RGICS

RAJIVGANDHIINSTITUTEFORCONTEMPORARYSTUDIES
JAWAHARBHAWAN,DR.RAJENDRAPRASADROAD,NEWDELHI-110001

RGICS
Issue Brief

(October 31, 2016)

Good Governance, Privacy and Surveillance

Prepared by: Niharika Bapna
(Under the guidance of
Ms.Barkha Deva)

RGICS Issue Brief

Good Governance, Privacy and Surveillance

I. Key Issues

- India has a number of separate and large database that capture identity information, including personally identifiable data
- Linking of all these databases with identity information should be a cause of concern considering it makes personal identity information vulnerable to misuse
- Individuals should worry about surveillance, even if they are always on the right side of law
- As biometrics become a part of metadata without safeguards to prevent misuse, is the present government stepping towards aggressive biopolitics?
- India will have to strike a balance between the right to privacy, security and good governance
- Current legislative framework cannot protect Indian citizen's privacy rights
- Internationally surveillance is undertaken under strong oversight legislation, India should follow example
- The way forward

II. Key Messages

- The good from good governance does not overpower the harm from not recognizing a fundamental human right of privacy of individuals, as the former is not immune to vagaries of politics.
- Aadhaar is likely to be used for State surveillance as the government has drafted rules to allow retention of record of services and benefits availed using Aadhaar number.
- There is no legislative oversight or judicial redress in case there is a breach of sensitive biometric data; considering the high costs and information asymmetry involved, individuals will have none to scanty legal recourse.
- It is true that there are many sections of our population who are more concerned about basic needs of food, shelter, safety etc. but that does not mean we understand civil liberties and personal freedom restrictively; rather we need to actively work to expand these rights.
- In India, the battle is not about preserving bodily privacy by not relinquishing biometric or identity information, rather it is about fighting for a right of privacy against surveillance.

The ruse that Aadhaar will be *voluntarily* obtained *random* number should have been obvious to policy makers, especially since the Union Finance Minister described Aadhaar number as an entitlement which is "mandatory if you want a benefit"[i] in the Parliament. The recent announcement declaring possession of Aadhaar number mandatory for availing LPG subsidies marks the beginning of making this 12-digit number a sine qua non. This would surely facilitate use of tax money for good governance by prevention of leakages, fulfilling the sole objective of the legislation for disbursal of subsidies, services and other benefits; as was emphasized by the government when they pushed for the Aadhaar Bill to be listed as a money bill.

Scope Creep: The recent developments around Aadhaar have become a cause of extreme worry. There is a large unexplained and unjustified gap between what Aadhaar was supposed to be and what it has become or rather will become. In a case of absolute task over reach the government drafted rules that will allow it to keep a record of all the services and benefits availed using the Aadhaar number for seven years, allowing users to check their records only for two years.[ii] With no Parliamentary oversight in drafting of these rules which exceed the legislative scope of the Act, this move of the government has shown a total lack of accountability to the people.

A multitude of questions arise- What is the need for data retention of services and benefits availed using the Aadhaar number? What happens if users have to check or correct their data post two years of availing the Aadhaar number? Why the Aadhaar legislation is, n this very underhand manner, being built to engage in mass surveillance? If this was what was intended why was the Aadhaar bill clandestinely passed as money bill? Can the dubious intentions of the government be inferred from the fact that it is still hesitant to consider the AP Shah Committee report to develop a privacy framework? Why even now there is no Parliamentary Oversight over how this government is continuously expanding the scope of Aadhaar? Will this government even proffer a justification for engaging in surveillance by the surreptitious exploitation of what was otherwise a benign 12-digit number?

It is difficult to answer these questions if one is on the other side of the government especially as new announcements regarding Aadhaar keep coming up, unbound by the diktat of the legislation that was drafted to govern it.

