last one month. While these are notable developments, the system could gradually evolve to offer more and more granular data on a daily basis, including historical data

In comparison, almost negligible amounts of information is available regarding the number of failed transactions in the Aadhaar ecosystem, in terms of generation of Aadhaar number, enrolment rejections (and reasons for the same), failure of authentication and eKYC requests, etc. Transparency demands that these and other process statistics should also be made available publicly by the UIDAI. Access to this information will guide the users of Aadhaar, researchers and other third parties in assessing the extent of its adoption, the purposes for which it is being deployed and the failure rates. The last of these elements can serve a legitimate basis for conducting a systematic audit of the extent and cost of

the potential exclusion from the bene ts that have been linked to Aadhaar. This is a prerequisite for an open and informed debate on issues relating to Aadhaar, including in the context of the ongoing litigations on the project. At the same time, this data can also be used as a basis to make improvements in the system, including enabling more e ective grievance redress.

## 2.2 Data generated by Aadhaar users

Authentication: Every day, large volumes of data are being generated through the use of UIDAI s authentication and eKYC systems, both by government as well as private entities. In case of an authentication query, the Aadhaar repository o ers only a positive or negative response to con rm whether the submitted information matches with the information recorded in UIDAI s database. None of the Aadhaar information is shared with the requesting entity although the process of authentication in itself leads to the creation of new data. For instance, a bank that uses Aadhaar authentication to verify the identity of a customer prior to authorising the transfer of funds from her account is creating new data in the process. The bank is then in a position to use the fact of Aadhaar authentication along with customer data already available with it to generate daily details of the number of persons of di erent age groups who used Aadhaar authentication to carry out fund transfers of di erent denominations.

The Aadhaar Act and the regulations framed under it circumscribe the manner in which information collected through Aadhaar can be used by such requesting agencies. As per Section 8(2), a requesting entity can use the identity information of an individual only for submission to the UIDAI repository for authentication purposes. In the above example, the bank would not need to (or be able to) use the customer s identity information collected by UIDAI, although it would already have similar information in its records. The bank would, however, need to utilise the authentication logs generated through Aadhaar. The current regulatory framework may constrain such use due to the requirement that the authentication logs can only be used for certain identi ed purposes. This includes sharing of the logs for grievance redress, dispute resolution and audits by UIDAI. The regulations may therefore need to be revisited to clarify that the generation of open data, within the framework speci ed by UIDAI, would be regarded as one of the permitted uses of authentication logs.

eKYC: There is marked di erence, however, when it comes to the amount of data made available to and generated by authorised eKYC partners. The Aadhaar (Authentication) Regulations, 2016 allow the requesting entity to gain access to the person s demographic information that is  led with UIDAI and printed on the

person's Aadhaar card. This information can be used by it "for its own purpose", i.e. for the purposes of its business. It may also share the e-KYC data with other agencies for a specified purpose, with the consent of the individual.

With eKYC agencies, there is scope for release of valuable data points. We illustrate this using an example from the telecommunications sector. In September, 2016, a new telecom player, Reliance Jio, entered the Indian market employing Aadhaar eKYC as its primary mode of verifying and enrolling new subscribers. It is estimated to have added approximately 600 thousand new users per day in its first six months. More recently, the Department of Telecommunications has issued a direction to all telecom service providers to re-identify their mobile subscribers through the eKYC process by February, 2018. Based on current figures, this move would cover a telecom subscriber base of about 1.2 billion connections.

While the aggregate number of mobile users is significant, reports suggest that there exists a vast gender divide in the adoption of technology in India (Aneja and Mishra, 2017 [19]). Yet, we do not have any official statistics on the ratio of men and women among telecom users in India, either at the country-wide level or in local areas. The move towards eKYC verification of all telecom subscribers in India, means that telecom operators will soon have a Aadhaar-verified (private) database of telecom users in the country. This would include the gender and geographic information of each operator's user base. Supporters of the Aadhaar-mobile number linkage see the re-identification process as an opportunity for improving trust in the existing customer information held by telecom providers.

Aggregated together, the verified database of each provider's telecom users can serve to find out the total number of female telecom users in each geographic location, including rural-urban variations. Further, periodic disclosure of such data by all telecom operators will also allow the trends to be tracked over a period of time. It may be noted that most of this information is already available with the companies today also, however, no systematic measures have been taken from the perspective of aggregating this data and exploiting its open data potential.

The online registration system (ORS), a framework that links various government hospitals across the country to an Aadhaar based online registration and appointment system, can be another use case. The ORS facilitates eKYC of the patient, which is then used for providing appointments at various departments of different hospitals. Using the appointments database along with the Aadhaar identification information, ORS will be in a position to disclose aggregated data about the age and gender profiles of the patients visiting different departments. This information can be sewn together to gain insights into the broad categories of health problems faced by different groups, the burden on different departments and the variations based on the location of the hospital. All of this can contribute

towards evidence-based research and policymaking in the field of healthcare.

Another notable feature of the Aadhaar database is that it was among the first government-issued identifications in the country to recognise 'transgender' as a separate category (Nilekani and Shah, 2014 [7]). The release of aggregated data related to use of banking, payments, telecom, health, education and other Aadhaar linked services by members of the transgender community offers a unique opportunity to study the extent of their exclusion from the mainstream discourse. This however remains subject to concerns about the targeting of individuals and possibility of re-identification from aggregated data, given the small size of the total data set. These issues will need to be addressed through careful thinking about the principles that should govern the sharing of Aadhaar linked open data, as discussed further in Section 4.

# 3 Incentives to "open"

The case for promoting disclosures of open data emanating from Aadhaar applies equally to all authorised users of Aadhaar. However, the incentives for public and private users to disclose this data are very different. Unlike the public sector, where legal requirements and policy initiatives compel and encourage government agencies towards proactive disclosures, private companies are outside the purview of this legal framework. They also typically view data as a source of competitive advantage, and would be reluctant to disclose data points voluntarily. The challenge therefore is to find ways to nudge all users of Aadhaar towards greater sharing of data, in the interests of transparency for accountability, research and more sound policy making.

## 3.1 For public bodies

The legal basis for the government to open up datasets to the public comes from the 'right to information' (known in some jurisdictions as freedom of information) regime. The idea of open government data presupposes willingness of governments to proactively disclose information to its citizens, and has been a hard fought battle in many countries. In India, this right of access to information held by public authorities has been codified through the Right to Information Act, 2005 (RTI Act). The passage of the law emanated from a grassroots movement that insisted on 'people's audit' of government services to address corruption.

There is a comprehensive proactive disclosure provision in Section 4 of the RTI

Act, which puts a general duty on every public authority to provide "as much information suo moto to the public at regular intervals through various means of communication, including the internet". This puts the onus on public authorities to release data, so that the public has to minimally resort to the use of the law to obtain information. The provision also states that all public authorities shall routinely disclose a varied list of information including about its functions, decision-making norms, documents held, employee contracts, budgets – along with a catch-all direction to release "such other information as may be prescribed". Some studies however suggest that the promise of Section 4 has been watered down significantly in practice due to insufficient proactive disclosures (RaaG & SNS, 2017 [13]).

Outside of the RTI Act, there have been a few other measures to encourage disclosures. The President of India, in her address to the Parliament in June 2009, voiced the need for "A public data policy to place all information covering non-strategic areas in the public domain. It would help citizens to challenge the data and engage directly in governance reform". In March 2012, the Indian Government brought out the National Data Sharing and Accessibility Policy (National Data Policy). It remains the only official policy document on open data, with the stated objective of increasing accessibility and easier sharing of "government-owned", "non-sensitive" data amongst registered users particularly for scientific, economic and social development purposes. Pertinently, the policy rationale for open data is the investment of public funds that goes into collecting and processing such data. The emphasis on government ownership and the use of public funds is also reflected in the scope of the policy, which defines data to be limited to that generated "using public funds by various ministries/ departments/ organisations and agencies of the Government of India". The policy however has not been operationalised in the form of binding legal rules.

Specifically in the context of Aadhaar, Nandan Nilekani, founding Chair of the UIDAI, made a speech in 2010 stating that "*Aadhaar enabled applications the UIDAI envisions can turbo charge the enforcement of Section provisions of the RTI across our subsidy and welfare schemes*". He further said that the "availability of electronic records within such programmes" would be a "natural outcome" of its linkage with Aadhaar.

The digitisation of records, however, on its own has not led to proactive disclosure. As discussed earlier, UIDAI has uploaded some heads of information on its Aadhaar dashboard, yet there remain several gaps in the publicly available data emerging from the usage of Aadhaar. This is particularly true in respect of its various applications, or "use cases". Research group IDinsight identifies "transaction or beneficiary-level data" as one area which would benefit those

doing data-driven studies of the e cacy of the project (IDinsight [5]). However, such granular disclosures could raise privacy concerns as a result of which the law itself restricts UIDAI and its related agencies from gathering and disclosing certain types of user-level data. Where there has been proactive disclosure of government databases seeded with Aadhaar, there has been signi cant controversy around the disclosure of Aadhaar numbers in the process, which is not permitted under the Aadhaar Act. A report by a civil society group found that government portals using Aadhaar for making payments had uploaded the bank account numbers, and Aadhaar numbers of 13 crore people, raising serious data protection concerns (Amber Sinha & Srinivas Kodali, [1]). These proactive disclosures on the disbursement of welfare schemes serve as a means to ensure accountability in the disbursement of social welfare bene ts. It is therefore essential to devise an acceptable mechanism of disclosures without compromising on the con dentiality requirements of Aadhaar or disclosing other personally identi able information.

Section 8(1)(j) of the RTI Act provides that personal information which does not relate to any public activity or interest, or could cause unwarranted invasion of an individual s privacy should not be , unless there is a compelling public interest reason to do so. Further, Section 6 of the Aadhaar data security regulations also lay down a requirement that no government agency should publish Aadhaar numbers, unless they are redacted or blacked out through appropriate means Absent clear speci cations about these means, governments could err on the side of caution by removing entire datasets. In the next section we explore how best to achieve the balance between the goals of open data for research and transparency for accountability on one hand, and privacy concerns on the other.

## 3.2 For private bodies

As discussed, Aadhaar is a public infrastructure being used by various private companies for authentication (through seeding) and veri cation (through eKYC). These companies, like telecom operators or banks, are custodians of several useful demographic data points, some of which have been identi ed above. We argue that there is scope to encourage and facilitate disclosure of information held by entities that use Aadhaar.

This could be done through various means. In the next section we propose a proactive disclosure regime, akin to the one in the RTI Act, which will be enforced through the UIDAI s contracts with such entities. Other options could include encouraging disclosures by way of non-enforceable but enabling government policies. This could be coupled with ongoing guidance on kinds of data that would be a priority for disclosure, along with the necessary safeguards.

Specific disclosures might also be mandated by particular government agencies or sector regulators. For instance, continuing with the earlier example of telecom subscriber data, the Department of Telecommunication or the Telecom Regulatory Authority of India (TRAI) could mandate that each telecom operator must share district, rural/urban, and gender-wise information of its subscriber base on a periodic basis, which could then be released as open data either by the government or the regulator.

This debate also needs to be situated within a broader global push to encourage private companies to contribute more to publicly available data, particularly for research and policy making. Although, the term open data is usually used in the context of government or government funded data, some like the Open for Business Report, 2014 (Gruen et al, 2014 [8]) suggest that the term would also encompass private sector data. For private sector data, the challenge is to incentivise the companies to release non-strategic data that would contribute to research and development.

The UK government has an innovative model of a voluntary programme (called Midata) for private sector disclosures that are made to particular consumers, rather than to the public at large. Established in 2011, Midata invites signatories to provide consumers with "increasing access to their personal data in a portable, electronic format" subject to certain principles (BIS, 2014 [17]). UK's Enterprise and Regulatory Reform Act (ERR) allows mandating private sector disclosures and empowered consumers to enforce their data access rights in court. In this way, the ERR Act serves as a way to incentivise companies to make voluntary disclosures, through the looming threat of enforcement of its punitive powers (Out-law, 2014 [10]).

The International Open Data Charter (a collaboration between more than 70 governments and stakeholders) also questions the boundaries of the data that a typical policy should cover. They state that while the focus has been primarily on "government owned data" - "often the datasets that most matter, and that could have the most impact if they were open, do not belong to governments" (Davies & Tennison, 2017 [15]). In fact, it goes further to recommend that governments should have the power to mandate open data publication as part of giving licences to run a register, or negotiating directly with private providers to secure access to data which can then be shared as open data.

Apart from government facilitated or enforced disclosures, the coinage of "data philanthropy" has been used to describe the trend of companies volunteering anonymised and aggregated data with (usually select) third party users who might use this for research or policy purposes. Facebook's decision to share data on disaster maps, including valuable location information shared by users, with

trusted organisations like UNICEF and Red Cross (Facebook Research, 2017 [4]) and ‘data grants’ by the Mastercard Centre for Inclusive Growth (Randy Bean, 2017 [14]) offer some examples.

We also find similar instances from the telecommunications sector. Orange Telecom's Data for Development challenge encouraged researchers to use aggregate data in pursuit of development goals like health, transport and agriculture (Orange Telecom, 2015 [11]). They also rewarded best practices of anonymisation and cross-referencing of data. In 2014, it was reported that South African telecom operator MTN made anonymised call records available to researchers through a data analytics firm that provides predictive solutions (UN Global Pulse, 2014 [18]).

While such voluntary initiatives, which focus on disclosures to certain trusted intermediaries, are very valuable and should be encouraged for the many benefits that they generate, it is relevant to distinguish them from actual 'open data'. The goal of open data initiatives is to create unrestricted public access to the underlying information. It is therefore important to think about additional frameworks that enable the release of data points publicly making it accessible to a larger and growing pool of researchers and policy makers.