India has a number of separate and large database that capture identity information, including personally identifiable data

The erstwhile Unique Identification Scheme and now Aadhaar, is neither the first nor the only government initiative to collect biometric information. Many government initiatives have already been collecting personal identity information and others (mentioned below) are being actively being pushed to bolster State surveillance.

The National Population Register, under the aegis of the Ministry of Home Affairs, has an objective to create a comprehensive identity database of every 'usual resident' in the country. This database would contain demographic as well as biometric particulars.[iii] Due to an overlap of collection of biometrics by UIDAI as well as NPR, in 2012 it was an executive decision of the Manmohan Singh-led cabinet to give the former precedence, leaving the Home Ministry with just three major states —Odisha, Tamil Nadu and West Bengal — apart from six north-eastern states and Jammu and Kashmir for biometric collection under NPR.[iv]

Post the 26/11 Mumbai terrorist attack in 2008 the then UPA government envisaged two projects- NATGRID to counter terrorism and CCTNS to counter national crime and criminals. NATGRID (National Intelligence Grid) can access 21 sensitive databases relating to domains such as banks, credit cards, cell phone usage, immigration records, motor vehicle registrations, Income-Tax records and NCRB into a single database for access by authorised officers from 10 central agencies such as RAW, IB, CBI, DRI and ED. It is essentially a collation of all of this information that will give Law Enforcement and Intelligence Agencies a 360 degree view of a suspect. While CCTNS (Crime and Criminal Tracking Network System) entailed digitisation of data related to FIRs registered, cases investigated, and charge sheets filed in all police stations, in order to develop a national database of crime and criminals. NATGRID was criticised by civil liberty activists on grounds of possible infringement of privacy and by members of the then Opposition political leaders. The current Union Finance Minister Arun Jaitley himself expressed his worry regarding sharing of 'actionable intelligence'. He states that while generic intelligence can be shared the specifics under actionable intelligence 'can never be put on such grids' as this will be counter-productive.[v] In a dramatic turn of events the present government is now keen on implementing NATGRID without having formulated privacy legislation before hand.[vi] It has rather decided to revive NATGRID which would, according to the current plan, collect sensitive information from 21 sets of data sources such as banks, credit cards, visa, immigration and train and air travel details, as well as from various intelligence agencies.[vii]

Another government program is the Centralized Monitoring System (CMS) which is a telephone interception provisioning system, said to be operational since March this year. In simpler words the intelligence agencies will now be able to lawfully intercept calls or messages without a need to approach the telecom operator first.[viii] And thus one layer of scrutiny based on a record of the approval process is removed as far as telephone interception is concerned especially since this layer would have been a repository of the paper or electronic trail for these requests. Without this layer there is no way of, albeit ironically, monitoring the number of government interceptions under the Centralized Monitoring System.

India has also attempted to unabashedly engage in mass surveillance. The Network TRaffic Analysis system or NETRA developed by a lab under Defence Research and Development Organisation (DRDO) is an internet spy system in order to intercept and examine communication over the Internet for keywords like "attack," "bomb," "blast" or "kill" by examining tweets, status updates, emails, chat transcripts and even voice traffic over the Internet (including from platforms like Skype and Google Talk) in addition to scanning blogs and more public parts of the Internet.[ix] The Global Technology Information Report (2015) while expressing concerns regarding the potential of NETRA of being a mass surveillance program states that between July-December, 2014 the Indian government made the second highest number of requests in the world for access to user to data to internet based platforms.[x] The present government's inclination to spy on the internet through "online filters" is evident from two reports of the Intelligence Bureau that were leaked to the media.[xi]

Linking of all these databases with identity information should be a cause of concern considering it makes personal identity information vulnerable to misuse

Aadhaar has been widely and rightly criticised for the repository of biometrics it creates for the most populous democracy and then leaves the same vulnerable to the possibility of some very serious transgressions. Similar arguments can be made against all the other government programs attempting to engage in surveillance. But what is scarier is the possibility of all these programs sharing their data with each other which would result in creating a mammoth database of personal information of individuals.

Aadhaar has the capability to link different databases[xii] and a good example of it is the proposed 'India Stack' program that would allow fin-tech firms to make finance friendly. Essentially the government, under the Digital India initiative, has mandated an open architecture for the five programmes that can 'talk' to each other: Aadhaar, e-KYC (know your customer), e-Sign (legally accepted digital document signing), privacy-protected data sharing, and the Unified Payments Interface or UPI that allows money transfer using a single identifier.[xiii] How protected is our financial information in this scheme of *privacy-protected data sharing* when there exists no right to privacy (as stated by the Attorney General in the Supreme Court last year) or legislation to mandate the same?

There is no end in sight on the road where biometrics can be linked across platforms and used without adequate and impartial monitoring. This linking of platforms has commenced as Madhya Pradesh police is considering linking Aadhaar card number to CCTNS to identify offenders easily[xiv] thus perpetrating a 'once an offender always an offender' mindset; as in the current scheme of things it is unclear if an individual would have the option to delink his criminal past from his personal identity even after serving time.

This sharing of information raises numerous questions- what will be the protocol governing the sharing of this information? What will be the norms governing data mining? Will we have agency-specific protocols on what information can be shared with whom and under what conditions? As Partha Mukhopadhyay had argued, "to protect privacy, each such database will need additional locks. Linking databases should need consent from multiple key-holders subject to legislative oversight and judicial redress."[xv]

With the government introducing controversial provisions through rules appended to Aadhaar legislation, blatantly ignoring to work on the 2011 AP Shah Committee report and making statements about absence of right to privacy in the Supreme Court, it is making a mockery of consent, legislative oversight and judicial redress.

Individuals should worry about surveillance, even if they are always on the right side of law

The disclosures of the former CIA employee Edward Snowden revealed the numerous global surveillance programs undertaken by the National Security Agency in 2013. Speaking on the issue of privacy Snowden commented that the common defence against right to privacy- *I do not need a right to privacy because I have nothing to hide*- is not a strong enough counter to obliterate the need for a right to privacy. He says so on two grounds- first, Snowden states that the justification for individuals refusing to assertively demand a right to privacy is the same as saying there is no need for right to free speech as they have nothing to say; and second the need for a right, in this case a Right to Privacy, does not need to be justified as the burden of justification lies upon one who is seeking to infringe it.[xvi]

Both the above arguments are important as India attempts to contextualize privacy rights. By pitting efficiency in disbursal of government subsidies, services and benefits through Aadhaar card and reducing threat to national security by national/international elements through government monitoring under NATGRID, CMS, NETRA, CCTNS, NPR, the State has saved itself from discussing the absolute lack of recourse left for individuals seeking remedy for misuse of personal identity information by the State or other entities. Sunil Abraham[xvii], a vociferous supporter of digital privacy, explains this looming threat in simpler terms. He says-maintaining a central database is akin to getting the keys of every house in Delhi and storing them at a central police station.[xviii] Will the naysayers agreeing to no urgent need for right to privacy also be agreeable to such an arrangement?

The personal identity information collected by the mentioned surveillance projects are the 'key' that are stored with the government. Even the 'innocuous' Aadhaar number does not escape this aspersion despite having a legislation to monitor it. Even though Section 33 of the Act states that identity information collected for the purpose of generating the Aadhaar number shall be confidential and not be revealed by the Central Identities Data Repository, the Oversight Committee that ensures the same is composed of the government employees themselves – a clear maker –checker conflict. Without a clearly articulated right to privacy right or legislation to tackle surveillance under what law and in which manner is an individual supposed to challenge the State?

As biometrics become a part of metadata without safeguards to prevent misuse, is the present government stepping towards aggressive biopolitics?