Another variation could be the use of interactive techniques. Here, the data administrator (say, in this case, UIDAI, government departments, banks, telecom companies) answers specific questions about the dataset without releasing the underlying dataset. For example, if priority areas for Aadhaar related open data were identified in advance, then this could act as a guide for the disclosures to be made subsequently. While the interactive method can prove to be instructive, we regard it to be only small part of the overall open data solution for the following reasons. Firstly, the RTI Act allows individuals to make such queries to public authorities, but the onus here would once again fall on individuals or research groups, taking away from the principle of open data altogether. Secondly, private companies are not included in its scope leaving any interactive disclosures on their part to be a voluntary exercise. Thirdly, the implementation of such a mechanism would still require a mechanism to scrutinise the data being released so as to prevent against privacy harms.

Taking into account these factors we proceed to identify the contours of what could be an Aadhaar-specific open data framework and the privacy and other challenges that may be encountered in that process.

# 4 Privacy and implementation framework

As we make a case for responsible data disclosures by the UIDAI and other government and private users of Aadhaar, the manner of implementation of this responsibility also needs to be spelt out. First and foremost, is the concern that any open data disclosures should not threaten the privacy of the individual data subjects, leaving them vulnerable to a host of harms, including financial fraud. In this section we propose an Aadhaar-centric open data privacy framework that must be supplemented by principles of interoperability, accessibility and comparability in the creation of open data.

## 4.1 Privacy framework for open data

Most data protection regimes today afford legal protection only to personal data or "personally identifiable information" (PII). The ability of this information to be traced to a particular individual or to an object associated or used by an individual is what creates the potential for harming the person's privacy. It is therefore unsurprising that anonymisation, which refers to the process by which information is manipulated to make it difficult to identify data subjects, has come to be adopted as safeguard to privacy concerns. As a result, anonymised data is often carved out as an exception to privacy principles. Recital 26 of the European Data Protection Directive, which is arguably one of the more comprehensive legal regimes on this subject, states that the principles of data protection shall not apply to "data rendered anonymous in such a way that the data subject is no longer identifiable".

However, in the last few years, there is mounting evidence that traditional anonymisation techniques do not adequately prevent the risk of re-identification of the data subject, thus leaving them vulnerable to similar threats as though they were explicitly identified. For instance, a study in United States found that 87.1 percent of the people were uniquely identified by their combined five-digit ZIP code, birthdate and sex (Sweeney, 2010 [6]). Another study re-identified data subjects based purely on their movie preferences on Netflix (Arvind Narayanan et al, 2008 [2]). Thus, the science of what data fields might lead to re-identification when combined with other fields (and even other available databases) is an evolving one.

Accordingly, in proposing a framework for open data related to Aadhaar and its uses, we begin with the foundational principle that a person's Aadhaar number or other PII can never constitute a part of an open dataset. Even when such data

is sought to be anonymised, it is critical to assess the risks of re-identification, and propose privacy principles that minimise these risks. We do not attempt a granular analysis of the re-identification risk in the sharing of raw data possibilities from Aadhaar (although such an exercise would also be valuable). Instead, we attempt to provide a heuristic by which to understand these risks, and recommend some approaches versus others. A similar study was done recently, by the Berkman Klein Centre at Harvard, which provided a risk-benefit framework to analyse open data emanating from municipal governments in the US (Green et.al.[4]).

Paul Ohm offers a sobering conclusion in his research on anonymisation and re-identification - "Data can be either useful or perfectly anonymous but never both" (Ohm, 2012 [12]). In doing so, the author highlights a necessary tension between the usefulness of data disclosures and privacy interests. In the following section we look at two methods by which anonymisation might be attempted, and identify possible points of tension:

1. *Redacting identifying information* : This is the process of redacting fields of information that are typically understood to identify individuals. In the case of, say, the telecom subscriber database, this might include name, phone number and legally mandated confidential categories like Aadhaar number. For a researcher it might well be that the existence of a unique identifier would allow far greater linkages and insights, particularly when comparing several telecom companies' datasets. However, it is precisely this that would make individuals identifiable and vulnerable to privacy threats, including from firms that seek to utilise this data for various purposes like marketing or promotions. An alternate mechanism is to hash/ transform the identifying information before it is used. Other techniques like adding "noise" - variations at random to the dataset - are also being explored as potential solutions.

   We propose that re-identification risk in any Aadhaar linked dataset, including that of telecom subscribers, even where only licensed service area, gender and age are being used as parameters, should undergo rigorous assessments to mitigate against such risks. The use of appropriate masking techniques and their effectiveness should constitute a critical element of the dataset designing process.

2. *Releasing aggregate statistics*: Ohm points to another critical lesson - when PII is actually redacted from the dataset, with minimal risk of re-identification, then the release of the dataset on its own has little value for research. In the telecom dataset example, the primary insights would be aggregate statistics about total number of male/female/transgender, as well

as statistics relating to age and licensed service area, and a combination of the three. Therefore, the release of summary statistics, without underlying full datasets, could be seen as a good starting point for facilitating more accountability, research and policy making.

Accordingly, we propose in the next section that the immediate focus could be on the release of aggregated summary statistics generated through the use of Aadhaar. As discussed earlier, there could be various granular statistics, like authentication volumes and error rates, about the operation of the Aadhaar system that would help to evaluate the various programmes it is linked to and the operation of the system itself. Similarly, crucial information about the demography is held by multiple entities, and remains unknown to both government and the public – we discussed gender-base split up of telecom subscribers and health care disbursements as some examples.

The full benefits of open data will however accrue over time, as we develop a shared understanding of Aadhaar-specific principles of anonymisation and disclosures which is then used for putting out complete datasets in the public domain, while accounting for privacy protections. Interestingly, there can also be some other innovative uses of the Aadhaar database, which can be adopted even now without disclosing sensitive personal information. For instance, the list of Aadhaar holders could be used to create a dictionary of Indian names (with frequency) and this can be tracked over time to trace the periodic shifts in the popularity of particular names.

## 4.2 Monitoring and enforcement framework

Drawing from the above discussions, we propose the need for an independent implementation structure that can leverage the existing provisions of the Aadhaar Act to create a robust open data framework. We suggest that this can be done through the creation of a multi-stakeholder 'open data committee' by UIDAI. Section 23(2)(p) of the Aadhaar Act entitles UIDAI to 'appoint such committees as may be necessary to assist the Authority in discharge of its functions for the purposes of this Act'.

The preamble to the Aadhaar Act recognises the importance of good governance and efficiency, particularly in the context of use of public resources. Further, the Aadhaar Act also lays down a number of requirements that are to be implemented by UIDAI through regulations framed by it and through the agreements that it enters into with authorised authentication and eKYC agencies. Accordingly,

the creation of a committee that can assist the UIDAI in the discharge of these activities would fall within the scope of the Aadhaar Act.

We recommend that this committee should be multi-stakeholder in character to bring in technical expertise and viewpoints from a wide range of actors. This would include representatives from the Government and UIDAI, civil society groups, open data and privacy experts and various authentication and eKYC agencies.

We propose the following steps in this regard:

**Step I**: Recognising the importance of transparency and accountability as critical tools of good governance, the government and UIDAI should agree on the key priority areas around which Aadhaar related open data needs to be be built. Given the nature of data collected by UIDAI, gender, age and geographic location, would appear to be the logical choices.

**Step II**: UIDAI should formulate a new set of regulations to implement the Aadhaar open data policy. This would include the creation of a multi-stakeholder open data committee with representation from the Government, UIDAI, civil society, authorised authentication and eKYC agencies and other experts. The regulations will encode principles and processes for generating Aadhaar related open data. This process should be accompanied by a review and amendment of existing regulations that might constrain such use. For instance, the Aadhaar authentication regulations would need to be amended to allow the authentication records to be used for the purpose of generating aggregated statistics for the release of open data.

**Step III**: The open data committee should identify the types of aggregate statistics that may be generated by (i) UIDAI; and (ii) different categories of agencies that use Aadhaar for authentication and eKYC. To the extent that disclosures are sought to be enforced through UIDAI contracts, the committee would also recommend the appropriate provisions to be incorporated in the agreements between UIDAI and the relevant agencies. This step becomes particularly important in light of the fact that the information generated by each entity would vary based on the nature of its business and the likely purpose of its linkage with Aadhaar. For instance, an e-governance programme will have very different uses of Aadhaar compared to a payments service provider or a telecom company.

**Step IV**: The committee should also drive the process of developing Aadhaar-specific principles of open data, including on issues such as anonymisation, masking techniques, interoperability, etc. This should be accompanied by an open, consultative process to test the robustness of the proposed principles and solicit feedback on the same from experts and the public. Based on the inputs

received through this process, the committee should make final recommendations to UIDAI, which should also be made available publicly.

**Step V** UIDAI should review the final recommendations of the open data committee and incorporate appropriate open data standards and provisions in the agreements entered into with different categories of authentication and eKYC agencies. In case the UIDAI does not agree with any of the recommendations of the committee, the reasons for the same should be indicated.

**Step VI**: The open data committee should also assist the UIDAI in the implementation of the open data principles adopted. They can do so by identifying potential violations and notifying UIDAI for the purposes of initiating necessary actions against any breach. It can also play a key role in adopting a communications strategy for sensitising Aadhaar users about the principles and value of Aadhaar related open data.

The proposed model will ensure multi-stakeholder participation in the Aadhaar open data framework. Further, a narrow focus on anonymised aggregate statistics in the initial phases will minimise privacy risks, while still contributing valuable data points to the public domain. The full benefits of open data will, however, accrue over time as we develop a shared understanding of Aadhaar-specific principles of anonymisation and disclosures. All of this will contribute towards better research, informed policy making, enhanced public accountability and design improvements in the Aadhaar ecosystem.

# References


[1] Amber Sinha and Srinivas Kodali, ‘Information Security Practices of Aadhaar (or lack thereof)’ The Centre for Internet and Society, https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof/view, 16 May 2017.

[2] Arvind Narayanan and Vitaly Shmatikov, Robust De-Anonymization of Large Sparse Datasets, Proceedings of the 2008 IEEE Symposium on security and privacy, 2008.

[3] Facebook Research, Disaster maps methodology, https://research.fb.com/facebook-disaster-maps-methodolog, 2017.

[4] Green, Ben, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer and Susan Crawford, Open Data Privacy (2017) Berkman Klein Centre for Internet and Society Research at Harvard University, https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook

[5] IDinsight, State of Aadhaar Report 2016-17, http://stateofaadhaar.in/wp-content/uploads/State-of-Aadhaar-Full-Report-2016-17-IDinsight.pdf, May, 2017.

[6] Latanya Sweeney, Simple Demographics Often Identify People Uniquely, Carnegie Mellon University, Data Privacy Working Paper 3, 2000.

[7] Nandan Nilekani and Viral Shah, Rebooting India: Realizing a Billion Aspirations, Penguin, 2016.

[8] Nicholas Gruen, Houghton and Tooth, "Open for Business: How Open Data Can Help Achieve the G20 Growth Target", Lateral Economics, June 2014.

[9] Open Knowledge International, What is open?, https://okfn.org/opendata/.

[10] Out-law, Government steps back from threat to legislate on midata, goo.gl/jx9Emg, 2014.

[11] Orange Telecom, Data for Development, www.d4d.orange.com, 2015.

[12] Paul Ohm, Broken Promises of privacy: Responding to the surprising failure of anonymization, 57 UCLA L. Rev. 1701, 2010.

[13] RaaG and SNS, Tilting the balance of power: Adjudicating the RTI Act, http://snsindia.org/wp-content/uploads/2017/07/Adjudicating-the-RTI-Act-2nd-edition-2017.pdf, January 2017.

[14] Randy Bean, Mastercard’s Big Data For Good Initiative, Forbes, August 7, 2017.

[15] Tim Davies and Jeni Tennison, “More than one way to open some data: government owned and government in uenced” Open Data Charter, http://opendatacharter.net/one-way-open-data-government-owned-government-in uenced/, 2017.

[16] UIDAI, Aadhaar dashboard, https://www.uidai.gov.in/aadhaar_dashboard, November, 2017.

[17] UK Department of Business and Skills, Review of midata voluntary programme, July 2014.

[18] UN Global Pulse, Mapping the Next Frontier of Open Data, http://www.unglobalpulse.org/mapping-corporate-data-sharing, Sep 17, 2014.

[19] Urvashi Aneja and Vidisha Mishra, “Digital India Is No Country for Women. Here’s Why” The Wire, https://thewire.in/139810/digital-india-women-technology/, 25 May 2017.

[20] Vrinda Bhandari, Amba Kak, Smriti Parsheera and Faiza Rahman, An analysis of Puttaswamy: the Supreme Court’s privacy verdict, https://ajayshahblog.blogspot.in/2017/09/an-analysis-of-puttaswamy-supreme.html, September 20, 2017.

# An analysis of Puttaswamy: the Supreme Court's privacy verdict

ajayshahblog.blogspot.in /2017/09/an-analysis-of-puttaswamy-supreme.html

by Vrinda Bhandari, Amba Kak, Smriti Parsheera and Faiza Rahman.

## Introduction

On 24th August 2017, a nine judge bench of the Supreme Court in *Justice K.S. Puttaswamy vs Union of India* passed a historic judgment affirming the constitutional right to privacy. It declared privacy to be an integral component of Part III of the Constitution of India, which lays down our fundamental rights, ranging from rights relating to equality (Articles 14 to 18); freedom of speech and expression (Article 19(1)(a)); freedom of movement (Article 19(1)(d)); protection of life and personal liberty (Article 21) and others. These fundamental rights cannot be given or taken away by law, and all laws and executive actions must abide by them.