Not only that the stated Oversight Committee does not adhere to the international standards prescribed by the UN High Commissioner for Human Rights Navi Pillay in a detailed report on 'The Right to Privacy in the Digital Age' in July 2014. The report stated clearly that internal procedural safeguards without independent external monitoring are inadequate for the protection of rights. Thus the system by which a Joint Secretary is authorised to issue orders which then are reviewed by three Secretaries, as per the Oversight Committee constituted by the new Aadhaar legislation, is not acceptable. Ms. Pillay's report said that effective protection of the law can only be achieved if all the branches of government as well as an independent civilian oversight agency are built into the procedural safeguards.[xix] Thus, the assurances by this government stating that privacy of identity information has been dealt with in the Aadhaar legislation itself clearly have dubious foundations.

The definition of biometric information as per the Aadhaar Act is very wide comprising of photograph, fingerprint, iris scan, and also allows discretion to include any other biological attribute of an individual as may be specified by regulations.[xx] This also aggravates the fear in case this information is compromised. One of the risks that we are subjecting our population is to religious/caste based profiling. As the Aadhaar number ceases to be a *random number* since June this year when the Centre directed all State Governments to link Aadhaar card number to the caste certificates issued to school students, the possibility of such profiling is not mere conjecture as this information is directed to 'fed into the Meta Data to be made online.'[xxi]

The government argues that biometrics will aid in identification of individuals to avoid pilferage while delivering government subsidy, benefit or service. However, as individuals whose biometrics will be under the government's control, we need to be wary of the fact that biometrics have since a long time associated with biopower and biopolitics. These are concepts developed by French philosopher Michael Foucault. According to him biopolitics works at a general level rather than through 'diagnostic scrutiny of the individual' aimed to identify risk groups, risk factors and risk levels. The transactions under this system characterise individuals by their capacity and identify them through 'pins, profiles, credit scoring, etc. rather than their subjectivities'. This dilution of subjectivity while characterising individuals reduces the possibility of resistance in governance thereby making it more effective.[xxii] Considering the recent attempts to expand the scope of Aadhaar is this government moving towards aggressive biopolitics?

India will have to strike a balance between the right to privacy, security and good governance

Consequences of a possible data breach become even more pertinent in case of Aadhaar since it collects the immutable biometrics of the second largest population. If this data is breached neither the people nor the government has any plan of recuperation from what would be a massive shock. Lack of national privacy legislation, with a system for making parties pay damages when they injure individuals by losing their critical personal information, prevents a legal respite as 'the courts may have no opportunity or power to deal with the consequences of poor planning and hasty public policy after the fact'.[xxiii] Information is power and by allowing the government to exercise this power over us without thought for the rule of law constitutes the ultimate submission possible in a democratic nation-state.[xxiv]

Mass surveillance threatens to halt the expansion of civil liberties, personal freedom and is further an infringement of democracy. Targeted surveillance requires reasons to be given for surveillance of particular people, this is not the case when it comes to mass surveillance which will be a consequence of the above mentioned surveillance projects and generation of Aadhaar number. It is true that there are many sections of our population who are more concerned about basic needs of food, shelter, safety etc. but that does not mean we understand civil liberties and personal freedom restrictively; rather we need to actively work to expand these rights.[xxv] Individuals need to be protected against arbitrary interference in case mass surveillance. Currently in India there is no independent regulatory body or the judiciary to oversee that there is no abuse of surveillance systems.[xxvi]

In 2013 the Supreme Court adjudicated retired Karnataka High Court judge K.S. Puttaswamy's plea demanding scrapping of UIDAI scheme as it was not backed by legislation or constitutional provisions. While the Supreme Court bench conceded that there were certain 'aberrations' in the scheme it would not be wise to view the issue only from a privacy angle as larger section of the Indian population would not see that as the main issue while they struggle for food and water.[xxvii] As is evident from the court's observations and also the discourse regarding right to privacy, this right is understood to be a homogenous right. However, unlike other fundamental rights the privacy is a more nuanced right.