The Supreme Court has, however, clarified that like most other fundamental rights, the right to privacy is not an "absolute right". Subject to the satisfaction of certain tests and benchmarks, a person's privacy interests can be overridden by competing state and individual interests. This post discusses the tests that have been laid down by the Supreme Court in the *Puttaswamy* case, against which privacy infringements will be evaluated going forward. Based on this analysis, the post argues that a majority of the judges in this decision have agreed that the European standard of proportionality shall be applied to test privacy infringements in the future. However, the rigour and technicality with which this doctrine is applied will depend on the nature of the competing interests in question and will evolve on a case by case basis. At the very least, any impugned action will continue to be tested on the "just, fair and reasonable" standard evolved under Article 21 of the Constitution. However, before we delve into the standards laid down by the Court, it is important to understand why the Supreme Court was called upon to decide if we have a fundamental right to privacy and how to read the decision it finally delivered.

## Why was a nine judge bench constituted to decide upon the right to privacy?

The question of whether or not privacy is a fundamental right first arose in 2015 before a three judge bench of the Supreme Court considering the constitutional challenge to the Aadhaar framework. The Attorney General had then argued that although a number of Supreme Court decisions had recognised the right to privacy, Part III of the Constitution does not guarantee such a fundamental right since larger benches of the Court in *M.P Sharma (8 judge bench)* and *Kharak Singh (6 judge bench)*, had refused to accept that the right to privacy was constitutionally protected. Consequently, this bench referred the matter to a five judge bench to ensure "institutional integrity and judicial discipline". Thereafter, the five judge bench referred the constitutional question to an even larger bench of nine judges to pronounce authoritatively on the status of the right to privacy.

## How do we read the *Puttaswamy* judgment?

The judgment, spanning 547 pages, contains six opinions and a lot of interesting observations. At the outset, however, it is important to note that only the majority opinion in a judgment is binding on future cases. In this case, Chandrachud J. wrote the plurality opinion, on behalf of four judges (Kehar C.J., Agrawal J., Nazeer J., and himself), while the remaining five judges (Nariman J., Kaul J., Bobde J., Sapre J., and Chelameswar J.) wrote concurring opinions. Thus, while Justice Chandrachud's opinion is the "plurality" opinion, it does not constitute the majority, since it has not been signed by a total of five or more judges. Similarly, the concurring opinions too, are not binding, and do not constitute 'precedent' for future cases. Thus, the operative part of the judgment, i.e. the *binding* part, is only the order that has been signed by all nine judges, which holds:

1. The eight judge bench decision in *M P Sharma (1954)*, which held that the right to privacy is not protected by the Constitution stands over-ruled;
2. The Court's subsequent decision in *Kharak Singh (1962)* also stands over-ruled to the extent that it holds

that the right to privacy is not protected under the Constitution;

3. The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution; and
4. The body of case law that developed subsequent to *Kharak Singh*, recognising the right to privacy, enunciated the correct position of law.

It is a well settled legal principle that a case is only an authority for what it actually decides, not any observations made in the course of the judgment or any propositions that may logically follow from it. Hence, to determine what aspects of the judgment are binding, it is important to examine each opinion, and see the point of agreement amongst a majority of the nine judges. So, if any judge agrees with a view taken by Chandrachud J. on any proposition, that would result in a majority of five out of nine, and hence, be binding on smaller benches and other courts. For instance, since a majority of the judges agree that privacy is an inalienable, natural right, that forms part of the binding element of the case.

With this in mind, let us now examine each of the opinions in *Puttaswamy* to see what they hold, how they construe the right to privacy, and what standard of judicial review they apply.

## The Court's (multiple) views on privacy

Writing the plurality opinion, Chandrachud J., holds that the right to privacy is not independent of the other freedoms guaranteed by Part III of the Constitution. It is an element of human dignity, and is an inalienable natural right. He focuses on the informational aspect of privacy, its connection with human dignity and autonomy, and rejects the argument that privacy is an elitist construct. During the course of his opinion, Chandrachud J. makes several observations about privacy in the digital economy, dangers of data mining, positive obligations on the State, and the need for a data protection law. He also raises an important point about the negative and positive elements of privacy. The former restricts the State from unfairly interfering in the privacy of individuals, while the latter obliges it to put in place a legislative framework to restrict others from doing so.

Chelameswar J. on the other hand, grounds the right to privacy, as comprising of three facets, namely repose (freedom from unwarranted stimuli), sanctuary (protection from intrusive observation) and intimate decision (autonomy to make personal life decisions). Nariman J. too, endorses Gary Bostwick's conceptual understanding of privacy as encompassing "repose, sanctuary and intimate decision". He gives further content to the right by classifying it into three categories: (1) that which involves invasion by the State into a person's physical body, (2) information privacy which captures unauthorised uses of personal information, and (3) privacy of choice, or "individual autonomy over fundamental personal choices".

For Bobde J., fundamental rights have two aspects - first, to restrict legislative powers and second, to provide the conditions for the development and dignity of individuals. Thus, similar to Chandrachud J., he recognises both the positive and negative aspects of enforcing fundamental rights, although he is clear that fundamental rights claims (as opposed to other laws) fall squarely on the State.

Kaul J., on the other hand, recognises the claims of privacy against the State *and* non-State actors. In respect of the State, he identifies concerns of surveillance and profiling, whereas in respect of non-State actors, he emphasizes on the impact of technology, in the form of pervasive data generation, collection, and use in a digital economy. Kaul J. also elaborates on the influence of big data, in particular, its impact on the actions of an individual and the resultant chilling effect it may have on free speech and expression. He thus observes the need to protect certain information from both the State as well as private actors. Finally, Sapre J. focuses his opinion on the importance of the Preamble to the Constitution, and the principles of liberty, dignity, and fraternity enshrined therein.

Given the Court's varying conceptions of privacy, it is easy to understand why the suggested standards for evaluating an infringement of the right also varied so widely. We turn to this in the next section.

## Tests for infringement of privacy

After a bumpy start in the *MP Singh* and *Kharak Singh* cases referred to above, the Supreme Court's jurisprudence on privacy evolved to accept that privacy forms an integral part of ``personal liberty" under Article 21 of the Constitution, which cannot be denied except through a "procedure established by law". The Supreme Court has clarified this to mean that the procedure prescribed by law must necessarily be "just, fair and reasonable". How this, and other standards of judicial review, will apply in the case of intrusion by the State into the right privacy, was the subject matter of much discussion in the various opinions in *Puttaswamy*. This section discusses some of the key observations.

The judgment written by Chelameswar J. provides a good overview by highlighting that the requirement of reasonableness pervades throughout Part III, albeit operating slightly differently for different fundamental rights. Accordingly, he suggests a "menu" of tests that can be used in privacy cases, depending on the underlying rights that are affected. Thus, a violation of privacy in the context of an arbitrary State action would attract a "reasonableness" enquiry under Article 14; similarly, privacy invasions that implicate Article 19 freedoms would have to fall under the specified restrictions under this constitutional provision like public order, obscenity etc; and finally, intrusion into life or personal liberty under Article 21, which forms the "bedrock of the privacy guarantee", would have to be just, fair and reasonable. For instance, over-broad telephone-tapping regulations would implicate both a citizen's freedom of speech (Article 19(1)(a)) as well as her personal liberty (Article 21). Under the Courts analysis, such a law would have to be justifiable under one of the specific restrictions in Article 19(2), in addition to being "fair, just and reasonable" as required by Article 21, as was held in the PUCL case.

Notably, Justice Chelameswar also includes a fourth test for privacy claims which deserve the "highest standard of scrutiny" and can be justified only in case of a "compelling state interest". Borrowing the strict scrutiny standard, typically reserved for discrimination cases in the U.S., he notes that there exists a category of privacy claims which must satisfy not just the tests of being "just, fair and reasonable" under Article 21, but also a higher level of importance in terms of the government's interest in the privacy intrusion. While laying down this higher standard of scrutiny, Chelameswar J., however, stops short of illustrating what sort of actions could fall under this category, and what would be the trigger for the application of this test. These issues have been left open for future Courts to deal with.

Nariman J. adds to this analysis by giving several examples to emphasise that the restrictions on privacy will need to be tested based on the combination of rights being infringed. For example, if the violation is of Article 21 read with Article 14 (right to equality), then tests of arbitrariness and unreasonableness will apply; or under Article 21 read with Article 19(1) (a) (freedom of speech), then the impugned law/policy will have to relate to the reasonable restrictions specified in Article 19(2), as described in the wiretapping example above. Thus, Nariman J., rather than elucidating a test, only clarifies that the analysis will be case by case - based on existing jurisprudence under the relevant fundamental right that is invoked. In a similar vein, Bobde J. states that privacy infringements will have to answer the tests under those particular freedoms ``in addition to the one applicable to Article 21".

Borrowing vaguely from the restrictions on the right to privacy as specified under the European Convention on Human Rights (Article 8), Sapre J. brings in a slightly different perspective. He notes that the State can impose reasonable restrictions on the right to privacy *"on the basis of social, moral and compelling public interest in accordance with law"*. If Sapre J. is indeed articulating a new test, it is unclear where its textual basis lies in the Indian Constitution, given that many fundamental rights, such as the freedom of speech and expression, do not recognise public interest as a valid restriction. Moreover, such an articulation lacks clarity on what standards will apply to judge the "social, moral, and compelling public interest" or how this would interact with Chelameshwar J's "compelling state interest" test. It may thus be better understood as a general articulation of the Article 19 standard for reasonable restrictions, which will apply differently based on the specific right that has been infringed.

Interestingly, two of the judgments (representing the views of five judges) provide more teeth in terms of how existing tests under Article 21 should be interpreted. Drawing from the concept of proportionality that is used to balance rights and competing interests under European law, Chandrachud J., notes that any invasion of life or personal liberty must meet the three requirements of (a) legality, i.e. there must be a law in existence; (b) legitimate aim, which he illustrates as including goals like national security, proper deployment of national

resources, and protection of revenue; and (c) proportionality of the legitimate aims with the object sought to be achieved. Although Chandrachud J. has used the term "proportionality", he stops short of actually adopting the very technical European proportionality standard, with its focus on narrow tailoring and least restrictive means.

Kaul J.'s "proportionality" test differs slightly from Chandrachud J. It requires (a) legality, (b) necessity (narrow tailoring) and (c) proportionality, which is closer to the European standard. He adds to this a fourth element of (d) procedural safeguards against abuse of interference with rights, which echoes Article 21's central requirement of having a "procedure established by law".

How then do we read the majority opinion on the judicial review standard adopted in *Puttaswamy*? One way of reading the judgment could be through the proportionality standard espoused by Chandrachud J. and elaborated by Kaul J. According to this, the four elements of the judicial review standard are as follows, although it is relevant to note that the additional observations made by Kaul J. do not constitute part of the "majority view":

1. **Legality**: The existence of a law.
2. **Legitimate goal**: The law should seek to achieve a legitimate state aim (Chandrachud J.). The proposed action must be *necessary* in a democratic society for a legitimate aim (Kaul J.). Justice Kaul's opinion can be read to espouse the EU narrow tailoring test.
3. **Proportionality**: There should be a rational nexus between the objects and the means adopted to achieve them (Chandrachud J.). Extent of interference must be proportionate to its need (Kaul J.).
4. **Procedural guarantees**: To check against the abuse of State interference (Kaul J.)

There was unanimity amongst the nine judges that privacy is not an absolute right, although the basis for assessing violations is less clear. While the content and applicability of the aforesaid proportionality test will be determined by subsequent decisions, what is certain is that privacy claims will be tested against the existing standards applicable under the Constitution or developed by Courts for different categories of fundamental rights. At the very least, the impugned action should satisfy the test of "just, fair and reasonable" procedure under Article 21 of the Constitution.

## Conclusion

The Court's broad interpretation of the right to privacy has paved the way for a wide range of claims. While the exact boundaries of the right will continue to develop on a case to case basis, it is clear that privacy claims will often have to be weighed against other competing interests. In the absence of a defined hierarchy among the various rights guaranteed under Part III of the Constitution, the decision in each case will vary based on facts at hand and the judicial interpretation. For instance, can the dignity of a married woman, which is central to her privacy and liberty, be infringed by a law on marital rape so as to shield the "private affairs" of the family? Does the efficiency of having a meta database of information on all citizens trump the autonomy of those who resist its adoption? Can an individual's "right to be forgotten" on the Internet override the open information needs of many others. In fact, just last week, a PIL was filed before the Delhi High Court that the restitution of conjugal rights provision in the Hindu Marriage Act and Special Marriage Act is violative of the right to privacy. The real test of privacy will lie in how subsequent Courts apply the *Puttaswamy* decision to determine these varied questions.

Vrinda Bhandari is a practicing advocate in Delhi. Amba Kak is a Mozilla Technology Policy Fellow. Smriti Parsheera and Faiza Rahman are researchers at the National Institute of Public Finance & Policy.

THE WIRE

AVIATION

# Why Having a Single Regulator Would Upset India's Game of Drones

BY TRISHEE GOYAL ON 17/09/2017 • 1 COMMENT

The regulatory spat between the DGCA and MHA is good for the future of drones in India, leading, as it hopefully will, to a holistic framework and not a blinkered approach.

Both the DGCA and MHA by themselves have an extremely limited approach towards drones. Credit: Reuters

The turf war over the regulation of unmanned aerial systems (UAS) between the Directorate General of Civil Aviation (DGCA) and the Ministry of Home Affairs (MHA) was a foregone conclusion when the latter called in for consultations almost a year after the former had formulated draft guidelines.