Bhairav Acharya, a constitutional lawyer who has extensively worked on free speech, privacy and technology, opines that privacy is a mutable concept without a single meaning. Different variations of privacy are dissimilarly applied in unrelated situations due to which the 'right to privacy' is a misnomer because it conveys singularity. Instead there are multiple rights to privacy, some of them only distantly related and therefore care needs to be taken to correctly match each privacy argument to its corresponding privacy right.[xxviii] Parting with certain personal information to avoid leakage in order to receive gains from the State would be an amenable proposition to beneficiaries. However this cannot be an excuse to not articulate a right to privacy at all. It has rightly been observed that an absolute denial of privacy will defeat democracy, but so will an absolute right to privacy.[xxix]

This was also the view held by the now Finance Minister, Arun Jaitley albeit a few years ago when he was a member of the Opposition. In an article written for the BJP blog Mr. Jaitley opines that- "*Every citizen in India has a right to privacy. His right to privacy is an inherent aspect of his personal liberty. Interference in the right to privacy is interference in his personal liberty by a process which is not fair, just or reasonable.*" Identifying the right to privacy in the strictest sense, as articulated by Samuel Warren and Louis Brandeis in 1890, Mr. Jaitley construes it as every person's 'right to be left alone'. Advocating for a liberal society he asserts that no place for those who 'peep' into the private affairs of individuals.[xxx] Sadly, his stance regarding privacy has not been as clear as when his party formed the government and the Aadhaar Act was debated.

In India, the battle is not about preserving bodily privacy by not relinquishing biometric or identity information. Rather it is about fighting for a *right* against surveillance. In current times it is probably expedient to collect personal information in the interest of national security but there is no justification for not providing individuals with any legal recourse whatsoever in case of unjust, unfair and unreasonable infringement of their rights.[xxxi]

Current legislative framework cannot protect Indian citizen's privacy rights

As we contextualize right to privacy as a protection from surveillance in the present document, it should be known that there are only two major statutes that deal with digital and telephonic surveillance. These are specifically Section 69 and 69 A of Information Technology Act, 2000 and Rule 419 A of the Telegraph Act, 1885. Both Acts provide for interception of communications in certain cases and are considered inadequate in regulating mass surveillance as they fail to address issues relating to the collection of, access to, sharing of, disclosure and retention of data.[xxxii] Some provisions from other legislations like the India Post Office Act, 1898, Section 91 and 92 of the Criminal Procedure Code, 1973 deal with surveillance indirectly. These statutes only 'deal' with instances of digital and telephonic interception and do not provide a strong recourse to the individual which is what has been lacking in India.

It cannot be emphasized enough how important it is to have an overarching privacy legislative framework for India. As privacy concerns are not contextualized adequately we are unable to deal with the repercussions of their transgressions. Instead of loosely using the term privacy there is an urgent need to define it and legally identify it by defining its current vague and often confused form. There is a difference between the public right to privacy against the state and the private expectations of privacy we have against other people. As a public right, privacy protects people from unwarranted intrusion by the state.[xxxiii] In India, this right is located in Article 21 of the Indian Constitution which guarantees the right to personal liberty. In addition to the judiciary locating privacy rights through its judgments an assertive stand by the legislature on privacy issue is necessary. The Planning Commission had held meetings of the Group of Experts on Privacy Issues throughout 2012, which was chaired by Justice AP Shah. It enlisted nine national privacy principles that must form the bedrock of India's first privacy legislation. Following are the nine principles as arrived at by the AP Shah Committee[xxxiv]:

The first principle of notice states that the data collector should notify all individuals of its information practices, before any personal information is collected about them.

The second principle of choice and consent states that the data controller should provide individuals the choice to opt-in or opt-out with regards to the provision of their personal data, as well as that individual consent should only be taken by the data controller after providing notice of its information practices.

The third principle of collection limitation states that the data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent from the individual taken.

The fourth principle of purpose limitation states that personal data collected and processed by data collectors should be adequate and relevant to the purposes for which they are processed.