In response, the DGCA has set up a committee of regulators and security agencies, for 'finalising' regulations for UAS. Such inter-ministerial bickering (http://www.thehindu.com/news/national/aviation-home-ministries-spar-over-regulating-drones/article19665327.ece) is neither new nor in any way unnatural, given that regulatory stipulations don't operate within sanitised boundaries. This, however, results in inadvertent, yet avoidable, policy paralysis.

Historically, as with most robotic applications, unmanned aerial vehicles (UAVs) developed from hobbyist pursuits of pioneers and gained a further impetus due to their military applications for works considered "dirty, dull and dangerous". However, at the turn of the millennium, their civil applications grew considerably, owing to advancements in computational, imaging and communication technologies. The potential civilian uses, today, are unequivocally innumerable, limited only by the temporality of imagination.

In India, as we reimagine technology-powered governance, drones have been proposed for the use of crop insurance claims, geo tagging of assets, surveillance of national parks, crowd management, etc. However, like the benefits, the potential threats they pose to safety, property and privacy are undefinable, limited only by morbidity of imagination and omnipresent due to operational negligence. It is in this context that the ministerial tussle can be located.

Prima facie, definitionally, UAVs fall within the jurisdiction of the DGCA. Section 2(1) of the Aircraft Act, 1934 (the Act) defines "aircraft" as "any machine which can derive support in the atmosphere from reactions of the air, other than reactions of the air against the earth's surface and includes balloons, whether

fixed or free, airships, kites, gliders and flying machines" (identical definition as Annex 7 of Chicago Convention, 1944). Further, section 4A of the Act entrusts to the DGCA the performance of safety oversight functions.

This jurisdictional claim of DGCA is further strengthened by the stand of the International Civil Aviation Organisation (ICAO). The ICAO has stated in the past (in parts of the Chicago Convention) that "whether the aircraft is manned or unmanned does not change its status as an aircraft" because it locates unmanned aircrafts in the continuum of technological advancement of aircrafts. Consequently, while discussing the various regulatory aspects, it unhesitatingly discusses the role of the "State Civil Aviation Authority" and does not contemplate a division in jurisdiction with respect to UAVs. As a signatory of the Chicago Convention, this is sure to hold persuasive value in India. From a comparative perspective, Australia, Canada, China, France, Germany, Israel, Japan, New Zealand, Poland, South Africa, the UK and the US, all vest the jurisdiction with their civil aviation authorities. None of them transfer authority to a body that has not been traditionally regulating the civilian airspace.

Therefore, both legal and comparative empirical authority seem to rest heavily in favour of maintaining the jurisdictional control of the DGCA. However, before holding in favour of the DGCA, it would be prudent to consider whether there may be reason to deviate from the norm. This, especially so, because the central government has the power under Section 3 of the Act, to "exempt from all or any of the provisions of this Act any aircraft or class of aircraft".

What is required is better identification of the stakeholders in drone technology. Credit: Reuters

**DGCA turbulence**

First, the biggest worry in handing over the jurisdiction to the DGCA seems to stem from the level of (in)competence it reflected in its draft guidelines (http://www.livemint.com/Politics/bAB3DaJLWsn3B5G5AfGS7N/DGCA-releases-draft-guidelines-for-unmanned-flying-devices.html). These guidelines came under heavy criticism (https://thewire.in/53455/dgca-drone-framework-civil-aviation/) for the slipshod treatment of property and privacy concerns, apart from the obvious overlooking of international best practices. For example, while almost all jurisdictions consider a matrix of a drone's weight, purpose, altitude and distance of flight to calibrate regulations, the DGCA proposes no requirement of an Unmanned Aircraft Operator Permit (UAOP) for civil operations below 200 feet. It can be discerned how dangerous this might be, given the logically-extreme imagery of a multi-tonne unmanned airbus flying below 200 feet actually fits neatly in the stipulation (or lack thereof) of not requiring a UAOP.

The second problem is particular to India. Most of the literature on drone regulation classifies regulation on the basis of aforementioned categories of weight, purpose, altitude and distance of flight of the UAV. What is missed is the regulatory differential that comes into play with population density. For

example, the four categories that France classifies its drones into, for commercial purposes, require that either when they are flown within a populated area they shouldn't fly over any third party or not flown at all. Similarly, Japan has amended its Aviation Act in 2015 to prohibit drone flying "over a place where an event attended by many people is being held". China requires operators to report to the UAS cloud at least every second when in densely populated areas. The Federal Aviation Authority of USA has only recently opened up discussions on the feasibility of commercial drones over highly populated areas. This rationale of risk of greater harm in highly populated areas has to be considered still more seriously in the Indian context because our spatial planning does not compare to developed countries. India has the second highest urban population density in the world. Therefore, security and safety aspects of UAVs should weigh heavier on the Indian mind. This makes a case against the carte blanche authority of the DGCA, that has managed operations in controlled airspaces.

Also read: The DGCA's Proposed Drone Framework Has No Vision

The third, is a further extension of the safety aspect. Foremost, the DGCA, in its own draft guidelines, relies extensively on the 'local administration'. Their role extends to permitting flight for drones for which UAOPs are not required. This requires unmitigated and seamless police cooperation. Next, the security architecture and infrastructure that would be needed to be put in place for a decentralised airspace is arguably beyond the gambit of the DGCA. For example, setting up of electric fences to stop UAVs from entering prohibited airspace. Further, expertise in cybersecurity still remains limited with central agencies and task forces. Moreover, and most fundamentally, the availability of the required technological capability to detect low flying UAVs with the DGCA is also circumspect.

Compound to all the above concerns that the incentive for safety related self-regulation may not be as compelling for a hobbyist

drone flier as it is for airlines and the DGCA's claim of exclusive jurisdiction undisputedly stands on shaky ground.

However, to conclude from all the above reasons that the MHA should get the jurisdiction is problematic, not least of all because there could be other contenders in the ring. For example, there could be uncertainty in the say that the Department of Telecommunications would have for the allocation of spectrum/bandwidth to UAS. Similarly, the IT ministry would be keen to delineate its authority in the approving of new design lines and technology of drones before their use in India. For offences, such as hacking, committed against the UAS, there would be overlapping between the anti-hijacking and cybercrime law. This would lead to sectoral run ins which hampers long term business investment.

Not only within the central government, creases need to be ironed out between the centre and states. In India, the power to legislate on UAS seems to fall squarely with the Union via entries 29 and 30 of List I, schedule VII. However, in the US, issue of federal jurisdiction has been initially contested. Although, it has been settled in favour of the Federal Aviation Authority, state regulations are allowed as long as they don't conflict with the former. This has led to over 40 states considering laws and regulations, providing one with interesting insights into the particularisation of the law. In the Indian context, there should be more involvement with the states on aspects of notifying restricted and permitted areas for UAS operations, height at which the UAV may operate, purposes (for eg. reconnaissance) and entities that would be allowed to operate UAV with standardised permissions. In doing so, a top down approach of an MHA legislation needs to be reconsidered. Another issue with federal connotations is that there might be state amendments to provide for extenuated punishment for offences committed using drones (entry 1, List III, schedule VIII). Broader consultations will also be required on states using UAVs for surveillance by way of amendment to the Code of Criminal Procedure, 1973. This becomes more important in the context of the recent privacy judgement by the Supreme Court that requires revisiting evidence law jurisprudence in India.

Last of all, an MHA legislation would be problematic because of the perspective it comes from. Undoubtedly, the UAS technology is still developing and state's caution towards safety and security concerns is well advised. But, policymakers should not see crippling restrictions as a logical culmination of regulation. By doing so, we handicap ourselves from benefiting from the full potential of the UAS technology. The European Aviation Safety Agency outlines two main goals for UAV regulation, one of which is to "foster an innovative and competitive European Drone industry, creating new employment, in particular for SMEs [Small and Medium-sized Enterprises]". For this, it advocates "proportionate, progressive risk based" rules. To allow for such flexibility, we need to have a more permitting approach to regulation. The field should not be so cribbed and confined that for every new commercial application of the technology, exceptions from an overarching prohibition have to be created. Worse still, a culture of non-compliance. Despite the DGCA's blanket ban on UAVs in 2014, it is not uncommon to see them being at events for aerial photography. Reams of paper have been used brainstorm and put forth the way UAVs revolutionise commerce. Business models like Amazon Prime Air, Project Wing of Google, Facebook's Aquila are being shaped around UAS. In our push for "Make in India", it will be foolhardy to have a blinkered view of commercial technology.

Therefore, rather than a bid to outdo one another's claims to regulate UAS, what is required is better identification of the stakeholders in drone technology. As shown above, this will range from security agencies, Bureau of Civil Aviation Security, DGCA, information technology experts, telecom regulators, state governments, local administration, industry experts and start-ups.

This is not expected to lead to a perfect legislation all at once, but it will ensure that India's continuing evolution towards a holistic framework for drones will not be chequered.

*Trishee Goyal is a lawyer and freelance researcher.*

# Building blocks of Jio's predatory pricing analysis

ajayshahblog.blogspot.in /2017/04/building-blocks-of-jios-predatory.html

by Smriti Parsheera.

In a recent post on predatory pricing and the telecom sector Ajay Shah questions whether the subsidised user base of Reliance Jio can set off a network effect. The post makes two claims. The *explicit* claim is that the combined effect of interconnection regulation; mobile number portability and open standards of TCP/IP ensures that there are no real network effects in the telecom sector. The underlying *implicit* claim is that the existence of network effects is central to a predatory pricing analysis in this context. This piece takes a closer look at both these claims and the other factors that should inform the Competition Commission of India (CCI)'s analysis in the complaint filed by Airtel against Jio's pricing practices.

## Network effects in telecom

Modern day tariff plans, including that of Jio, comprise of three main components - voice, data and access to content - all bundled into one product. A competition law analysis of Jio's pricing strategy must focus on each of these segments individually, and then their collective effect.

*Voice services:* Telecommunication services are known to generate strong network effects - the value of having a phone number is linked to the number of people who can be called using it. This creates a classic case for concentration of market power in the hands of the incumbent. Telecom regulators have overcome this issue by mandating operators to link their networks with the networks of other operators, allowing users to communicate across networks. Research on telecom networks, however, finds that despite interoperability, users tend to display a preference for being on a larger network, particularly when operators offer lower tariffs for calls made within their networks (on-net/off-net price differentiation). Others suggest that the network effects in telecom are more 'local' in nature - the preference to be on the same network as one's family and friends leads to the formation of *calling clubs*. This is not necessarily dependent on the overall size of the network.

In summary, even with mandated interconnection norms, traditional telecom services display a certain level of network effects. Arguably, the relevance of being "on the same network" would have gone down with the convergence of voice and data services and availability of various over-the-top calling apps. This requires a deeper study of consumer behaviour and preferences in the post-data world.

*Internet services:* Network effects on the Internet are not about the provision of *Internet access services* (i.e. the data services offered by ISPs) but rather about the direct and indirect network effects that define the business models of many *Internet-based platforms and businesses*.

Telecom service providers are increasingly stepping into the role of Internet platforms by bundling access to online music, TV, movies and news along with their communication services. In Jio's case, every new SIM comes bundled with a bouquet of Jio-branded apps, making it one of the fastest growing content aggregators in the country. Its free offer period from September to March has helped Jio build a massive user base, which in turn helps in attracting other complementary users to its platform. For instance, Uber's recent decision to partner with Jio Money reflects the value that it sees in being able to access Jio's users. The same holds true for other merchants and suppliers, like providers of music, video and news content, who are attracted to platforms with a large number of users.

## Integration of data services and content

The vertical integration of data services and content offers Jio many advantages. *One*, convenient access to free content along with free/discounted data services has helped Jio in promoting higher consumption patterns. The aggressive data usage on Jio's network, particularly of video content, will gradually translate into higher revenues. The company claims that its users *"consume nearly as much mobile data as the entire United States*

*of America...and nearly 50% more mobile data than all of China."* It would be interesting to see what percentage of this data is being consumed within the Jio ecosystem and the change in consumption patterns after Jio starting charging for its data services.

*Two*, it promotes faster adoption of in-house services. To take an example, the AT&T/FaceTime case study in the United States found that less than 10 percent of iPhone users downloaded Skype while all of them had automatic access to Apple's FaceTime. Adoption of Jio Money versus rival payment apps (among Jio subscribers) is likely to show similar results. Reports about the launch of Jio's 4G feature phone with built-in Jio apps suggest the possibility of further entrenchment of new users in the Jio universe.

Can Jio's pricing strategy in telecom enable it to indulge in monopolistic behaviour in related markets like mobile payments? Unlike telecom services, the payments sector continues to suffer from the lack of interoperability among providers, leading to significant network effects. Safaricom's M-Pesa service in Kenya offers an example of how the company was able to leverage massive network effects in the mobile-money space to establish its dominance in calls and text messages. The situation in India is certainly different - we have higher levels of competition, both in telecom as well as online payments. Yet, the Kenyan example is a helpful reminder of the extent to which cross-linkages between bundled products can influence their adoption and usage, to the exclusion of other competitors.

Jio's dual role as a telecom provider and platform offering access to online content makes it difficult to outright dismiss the role of any network effects. Moreover, any subsequent recoupment of the losses suffered by Jio in its early days need not necessarily be through a significant markup in data tariffs. Increase in volume of data consumption, future monetisation of Jio apps and opportunities for utilisation of data collected from users, are all factors that must be considered.

## The tests of predatory pricing

The law and jurisprudence on predatory pricing defines it as below cost pricing by a dominant firm, with a view to exclude competitors. Sustained discounting practices in a market with strong network effects certainly raises a red flag due to the tendency of a single network to dominate the market. In such a scenario, there is a strong likelihood of recoupment after other competitors have left the market and structural barriers deter the entry of new players. The determination of predatory pricing, however, does not hinge on the existence of these network effects.

When Jio first launched its services in September, 2016 it was a fresh entrant in a market with several established players. Its price point of zero was certainly below cost but there was no question of it being a "dominant player". Any regulatory intervention to stop the pricing plans at that stage, whether by the sectoral regulator TRAI or the CCI, would have been premature.

This position has come to change over the last few months. Jio has managed to acquire a sizable presence in the market for high-speed data services - it holds about one-third of the country's broadband subscriber base and about 85 percent of the market in terms of mobile data traffic. Its share in the overall market for telecom services (voice plus data) still remains small since telecom subscribers continue to outnumber Internet users by a wide margin. The manner in which CCI delienates the "relevant market" will therefore form the crux of its analysis in this case.

Accordingly, the *first* step for CCI would be to determine whether there is a market for data services that is distinct from the broader cellular services market? This will hinge on a factual analysis of whether users regard voice, data and high-speed data services as being interchangeable in terms of their end-use and characteristics, based on a number of factors. *One*, voice calls can be made using the Internet but the reverse is not true - this indicates a one-way substitutability between the services. *Two*, there are some differences in the utility of 2G and 4G networks based on the applications that they are able to support. *Three*, CCI will need to collect data on Jio's usage patterns, that of its competitors and the switching behaviour of consumers. *Four*, supply-side constraints (like spectrum holdings) that can make it difficult for providers to switch from one type of service to another will also need to be considered.

In the *second* stage, CCI will need to examine whether Jio can be regarded as being dominant player in the identified market. Besides looking at its market share, in terms of subscriber base and usage volumes, this analysis must also consider the various other factors that have been given under the Competition Act, 2002. These include:

1. *Size and resources of Jio and its competitors* - Telecom being a capital-intensive industry has many big players. Each of them has access to significant capital resources, although there may be differences in the extent to which these firms have been leveraged.
2. *Vertical integration of the enterprise* - As discussed above, the bundling of voice, data and content offers Jio certain clear advantages. Other players are also offering similar bundles but not necessarily at the same scale. In many cases, the prices and bundles offered by other players have come about as a response to Jio's entry strategy.
3. *Entry barriers* - Telecom is a heavily regulated sector and there are entry barriers, both in terms of licensing requirements and the availability and price of spectrum.
4. *Relative advantage through contribution to economic development* - The arrival of Jio's 4G LTE network, with its aggressive pricing strategy, could also have some pro-competitive effects. Arguably, it has nudged the telecom market towards greater price competition, resulting in lower tariffs. Over time, this could also push other operators towards faster upgradation of technology.

Assuming that CCI's analysis leads it to delineate a separate broadband market (and Jio is found to be dominant in it), the *third* challenge would be to assess whether its current prices are in fact "below cost". This again will require data on the costs incurred by Jio for delivering its voice and data services and the free apps that are on offer. *Finally,* CCI will have to determine whether Jio's current pricing continues to be in the nature of a genuine "promotional strategy" by a new entrant or is it a deliberate attempt to reduce competition in the market.

Many have linked the consolidation that we are seeing in the market today with Jio's entry strategy. One one hand, consolidation reduces the number of players, hence reducing competition. On the other, it might be a sign of the sector's movement towards a more mature market with fewer players who are able to focus better on infrastructure expansion and quality of services. CCI will need to weigh in all these factors while examining the impact of Jio's prices on consumer interests, competition in the market and overall economic development.

These are all complex questions, with no obvious answers. The solution lies in a multi-stage, data-driven analysis of predation that should be rooted in an understanding of competition policy and telecom economics. Co-operation and knowledge-sharing between CCI and TRAI is key to finding these solutions.

Smriti Parsheera is a researcher at the National Institute of Public Finance & Policy. The author would like to thank Amba Kak, Kaushik Krishnan and Faiza Rahman for useful discussions.

# Predatory pricing and the telecom sector

ajayshahblog.blogspot.in/2017/04/predatory-pricing-and-telecom-sector.html

by Ajay Shah.

1. When there are network effects, we should be cautious about the business strategy of discounting. What looks like a gift to consumers today is often a plan to achieve market power and recoup those gains by extracting consumer surplus in the future.
2. The burn rate at Reliance Jio is likely to be pretty large. However, the question that we should be asking: *Can this subsidised user base set off a network effect?*
3. In telecom, interoperability regulation is in place. Even if Reliance Jio was able to establish a commanding market position through discounting, there is no way to close off its user base for rival firms. Interconnection regulation by TRAI imply that a phone call from a rival telecom company, to a Reliance Jio customer, will always go through. The open standards of TCP/IP mean that a data packet from a customer of any data communications company in the world will successfully reach a Reliance Jio customer. Even if all my friends and family are on Reliance Jio, it makes no difference to my decision to be on Reliance Jio. There is no network effect.
4. Recoupment test: If in the future, Reliance Jio tries to increase prices, nothing prevents customers from switching to rival firms. There is no reason for a consumer to stay with Reliance Jio at future dates if it turns out that Reliance Jio is expensive.
5. Market power in this industry has been checked by the three key building blocks -- interconnectivity regulation + mobile number portability + the open standards of TCP/IP.
6. In fact, there is a negative network effect, as follows. Suppose a lot of customers switch from rival telephone companies to Reliance Jio. This will clog the airwaves of Reliance Jio's base stations, so the performance of Reliance Jio will go *down* while the performance of rival companies will go *up*. Through this channel, if Reliance Jio succeeds a lot in gaining customers, it will fail in delivering the best mobile data services.

Second order issues:

1. Interconnectivity regulation imposes costs upon all regulated persons and these costs should be placed in a fair manner.
2. There is an opportunity to obtain market power in JioMoney as payment regulation lacks all three components: interconnectivity regulation + number portability + open standards.

# Emerging themes around privacy and data protection

ajayshahblog.blogspot.in/2017/04/emerging-themes-around-privacy-and-data.html

by Vrinda Bhandari, Amba Kak, Smriti Parsheera and Renuka Sane.

Issues of data protection and privacy have become the subject of intense discussion and debate, in India as in the rest of the world. In this post, we identify certain key themes that arise in the context of these issues, that can augment our understanding of privacy and data protection and help towards forging safeguards in the form of a privacy law. Many of these were discussed recently at a round table organised at NIPFP on 24th March 2017. The key themes that emerged are summarised below.

### What do we understand by privacy?

The term privacy has many connotations, takes different forms in different contexts and is viewed differently depending on the individuals own subjectivity. Defining it has been a challenge, with many scholars leaning towards more conceptual, and less rigid formulations. In philosophical debates, privacy can be characterised in terms of defining a sphere of private life that is separate from political activity and government interference. The sociological argument traces its roots in the fundamental haracteristics of social life - social context determines what is considered private in different circumstances. Others, like Solove 2006), however, move away from these conceptual discussions to identify specific privacy harms that have been recognised by society. His taxonomy of privacy encompasses four aspects - *first*, information collection (through surveillance and interrogation); *second*, information processing (through aggregation, identification etc.); *third*, information dissemination (through disclosure, exposure, breach of confidentiality etc.); and *fourth*, invasion (through intrusion and decisional interference).

Taking a slightly broader view, Calo (2011) speaks about privacy through the boundaries of subjective and objective harms. A subjective harm is *internal* to the person harmed, and is caused by unwanted observation. This encompasses, for instance, the knowledge or perception that some negative information about oneself is out there, which leads to distress and anxiety. Conversely, objective harm is *external* to the person harmed, when coerced or unanticipated information about oneself is used by other persons. Understanding of the potential harms is extremely important for the design of a policy response.

Another debate that emerges is whether privacy should be viewed as a *right*, an *interest*, or a *property*? Interestingly, the early parameters of what is now regarded as privacy evolved in the context of property rights. In 1890 Warren and Brandeis argued in a seminal paper that the right to privacy goes much beyond the concept of personal property rights, and must be recognised as such (to include for instance, the principle of an inviolate personality). By now most countries view privacy through a rights lens, because property, by its very nature, once bought, can be destroyed, transacted, and shared without the consent of the original owner. The economic dimensions of private data in the digital age have, however, once again triggered these rights versus property debates focused around the concept of "propertarian privacy".

Discussions on privacy also raise the question of *privacy from whom*. Traditionally, privacy was viewed in the context of the surveillance and law enforcement powers of the State. However, with the rise in big data and the explosion of social media, we now have to think of privacy from private actors as well, whether in the context of data mining, data retention, or data sharing arrangements. Surveillance, in this context, includes what Roger Clarke terms dataveillance - systematic monitoring of actions or communications using information technology.

### Do people in India really value privacy?

While a lot has been written about the value of privacy (for example, Westin (1968)), it is often argued that people do not really know how to gauge the value of their own privacy. Many view the debates on privacy protection as the privilege of the elite who do not have to worry about accessing basic services, or as refuge for those who have "something to hide".

It is, however, important to remember that privacy is context specific. It is not always about what one may have to hide, but also what one may have to lose. These considerations vary across class, gender, caste, age and are often be different for different intersections of these categories. For each person, there are aspects of their life that are "personal", that they do not wish to be revealed to the public at large- and the control over which is integral to their sense of autonomy. In the digital context, the oft-heard lament is that privacy does not seem to be valued enough perhaps because people either don't know or feel ambivalent about how much data they are sharing (unwittingly), to which entities and the picture of themselves that their data is able to generate to these entities.

For awareness to be effective it must move from the risks to the harm. Sunil Abraham offers a useful analogy of tobacco use. Most smokers are well aware of the risks of smoking, but do not bother to stop, until they face a health crisis. Similarly, most people, while well aware of the privacy risks associated with their activities, for instance careless use of social media, do not take any remedial action until and unless they face a data breach. Therefore, just as health policy workers have tried to change the attitudes of smokers by scaring them through the inclusion of graphic images on the cigarette packs, it might be useful to alert people to the harms caused by the loss of privacy.

## "Privacy by design" holds important lessons

The principles of Privacy by Design (PBD) developed by Ann Cavoukian are worth emphasising. The approach highlights that measures to protect privacy should be proactive and preventive, and not remedial. Privacy should be the default setting, embedded into design of technologies and services.

This overcomes many of the problems associated with choice/consent based regimes although adoption still depends on voluntary buy-in from businesses and users. So far, businesses in India are said to find an unwillingness among users to pay for privacy. For this reason, most privacy-enhancing technologies (PET) based solutions are B2B rather than B2C, and even these are far and few. We, in India, need to think of innovative ways to bring about a regime of data protection. A law on the subject and privacy-enhancing design elements are both part of the solution.

## Issues of surveillance

Perhaps the most contentious of all issues is the one on where to draw the line between privacy and security, which often requires the use of various surveillance tools by the state. The PBD framework calls for "full functionality" in this context, i.e. it seeks to accommodate all legitimate interests in a positive-sum manner. Instead of a dated zero-sum approach with unnecessary trade offs of privacy vs. security, PBD says that it is possible, and far more desirable, to have both.

Yet, in reality there remains no consensus on a) the extent to which the state is engaging in surveillance, b) the extent to which Aadhaar and other big data techniques are being deployed, and c) the relationship between national security and privacy (is balance the appropriate metaphor? what is the trade-off, if any). The State claims that surveillance fears are misguided and overstated, while civil society argues that surveillance is broad based, and inadequate checks and balances leave citizens vulnerable. Given that both national security and privacy remain nebulous terms, there is no clarity on when one gives way to the other, and it is undeniably the rhetoric of national security that invariably overwhelms privacy. This issue requires unpacking and principles-based resolution as unchecked intrusions by the State can damage the very essence of what it means to be a liberal democracy.

## Problems of Aadhaar

Given the pervasiveness of Aadhaar in our lives today, a debate on data protection cannot be complete without evaluating the legal framework surrounding it. The current legal framework of Aadhaar is weak. The Act delegates a number of core functions to be specified by the regulations, and these regulations further defer these functions as matters 'to be specified' by the UIDAI in some undefined future. This suggests that Aadhaar is currently functioning in some sort of a legal vacuum in terms of the nuts and bolts of important issues such as

enrollment, storage, and sharing of data.

The regulations that have been issued by UIDAI did not go though a rigorous consultative process - both while preparing the draft, and in seeking comments from the public. The UIDAI should voluntarily opt for greater transparency on issues that have implications for privacy and data protection.

### There is a case for a horizontal law

In India, the Supreme Court is yet to decide, what was until recently regarded a settled position - whether the right to privacy constitutes a fundamental right under Part III of our Constitution. While this is being debated, we have sector specific frameworks, like Section 43A of the IT Act, for protection of personal information and data security. More recently, the Ministry of Electronics and Information Technology (MeitY) has released the draft Information Technology (Security of Prepaid Payment Instruments) Rules 2017 for public comments. The draft rules aim to ensure the integrity, security and confidentiality of electronic payments through prepaid instruments, although amid concerns over the scope of the draft rules, MeitY's jurisdiction, and overlaps and conflicts with existing laws. Several other regulators such as the RBI, telecom authorities and health departments also have, or are in the process of developing, privacy/data protection norms pertaining to their jurisdictions.

These are all notable moves, but in the absence of a horizontal law, they will lead to the development of certain pockets of protection in certain sectors, while many other facets of private data will remain unprotected. Another concern is that the current legal framework does not hold meta data to the same standards as data in privacy and data protection debates.