The fifth principle of access and correction applies to individuals. In particular, this principle states that individuals should have the right to access their personal information which is being held by a data controller and to make corrections or to delete information when it is inaccurate.

The sixth principle of disclosure of information prohibits the data controller from disclosing personal data to third parties, unless informed consent has been provided by the individual for such disclosure.

The seventh principle of security states that data controllers should be responsible for ensuring the security of all personal data that they have collected or which is in their custody.

The eighth principle of openness requires data controllers to take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

The ninth principle of accountability states that the data controller should be accountable for complying with measures which give effect to the privacy principles.

No legislation including the Aadhaar Act, 2016 gives prominence to privacy as per the nine principles comprehensively identified by the AP Shah committee. While parting with personal identity information will aid technology in providing for smoother governance, we cannot forget that technology does not work in a silo. It influences lives of individuals and changes the relationship between an individual and the State and therefore has to have social or political implications. The mentioned privacy principles offer a greater bargaining power to an individual as compared to the State or even a private entity.

The simple case of right to privacy stands on the reasoning that if collection of biometrics and other identity information is for the benefit of the people at large then there is no reason why these people are not offered legal protection in case their data is compromised.

Internationally surveillance is undertaken under strong oversight legislation, India should follow example

Modern nation states with porous borders and seamless technology beyond geographical boundaries see surveillance as a necessity. This however cannot be an excuse for unchecked surveillance power.

The USA Freedom Act, 2015 imposes some new limits on the bulk collection of telecommunication metadata on U.S. citizens by American intelligence agencies, including the National Security Agency. There has been rewriting of surveillance laws post the Snowden era in the USA. There are statutes that are criticised for not executing their objectives like the Foreign Intelligence Service Act, 1978 which originally had a primary purpose to ensure that the US government would be barred from ever monitoring the electronic communications of Americans without first obtaining an individualized warrant from the FISA court, which required evidence showing "probable cause" that the person under surveillance was an agent of a foreign power or terrorist organization.[xxxv] The important takeaway is that there is statutory monitoring of surveillance activities of the State, which presently are absent in India.

Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. The persons or organisations collecting and managing this personal information are liable to protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law. Although Europe does not have any specific laws to govern surveillance the general Protection Regulations monitors the processing of personal data within European Union and also UK's Regulation of Investigatory Powers Act, 2000 is used as a general guideline.

In the United Kingdom, the Regulation of Investigatory Powers Act, 2000 governs the provisions for surveillance and investigation by governmental bodies. This Act provides guidelines to public authorities desirous of obtaining private information. The Act specifically mentions that surveillance and investigation can be done in case of terrorism, crime, public safety or emergency services. Another significant legislation of UK is the Intelligent Services Act, 1994 which inter alia establishes a procedure for the investigation of complaints about the Secret Intelligence Service and the Government Communications Headquarters. The GCHQ is a British intelligence and security organisation responsible for providing signals and information assurance to the British government and armed forces.

A case in point is the National Identity Documents Act, 2010 passed by the UK Parliament 'destroyed' the National Identity Register which was a database containing the biographic and biometric fingerprint data of card holders, created via the Identity Cards Act 2006. The then Home Secretary, Theresa May, stated that the Act was a first step to reduce the control of the state over decent, law-abiding people and hand power back to them.[xxxvi] India has a lot to learn from US, UK and Europe in terms how to balance the need for surveillance as well as preserve individual autonomy. This learning has to be incorporated and legislative changes need to be introduced to further the same.

The way forward

Once the bunch of privacy rights are broken down for understanding our right against surveillance emerges as an important condition to limit pervasive governmental observation of our activities. It is no one's case that personal identity information should not be collected to foster efficiency in governance. The argument is that good from good governance does not overpower the harm from not recognising a fundamental human right of privacy of individuals. This argument assumes significance as methods of governance unlike a legally defined privacy right is not immune to the vagaries of politics. What is the bulk personal datasets that will now be retained as per the Aadhaar rules used to keep a tab on those who criticise the government actions or initiatives? Will such people be then persecuted or even prevented from availing benefits? Whatever be the course adopted by the government, we can be sure of one thing that the individual being so persecuted will have feeble to no legal remedy against it.