There is a case for a comprehensive, principles-based, horizontal privacy law with basic minimum standards of privacy. These standards can then be tuned further to meet the requirements of different sectors. Thus, regardless of whether the Supreme Court of India considers privacy as a fundamental right, the State must define the circumstances in which it, as well as other private sector entities, may intervene with an individual's rights. Work on the draft privacy bill which began a few years back needs to be pursued with haste.

Vrinda Bhandari is a practicing advocate in Delhi. Amba Kak, Smriti Parsheera and Renuka Sane are researchers at the National Institute of Public Finance & Policy. We thank all participants at the round table on privacy and data protection organised by NIPFP on 24th March, 2017 for their contributions. Any omissions are our own.

# Competition issues in India's online economy

ajayshahblog.blogspot.in/2017/03/competition-issues-in-indias-online.html

Smriti Parsheera, Ajay Shah and Avirup Bose.

The world of high technology companies is seen as a dynamic area with a rapid pace of creative destruction. There is, however, a class of industries where there are strong network effects, where the market tends to collapse into a narrow set of players. After one burst of innovation where a new online business is born, there is the possibility of entrenched market power with the extraction of consumer surplus.

Many firms, global and Indian, have resorted to the strategy of making large losses by subsidising users, as a way to obtain those network effects. This has created a new class of concerns about predatory pricing, with unprecedented negative profit margins on a sustained basis, being supported by equity capital infusions. In the short run, discounts are popular, but recoupment is inevitable and market power will adversely affect consumers in the future.

In a recent Paper, we argue that the existing competition law regime in India needs to be fine tuned, for technology-enabled markets with significant network effects, to address the possibility of new kinds of abusive conduct. We offer a series of tangible proposals through which the Competition Commission of India can better handle these emerging situations. We also look into the role and responsibilities of the investors who back these online businesses and the impact of their conduct on competition in the underlying markets.

## Entry barriers in the new economy

Innovation is the foundation of economic progress. While we normally revere technology companies for their disruptive innovations and the efficiencies that they create, we must recognise that some technology-driven businesses are susceptible to the acquisition and abuse of market power. The Indian competition regime is an evolving one, and has only recently started facing some of these concerns. Our paper brings new evidence and arguments to the table, on these questions.

Internet-based businesses, along with several other high-technology sectors, form part of the 'new economy', characterised by high rates of innovation; low marginal cost; increasing returns of scale; and, in many cases, network effects. Direct `network effects' arise where a user's benefit from a product or service increases with the number of other users on that network. The benefit of being on Facebook or WhatsApp, for instance, corresponds with the number of friends and family who use that service. Contrast this with the benefit of having an email address, where the benefits are not limited to closed proprietary networks. This became possible due to the early adoption of interoperability standards in email protocols.

Network effects are particularly important in two-sided markets where users on each side of the market derive a positive effect from the expansion of users on the other side. Commuters who use taxi aggregation platforms like Ola and Uber will logically be attracted to a service that has a large number of drivers on its network, which yields a lower waiting time. The same is true for the drivers working with these platforms. Similarly, in case of payments wallets, in the absence of interoperability regulation, merchants and customers will both prefer a service that has the most addressable users.

With the use of modern technology, the cost of running the marketplace itself has dropped to near zero levels. As an example, the online classifieds site Craigslist reports that it has about 40 employees who manage a network that sees over 80 million classified ads per month. The marginal cost of a transaction has gone to near-zero levels. This gives a unique class of problems where technological innovation that yields cost reductions cannot be a mechanism to take on an incumbent.

## Brain versus brawn

How can market power be established, in this new world? One mechanism through which one player can obtain

a competitive advantage is to attract users through technological innovation, and thus get a network effect started. This is an attractive strategy for firms which have deep human capital. Another mechanism is by using financial capital to pay subsidies that entice users. This is an attractive strategy for firms which have superior access to financial capital. Many online businesses have resorted to practices like deep discounting, cash-back offers and other schemes designed to attract new users and establish the network effect. Sometimes, heavy losses have been sustained for years on end.

As an example, the global taxi company 'Uber' made worldwide losses in the first half of 2016 of US\$1.27 billion (approximately Rs.86.5 billion). Uber's behaviour impacts upon the Indian economy as it has applied the strategy of using financial capital as a competitive lever in India also. On a similar note, the Indian taxi company 'Ola' reported a net loss of Rs.7.96 billion in March, 2015. The company's financial records for the periods after that are not yet available although it is reasonable to expect that the losses will be significantly higher due to the higher driver incentives. In the last two years, it is estimated that the two taxi companies, Uber and Ola, burned cash adding up to about Rs. 130 billion in India.

Such behaviour is found in other industries also. In the field of payments, where regulations have *blocked* interoperability and thus created the opportunity to kick off a network effect, the firm One97 Communications, which owns 'PayTM', reported a loss of Rs.15.49 billion in March, 2016.

The scale of these discounting practices, and the sustained periods for which they are continued, has created new barriers to competition. It is difficult to rationalise these sustained losses as being an introductory offer by a new player. Rather, these practices appear to be a systematic competitive strategy. Capital has become a competitive weapon. This gives rise to concerns that the market may eventually tip in favour of the player that may not necessarily have the most innovative product or service, but one that succeeds in obtaining more capital and enticing more users in the early days, using subsidies. While seeming beneficial for consumers in the short run, such practices raise concerns about competition on account of the creation of market power, and elevated prices for consumers in the following years when losses are recouped.

The FDI guidelines issued by the government in March, 2016 turned the spotlight on pricing practices of e-commerce firms. It clarified that the automatic route of foreign investment would be available only to those e-commerce marketplaces that avoided such subsidies.

These issues have also come to the attention of the CCI in a few recent cases. In April 2015, the CCI passed a *prima facie* order recommending a detailed investigation into the allegation that, armed with substantial funding received from various investors, Ola had indulged in abusive market practices to garner greater market power in the city of Bengaluru. More recently, the COMPAT directed the Director General of the CCI to initiate a similar investigation to assess Uber's dominance in the market for radio taxi services in the National Capital Region (NCR) of Delhi after the CCI had refused such an investigation. Uber has now challenged this decision before the Supreme Court, citing a 'jurisdictional flaw' in the Tribunal's ability to order such an investigation. Alongside these developments, CCI is also reported to have set up an in-house panel to understand the cash-back incentives being offered by various online companies from the perspective of predatory pricing provisions under the Act.

Our paper explores the recent developments in India in this area, in the light of foundations of economics and competition law. It argues that there are grounds for concern about the harm to competitive dynamics from these new business strategies. At the same time, it is important to avoid intrusive interventions that bring the State into excessive involvement in the world of business.

## New economy requires new thinking

There is a need to take into account the distinct economic features of certain high-technology businesses when looking into allegations of anti-competitive conduct by them. Practices like deep discounting and cash back offers may be aimed at building sufficient scale in today's market to ensure that the business is able to fully capture tomorrow's market, to the exclusion of other competitors. A robust economic analysis of the impact of increasing returns to scale, and network effects, is required for understanding the present and future impact of these practices on competition and consumer interests. A novel dimension, which is addressed in the paper,

concerns collaboration between the investors in the multiple firms that they invest in.

## Transient gains to consumers

We examine the question about gains to consumers from discounting. We suggest that the gains in the short term need to be seen in a larger context. The recoupment test examines the extent to which market power can be achieved in the future, after which prices can be raised. If the CCI were to adopt this test in investigations relating to predatory pricing by online firms it would see that in certain areas, there are network effects, and once a small cartel of firms has acquired market power, it would be difficult for entrants to compete with them in the future. In that future scenario, it would be possible for incumbents to raise prices, and recoup earlier losses.

## Interoperability as a tool for competition policy

In some situations, the CCI could rely on the essential facilities doctrine to mandate interoperability between a dominant player that is found to be indulging in the abuse of its position and other operators in the market. For instance, imposing interoperability requirements on a dominant payments network can help extend the network effects of digital payments to the economy as a whole, rather than being limited
to a closed network. The imposition of any such requirements will, however, need to be balanced against factors such as the payment of fair and reasonable access fees, the complexity of institutional arrangements required to monitor such arrangements and assessment of the impact on future innovation. More generally, open standards are an important element of interoperability, and various arms of the regulatory State need to push in favour of competitive markets through interoperable open standards.

## Acting within Internet time

Given the fast-changing nature of online businesses, there are concerns about the elapsed time between a full-fledged investigation and the determination of a violation. We suggest a two-pronged approach to address this issue. On one hand, the CCI needs to work towards adopting stricter time frames for the disposal of cases, particularly those relating to new economy firms. On the other, we propose a voluntary settlement process that will allow a business that is under investigation to voluntarily alter its market behaviour, with the concurrence of the authority but without the need for a conclusive finding of violation by the CCI.

## Conclusion

In India, technology companies are generally revered as the source of technological progress. However, the problems of competition policy are universal and cut across all industries. The basic principles do not change. The purpose of competition policy is to stave off situations where a narrow set of firms have market power, and new players are not able to enter. Society gains when firms obtain profits and valuation through innovation, not through the crafty use of financial capital to kick off network effects.

These issues were not faced in thinking about Indian competition policy as recently as five years ago. They are, however, likely to become increasingly important in the future. We argue that this calls for fresh think about the legal framework also. There is a case for competition authorities to look into the unilateral abusive conduct of a firm, which, although not dominant at the given point of time, is engaging in anti-competitive practices that create a strong and imminent possibility of its dominance. We highlight some pros and cons of this approach and leave this question open for further research.

Smriti Parsheera and Ajay Shah are researchers at NIPFP, and Avirup Bose is a researcher at Jindal Global Law School.

# TRAI's consultation towards a net neutrality framework in India

ajayshahblog.blogspot.in/2017/01/trais-consultation-towards-net.html

by Amba Kak, Mayank Mishra and Smriti Parsheera.

### The context

The Telecom Regulatory Authority of India (TRAI) has issued a Consultation Paper (CP) on Net Neutrality seeking inputs for the formulation of final views on the subject. This comes almost a year after TRAI's regulation prohibiting discriminatory tariffs for data services based on content, framed using its power to determine the rates at which telecommunication services are to be provided. The present exercise covers a broader canvas of trying to identify the acceptable limits of interference in the provision of Internet access services. This includes practices like blocking, degradation or prioritisation of specific traffic, which often form the focus of the net neutrality debate. In TRAI's words, it is an attempt to "*rethink the first principles of traffic management by telecom service providers (TSPs)*".

While issuing the discriminatory tariff regulation, TRAI had highlighted the importance of "*keeping the Internet open and non-discriminatory*". This idea also flows through the CP and the pre-consultation paper that preceded it in May, 2016. In fact, TRAI acknowledges in the CP that the term "net neutrality" is being used in its commonly understood sense of *equal or nondiscriminatory treatment of content while providing access to the Internet*. The word "equal", however, does not appear in the ultimate question posed by TRAI on what should be the "*principles for ensuring nondiscriminatory access to content*". The CP does not clearly spell out the reason for this. It could be due to the difficulties of monitoring equality in a best efforts delivery system; or perhaps because the term non-discriminatory already captures the concept of equality.

### Key issues raised by TRAI

The CP is reasonably comprehensive in its coverage of all major aspects that countries have considered while formulating their positions on net neutrality. Several of these, like reasonable traffic management, scope of prohibited activities and need for transparency were also discussed by TRAI at the pre-consultation stage. The difference, however, is that this CP takes a deeper dive into those issues, identifying the different approaches that could be considered and, in some cases, also weighing their pros and cons. On some issues, TRAI explores new areas, not covered in its earlier papers on the subject. The following are some key points discussed in the CP.

- First, TRAI notes that each country's approach on net neutrality is defined by its local context. Accordingly, it refers to some India-specific factors that may influence its approach. These include, the predominantly wireless character of access services -- 97 percent of Internet subscribers are on wireless networks. The CP later explains that traffic management on wireless networks may pose certain unique challenges due to spectrum constraints and variable usage patterns. It also refers to India's circle-wise licensing regime which often results in the usage of third party networks outside one's home service area. TRAI queries, who will be responsible for any neutrality violations in such situations?
- Second, the CP raises pertinent questions about the appropriate footprint of regulation, in terms of the services that are covered and the persons rendering them. In particular, it refers to the potential exclusion of "specialised services", which could be defined in several different ways. The manner in which India eventually chooses to answer this question will have far reaching effects on the adoption of future technologies in the country, particularly in the context of the Internet of Things revolution.
- Third, beyond trying to identify the reasonable limits of traffic management, this CP gets into more practical aspects of detection and monitoring of violations. It also suggests a collaborative approach for implementing the operational aspects of net neutrality, which, if adopted, would be a novel approach for

the Indian telecom sector.

- Fourth, TRAI discusses the role of disclosures and transparency in guarding against discriminatory traffic management practices, an issue that was also raised in earlier consultation papers. However, in this case, it goes on to suggest two approaches on how this can be achieved -- a "direct approach" that would require a TSP to make specific disclosures only its own users; and an "indirect" one would also involve transparency towards third parties like content providers, consumers groups, research organisations and users of other TSPs.

### Scope of acceptable traffic management

The chapter on "Traffic Management" in the CP sets out the crux of the net neutrality policy debate. First, it explains why traffic management is an integral function of access providers -- to address congestion, security and the integrity of the network. Next, it notes that while such motivations for traffic management practices (TMPs) could be considered "reasonable", others might be "non-reasonable" due to their potentially discriminatory and anti-competitive effects. As such, it explains why regulating traffic management is being considered as a policy option and then mulls over the varied regulatory approaches that could be adopted.

Congestion management, which is explained in terms of the variability of demand or "peak-load", particularly on wireless networks, is explained to be one of the reasons for which access providers might legitimately engage in TMPs. TRAI recognises that the real solution to such issues lies in enhancing the overall network capacity but goes on to note that "*even in a situation of enhanced capacity, some degree of scarcity might persist*", hence creating a role for traffic management. The key takeaway from this discussion is that "*differences in network architecture and technology*" will play a role in assessing the reasonableness of any TMPs.

Next, the CP highlights that the same commercial considerations that prompt the use of traffic management tools to improve network performance could also become the cause of exclusionary or discriminatory practices. It notes that there have been global examples of TSP interference in networks for patently anti-competitive purposes, namely "*service blocking, prioritising affiliated content provider services or throttling competing ones*". While this explains the calls for regulation, traffic interference driven by commercial arrangements is not the whole scope of TRAI's enquiry. Instead, the CP provides two conceptual frames that might be used for such regulation -- the "broad approach" and the "narrow approach".

The "broad approach" appears to be a principles-based approach to identifying which practices would be considered reasonable. Drawing from the European Union's regulations, it refers to guiding principles like proportionality, non-discrimination, transparency and absence of commercial considerations that can be used to define the bounds of reasonableness. Practices like application-specific discrimination, throttling encrypted content, deep packet inspections, etc. can then be tested against these standards.

In contrast, the "narrow approach" will confine itself to formulating a "negative list" of practices that will not be permitted, without going into the contours of reasonableness. TRAI leaves the content of the negative list open for discussion, but gives the specific example of practices motivated by commercial/strategic partnerships with content companies as a potentially proscribed activity.

The distinction between the two approaches does not appear to be one of mere semantics. The paper acknowledges that a negative list is, by nature, likely to be restricted to situations that we are aware of today -- "*This may motivate providers to develop other types of business practices that are not explicitly covered in the narrow restrictions although they may have similar harmful effects*". It also notes that there could be difficulties in establishing a commercial motive. One way to address this could be to treat the lack of any objective/ technical reasoning for a traffic shaping practice as being indicative of "commercial motive", even where this may not be explicit.

By weighing these different approaches, TRAI seems to acknowledge that regulating TMPs is a tricky exercise, with high likelihood of false positives and negatives. Narrowly defined ex-ante rules may therefore be an uneasy fit with the complex and technical nature of traffic management. The controversy over AT&T restricting Apple's FaceTime application, its high-quality video-calling service, on its cellular network, presents an interesting

example. In 2012, when Apple first launched FaceTime for use on mobile networks, AT&T declared that the service would be available only on select pricing plans. On the face of it, this constitutes an application-specific discrimination that violates net neutrality principles, as pointed out by many neutrality advocates. The case, however, also throws up several complex issues, which were discussed in the case study prepared by a Working Group of FCC's Open Internet Advisory Committee.

First, pre-loaded applications, like Facetime, are likely to enjoy more large-scale adoption, thus more likelihood of creating pressure on the network -- only about 10 percent iPhone users voluntarily downloaded Skype, while all had Facetime preloaded on their phones. Second, high-bandwidth video calling applications put a particular strain on mobile data networks, in both the upstream and downstream direction. FaceTime, in particular, was found to consume "*on average 2-4 times more bandwidth than a similar Skype video call*" at that point of time. Third, limited trial deployment of a new application, for instance, by limiting it to particular pricing plans, could be useful for gathering measurement data to assist in developing better TMPs. Fourth, application management can take place on the device, as was happening in this case, or on the network -- "*whether it matters where an application-management decision is enforced, and which organization decides on it*". TRAI has also touched upon some of these aspects in the CP by raising questions on "application-specific discrimination", "duty-bearers" in a net neutrality regime and impact of traffic management at the level of the device or operating system being used by a person.

## Conclusion

The public discourse that preceded the discriminatory tariff regulation took place in the shadow of Facebook's Free Basics offering. It led to heated debates and sharply polarised views, many of which were focused on the specifics of Free Basics. In contrast, this current consultation is taking place in a relatively less charged environment, with no poster child violation. This presents an opportunity for the regulator and stakeholders to proactively engage with one another for developing a suitable framework for India that can be tested against a range of potential practices. The real test will be to ensure that whatever principles India chooses to adopt at this stage convey a strong regulatory message on non-discrimination, but also have the flexibility to adapt to the dynamic environment of this industry.

The authors are researchers at the National Institute of Public Finance and Policy.

# India needs drones

ajayshahblog.blogspot.in /2016/06/india-needs-drones.html

by Shefali Malhotra and Shubho Roy.

The two vital raw materials that went into the Indian software miracle was access to computer hardware and access to data communications. The first became possible when customs tariffs were removed, and the second became possible by opening up to private and foreign telecom companies. When thinking about another new industry, drones, it's useful to imagine: What would have happened to the Indian software industry if the coercive power of the State was deployed to ban computer usage by civilians? Registering to fly a drone in Nigeria costs \$4,000 and \$5 in the US. So far, India has banned all civilian use of drones, i.e. the cost of registration to fly a drone in India is much higher than that in Nigeria.

Drones have a variety of civil/commercial applications. In areas like crop insurance, soil mapping, disaster, conservation, traffic management, crowd management, photography and filming, drones may be a game changer. All these applications are hobbled by the ban.

The DGCA has come up with draft regulations which is designed to allow civilians to use drones. These draft regulations are not accompanied by an analysis of the costs of complying with the regulations. Moreover, these regulations do not seem to consider the needs of a nascent industry. Consequently, drone applications will remain extremely expensive in India. Capabilities in technology flow from a vibrant user community which demands increased sophistication; as long as India does not avidly *use* drones, we will not become designers and makers of drones. India's expertise in software and technology gives India an edge in this important emerging area. However, if the regulatory regime is hostile to the development of technology; India will soon fall behind.

### One example of an application of drones: Crop insurance

Insurance depends on verifying two facts. Did the insured event actually occur? And how much was the damage (monetary terms) to the insured? Today, when a Haryanvi farmers' crop gets ruined by hail, there are two problems for the insurance company and the farmer. First, did the hail storm actually take place? India does not have accurate village/taluka level weather data. Second, how much of the crop was actually damaged by the hail storm and not removed by the farmer to inflate the insurance claim? Answering these questions in rural Haryana is not easy.

While these facts could be ascertained by sending persons called "claim verifiers/processors" to farms, it is very costly to send individuals to each insured farm on repeated visits to verify claims. As farm sizes are small, the *transaction costs* of settling insurance claims become very high. This in turn makes insurance commercially unviable for insurers or the premium is too high for farmers to pay.

Drones can change this industry for the better and make crop insurance much cheaper for the insurance company and the farmer. Here is the arrangement that can be used.

When the farmer makes the initial purchase of insurance, an agent of the insurance company would map the latitude-longitude of borders of the farm. The insurance company can charter high altitude drones to collect accurate weather data. Lower flying drones can take high resolution pictures of the farm right after an insured event (hail storm) takes places. These photographs can allow an insurance company to establish if the hail storm actually damaged the crops and also the extent of damage.

Drones will be substantially faster, cheaper and probably more accurate than human verifiers. Drones can also cover much larger areas in much lesser time than individual human claim verifiers. The high quality aerial images can be processed by computers to determine whether the damage was by hail (rather than being a false claim where the crop had been harvested) and even the extent of damage. The insurance company can process

the information and transmit the insurance payout directly to the farmers account. No human intervention. In future disputes about insurance claims, these high quality images can form the best evidence to determine the truth.

This is not just a hypothetical illustration. It is coming about in India.

### Some other application areas

Farmers in other countries are already using drones to identify soil conditions, health of crops, watering needs, etc. Some of these drones cost less than Rs.5000 [link].

Farmer in China spraying crops using a drone

India has one of the lowest police to citizens ratio. Drones can increase the effectiveness of the few policemen. Common policing work like crowd management, traffic, security in large events can be helped by drones. In such areas drones are force multipliers where the Indian state can provide basic public goods like security to more citizens at lower costs. The Andhra Pradesh police has begun moving in this direction.

### The need for regulation

Any proposal to regulate must be backed by a full articulation of the underlying market failure. In the case of drones, there are two dimensions. One element of the market failure is the possibility of negative externalities in the form of harm to innocent bystanders. The other element is the possibility that drones are new weapons for committing old (IPC) crimes.

Drones are aircraft without pilots and passengers. Therefore, regulations governing certification of safety for pilots and passengers are not applicable for drones. However, just like an aircraft, drones can fly over properties and persons without their consent. Badly made or badly flown drones crashing into people or property is a concern. This justifies basic safety/quality standards for drones, and some level of competence for the drone operator.

Drones can now enable a class of crimes which were previously hard to organise. Drones have fundamentally changed the nature of privacy in ones home. High walls and thick screens are no protection against snooping by a drone which could be operated by a media company, government agency or a personal enemy. Drones can

also be used to carry out attacks by dispersing chemicals or mounting weapons. Drones can be used to spy on military establishments or carry out attacks on industrial/nuclear installations. While the easy answer for a lazy government is to ban drones, this is a very intrusive intervention. A better tradeoff in security would be to create checks and balances which permit society to gain from applications of drone technology while avoiding the problems. A natural point of departure is the registration system for cars.

India should develop the regulatory framework for drones now. Other countries are already doing this. Delaying the process will impede innovation in drones and derail development of the drone market. India will fall behind in the global drone market. One day, when India wakes up to civilian applications, we will then be a mere importer of drone technology as this knowledge will not have spread deeply in the country.

## Approach to regulation

There are three approaches to regulating drones:

1. *Banning them:* Prohibit the civilian use of drones. This is where we are today.
2. *Regulating them:* Regulate civilian use of drones to minimise the harm to others and prevent the potential misuse of drones.
3. *Regulating and encouraging them:* Positive interventions by the government to facilitate innovation.

## Regulating drones

This approach requires drone operators to comply with safety and security standards. At the same time, the cost of compliance should be borne in mind so as to not make investment in the drone industry unviable. Other jurisdictions are balancing these two competing interests through a multi-pronged approach.

Risk based regulation
: The riskier the drone operation, the greater propensity it has to cause harm to others. It follows that risky drone operations must have higher standards of compliance with safety and security requirements. For example, the US law creates a distinction between drone operations conducted for research or recreational purpose (in demarcated areas) and drone operations conducted for non-recreational/commercial purpose; which may fly over strangers who did not consent to drone over-flight. In the former case, the drone operator does not require US Federal Aviation Authority (FAA) approval, but must operate safely and in accordance with law. In the latter case, the drone operator requires specific authorisation from the FAA. The EU and UK categorise drone operations depending on the level of risk. For example, a drone operating over the open sea is less risky than a drone operating over spectators in a stadium. In the former case, a drone operation may not require any approval but may have operational limitations, such as, the drone operator should maintain visual line of sight with the drone and the drone operation should not be conducted above 400 feet. In the latter case, the drone operation may require multiple approvals, such as, design and production approval, air worthiness approval, operational approval and proof of pilot competency.

No-fly zones
: Certain areas, like nuclear installations and ammo-dumps, are sensitive. Drone accidents in such areas may cause widespread devastation. There are other sensitive areas where any breach of the security protocol may cause a national security threat, like the border of a country. Hence, there is a need for airspace restrictions to minimise the perceived harm in sensitive areas. For example, the US FAA prescribes fly and no-fly zones based on airspace-centric security requirements. These airspace restrictions are used to protect special security events, sensitive operations, high-risk areas, etc. As an example, Raisina Hill may be classified as a restricted airspace area.

Drones as weapons

Drones may be used for criminal activity, such as a terrorist attack. Developing some standards of compliance will help minimise the risk of such criminal use. For example, drone operators in the US are mandated to display the registration number of the drone, on the drone. This enables easy identification of the drone operator in the event of a criminal activity. Singapore criminalises carriage of prohibited items, like a weapon, on a drone and discharging anything, whether gaseous, liquid or solid, from a flying drone.

Privacy

Drones have been used to track unsuspecting individuals and trespass into private property or a restricted area. To prevent this, Singapore has criminalised taking photographs of a protected area (as declared by the Singapore Government) using drones. In the US, any government operated drone operation is required to comply with the provisions of the US Constitution, Federal law and other applicable regulations and policies on privacy, like the Privacy Act, 1974. The US FAA has also formulated guidelines to encourage private parties to advance privacy, transparency and accountability during commercial and non-commercial drone operations and prevent unintentional violation of the privacy of others. For example, a drone operator is encouraged to provide prior notice to individuals of the time frame and area where the drone is intentionally collecting data and develop a privacy policy for the collected data. The UK CAA has also framed similar guidelines.

## Encouraging drones

Alongside these enforcement perspectives, there is a need for positive interventions by the government to facilitate drone innovation. This approach recognises that the drone industry is in a nascent stage. The quality and pace of innovation in drones will not only depend on the players involved, but also the regulatory framework within which the innovation is taking place. These interventions may not be in the form of fiscal incentives (the most commonly used in India) but more in the nature of creating an enabling environment for the private sector to innovate and operate.

This may require a change in laws that discourage the suppliers and users of the drone industry. For example, drones actively interact with other users of airspace and should operate without causing harm to these users. To ensure this, the US FAA carries out safety studies to support safe integration of drones in the national airspace system. It may also require some institutional changes to facilitate the development of the drone industry. For example, the US FAA allocates research and test sites within the US to allow drone testing and enable development of drone technology in a safe environment.

The UK Civil Aviation Authority (CAA) supports the research and development process in the drone industry by facilitating full and open consultation with the developers of drone technology so that the CAA can provide guidance on the applicable rules and regulations. The US FAA coordinates with other Federal Agencies and the international community to designate permanent areas in the Arctic where small drones can operate 24 hours for research and commercial purposes. The US FAA has recently entered into a partnership with the drone industry to explore next steps in drone operations beyong the scope of the applicable law.

## Next steps

The DGCA draft guidelines is a step in the right direction. However, the guidelines leave much to be desired. India needs to move on to formulating a regulatory framework which regulates and encourages the drone industry. It has some natural advantage (expertise in software technology and IT) which may allow it to be a key player in the global drone market. However, if India squanders away the lead by not creating a conducive environment for drones, it will end up lagging behind other nations.

## Minimising the regulatory burden

There is a need to regulate the drone industry to minimise the risk of harm that it may cause to third parties. On the other hand the cost of compliance should not be higher than the profits/benefits. High regulatory cost will discourage players (especially small firms) from entering the market and will nip the industry in the bud. The draft regulations (in some places) have very high costs of compliance, without any attendant benefit to the society. This is a result of the *vague language* used in the draft regulations.

An example of vague language increasing the cost of the compliance is the requirement of permission for low drone flights. Regulation 5.3 of the draft regulation states:

> *the operator shall obtain permission from local administration, the concerned ADC.*

The guidelines are silent on what is 'local administration'. Is it the district magistrate, local police station, local court? No one knows. It is also not clear whether you need permission from "local authorities" *and* "the concerned ADC" or "the concerned ADC" is the "local authority". The abbreviated term ADC is not expanded or explained anywhere in the guidelines.

Such vagueness drives up the cost of technology adoption by small firms. These firms would have to run from pillar to post to get the above "permission". Since these local authorities will also not know whether they are the right "local authorities", and lack a guidance document based on which they can to analyse applications, they will probably take inordinately long or refuse.

The draft guidelines is peppered with other technical terms, like "Temporary Segregated Areas (TSA)" and "Temporary Reserved Areas (TRA)", which are also referred to but not defined. There is also no cross-reference in the guidelines allowing a reader to find what they mean and which areas they apply to. They may be the terms of art for airlines, but such opacity hampers the large technology community who must tinker with drones.

## Making regulations user-friendly

Till now, the airspace was used by a niche population, pilots. Hence, if airspace regulations were not easily available and were technical, it was not a problem. With the coming of drones, airspace will become accessible to a large section of the population from a 16 year old kid to hobbyists, researchers, companies large and small, government, etc. Airspace regulations must now become comprehensible and reader-friendly. For example, it is crucial for a drone operator to know areas where a drone can be used and areas where it cannot. The draft guidelines state that drone operations cannot be carried out in notified prohibited area, restricted area, danger area, TSA and TRA.

However, the draft guidelines do not provide much guidance on what constitutes these areas or even where one can find these areas. Although, the regulations refer to the Aeronautical Information Publication (AIP) regarding details of these terms, the AIP is not readily accessible to the general public. In contrast, the US FAA has developed an app (B4UFLY) illustrating the fly and no-fly areas for ready reference of drone operators. Using this app, a 12 year old child can understand where to fly a drone.

## Conclusion

Induction of drone technology into India is, at present, very costly. When authorities, processes and systems are unclear in a law, the potential cost of getting a drone permission can literally be infinite. There is no way to know which authority to apply and the authority itself does not know whether he/she has the power to grant an application. We need clearer regulations, and we need a regulatory framework to support the industry.

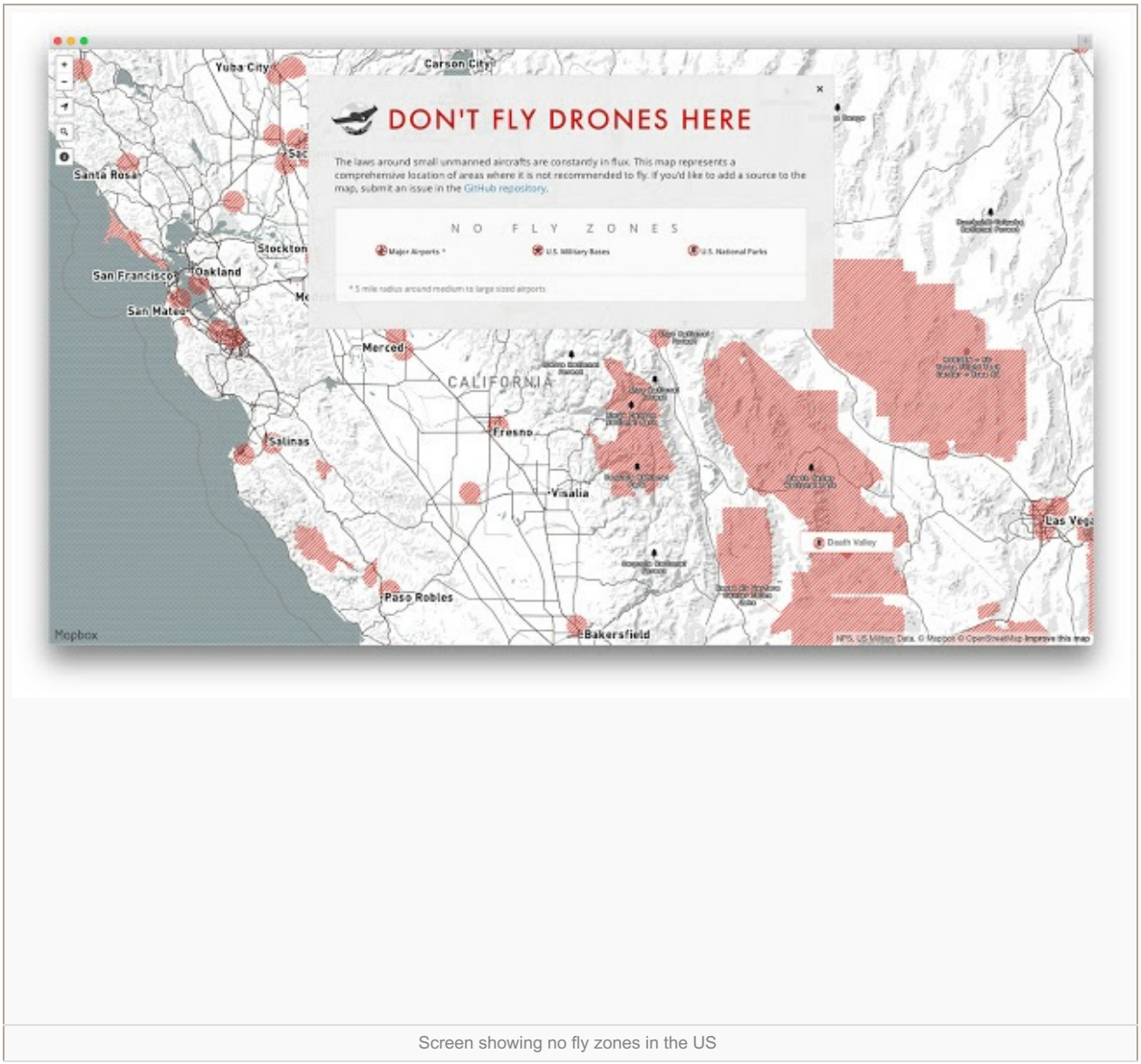
## References


Subtitle B, Title III of the US *FAA Modernisation and Reform Act, 2012*.

EASA *Proposal to Create Common Rules for Operating Drones in Europe* (September 2015).

CAA *CAP 722: Unmanned Aircraft System Operations in UK Airspace: Guidance* (March 2015).

Singapore *Unmanned Aircraft (Public Safety and Security) Act 2015* (No. 16 of 2015).


Screen showing no fly zones in the US


Johan Hauknes and Lennart Nordgren, *Economic rationale of government involvement in innovation and the supply of innovation-related services*, STEP Report Series R-08 (1999).



The authors are researchers at the National Institute for Public Finance and Policy. They thank Sumant Prashant, Bhargavi Zaveri and Pratik Datta for discussions.

# Towards a privacy framework for India in the age of the internet

ajayshahblog.blogspot.in /2016/11/towards-privacy-framework-for-india-in.html

by Vrinda Bhandari and Renuka Sane.

The Supreme Court order during the Aadhaar hearings in August 2015, that raised the question of whether privacy is even a fundamental right under Part III of the Indian Constitution, brought the debate on the right to privacy at the forefront in India. More recently, the *Laksh Vir Singh Yadav v UOI* case pending in front of the Delhi High Court has led to discussion on the merits and demerits of the right to be forgotten. The Delhi High Court, has in this case, reportedly asked the Centre and Google on whether the right to privacy includes the right to delink irrelevant information from the internet.

What separates these two cases is the different nature of the parties involved. The first is largely related to the dangers of unfettered surveillance by the State. The second is related to the immense power wielded by private actors such as Google and Facebook in the new-age digital economy. What is common between the two, however, is that they open up the question on the right of privacy of personal information.

How should we think about the right to privacy? Who do we need privacy from? What are the consequences of inadequate privacy protections? What principles should underlie a privacy law? A lot of work has been done on the examination of the state of law of privacy in India (CRID, 2006; CIS, 2011; Justice Shah Report, 2012). In a recent paper, *Towards a privacy framework for India in the age of the internet*, we contribute to the debate on privacy in India in two ways. First, we conceptualise the right to privacy in the context of the State and private actors in the age of the internet and big data. Second, using globally accepted privacy principles, we propose a privacy framework on the basis of which to evaluate any future privacy law.

## Privacy from whom and why?

*Privacy from the state*

Traditionally, we thought of privacy as privacy from surveillance by the State. Governments' wield enormous influence and have coercive powers including those related to law enforcement and criminal justice. This made citizens wary about the invasion of their privacy by the State.

The government's surveillance capabilities have vastly improved over the last couple of decades. The emergence of new technologies comes with the possibility of misuse, especially considering the relatively low level of effective oversight and awareness about such programmes. The right of privacy against the State is thus premised on the idea of personal freedom in a liberal democracy, and primarily focused on surveillance and information gathering.

*Privacy from private actors*

Private actors were never really the focus of the privacy debate. This has, however, changed with the rise of big-data and of global corporations such as Google, Facebook, and Amazon, whose business model relies on the collection, storage, and use of customer data. It has also been aided by the increasing popularity of social media, which encourages people to share more information about themselves.

The right to privacy against private actors is founded on principles of contract law, most prominently involving notice and consent. It is focused on the collection, storage, processing, transfer, and use of personal data of customers for business purpose.

Would simple disclosure policies be enough to prevent any privacy violation? We think, not. This is because of

what is seen as a privacy paradox, where users profess to, and are indeed, concerned about their right to privacy, but their behaviour does not reflect their apprehensions. In fact, very often, not only do individuals fail to understand the fine print of privacy policies, we see that individuals often view such policies as guarantees of data protection, instead of liability disclaimers for firms.

With the ease of tracking our movements through geo-location and wifi on smartphones, and the data sharing requests sent by the Government to these corporations, the difference in the privacy protections sought against the State and private entities is slowly disappearing.

*Consequences of loss of privacy*

Inadequate privacy protection can have significant consequences - ranging from identity theft, and increased profiling and discrimination of individuals, to a loss in free speech due to an ensuing ``chilling effect''. Privacy protections are thus required not only from the State but also from the private sector. In fact, a recent Nasscom-DSCI survey showed that inadequate data protection frameworks were causing losses worth billions of dollars to the Indian IT-BPO sector, in part because India's data protection regime was not considered adequate by the EU.

## Framework for a privacy law

A privacy law has to inevitably deal with two competing concerns. The first is that of national security vis-a-vis privacy. The second is that of the big data's multitude of benefits vis-a-vis the costs of the loss of privacy. The design of a law, therefore, is a not a simple question of enacting a law where privacy trumps every other consideration - be it security or big data benefits - every time. We use the nine principles enumerated by the Justice Shah Report (2012) as the basis for a national privacy legislation in India.

We propose certain design elements that can be a part of a national privacy legislation. These are:

1. Objective of the privacy law
2. Value of personal data
3. Scope and ambit of the law
4. Coverage
5. Principles governing collection and retention of data
6. Principles governing use and processing of data
7. Principles governing sharing and transferring of data
8. Rights of users
9. Supervision and redress mechanisms

## Conclusion

In India, in the absence of an over-arching law, our regulatory surveillance architecture is heavily weighted in favour of the State. This is extremely problematic as mass surveillance is being carried out in a legal vacuum, with little regard for the effect on individuals' rights to privacy. In such a situation, regardless of whether the Supreme Court of India considers privacy as a fundamental right, the State must define the circumstances in which it may intervene with an individual's rights. Similarly, law must define how private sector entities deal with user data.

An important limitation of our framework is that it does not deal with traditional modes of surveillance and information gathering. Further, while privacy is understood variously as being linked to decisional autonomy,

secrecy, and freedom from intrusion, both in the physical and information data sphere, we focus primarily on data privacy and the privacy of personal information. Finally, it is important to bear in mind that any law on privacy will have the un-enviable task of keeping pace with the development of technology.

## References


CIS (2011). *Privacy in India - Country Report*. Centre for Internet Society, Privacy India, Privacy International, Society in Action Group.

CRID, University of Namur (2006). *First Analysis of the Personal Data protection Law in India*. Report delivered in the framework of contract JLS/C4/2005/15 between CRID, the EU Directorate General Justice, Freedom, and Security.

Justice Shah Report (2012). *Report of the Group of Experts on Privacy*. Government of India, Planning Commission.

Moore, Adam (2008). *Defining Privacy*. In: J. of Soc. Phil. 39.3, pp. 411–428.



Vrinda Bhandari is a practicing advocate in Delhi. Renuka Sane is a researcher at the Indian Statistical Institute, Delhi.