The need of the hour is not curbing collection of identity information is but strengthening individuals to negotiate in case their information is compromised in any manner is a legal necessity. This is particularly significant as even infants are being now enrolled for Aadhaar number. In the interest of the rights of this future generation that may not agree with the possibility of surveillance owing to a decision taken by their parents there needs to be a legal remedy. Akin to the international practice of legislating on State surveillance, India too needs statutory recognition for state surveillance. Starting with the nine principles enlisted by the AP Shah Committee report parent privacy legislation must be formulated by the present government.

References

[i] Uncorrected debates of Rajya Sabha dated 16.03.2016 Available at: http://164.100.47.5/newdebate/238/16032016/Fullday.pdf Accessed on 06.10.2016
[ii] Aloke Tikku, "Government to Keep Aadhaar Records for 7 Years, Prompts Fears of Surveillance", Hindustan Times, October 17, 2016 Available at: http://www.hindustantimes.com/india-news/govt-to-keep-aadhar-record-for-7-years-activists-worried/story-jSY820Ee1ZnQNLL5vuWMOI.html Accessed on 24.10.2016
[iii] National Population Register Available at: http://censusindia.gov.in/2011-Common/IntroductionToNpr.html Accessed on 06.10.2016
[iv] "Modi's Aadhaar Bill May Choke Advani's Citizenship Card Plan", The Hindustan Times, March 8, 2016 Available at: http://www.hindustantimes.com/india/modi-s-aadhaar-bill-may-choke-advani-s-citizenship-card-plan/story-tUX2lW4IAAA0XEMGsNArNO.html Accessed on 06.10.2016
[v] Uncorrected debate, August 4, 2011 Available at: http://164.100.47.5/newdebate/223/04082011/Fullday.pdf Accessed on 21.10.2016
[vi] In the first week of October members of the Parliamentary Standing Committee on Home Affairs questioned home ministry officials on why projects like NATGRID and NCTC have been slow to take off Available at: http://indianexpress.com/article/india/india-news-india/s-y-quraishi-ila-sharma-kiran-bedi-maneka-gandhi-hrd-iit-natgrid-3074304/ Accessed on 13.10.2016
[vii] "Revive NATGRID with safeguards", The Hindu, January 2, 2016 Available at: http://www.thehindu.com/opinion/editorial/revive-natgrid-with-safeguards/article8054989.ece Accessed on 06.10.2016
[viii] "Government's Call Intercept System to be Ready by End of Fiscal Year", The Hindu, December 3, 2015 Available at: http://www.thehindu.com/business/central-monitoring-system-to-be-ready-by-end-of-fiscal-year/article7941946.ece Accessed on 06.10.2016
[ix] Chinamyi Arun, "Big Brother is Watching You", The Hindu, January 3, 2014 Available at: http://www.thehindu.com/opinion/op-ed/big-brother-is-watching-you/article5530857.ece Accessed on 06.10.2016
[x] Siddharth Deb, "India Only Partly Free When it Comes to Internet Freedom", The Wire, November 8, 2015 Available at: http://thewire.in/14963/india-only-partly-free-when-it-comes-to-internet-freedom/ Accessed on 06.10.2016
[xi] "The Government is Watching Over Even your Internet Usage", The Scroll, March 16, 2015 Available at: http://scroll.in/article/713966/never-mind-the-snooping-on-rahul-the-government-is-watching-over-even-your-internet-usage Accessed on 06.10.2016
[xii] Pratap Bhanu Mehta, "Privacy After Aadhaar", The Indian Express, March 26, 2016 Available at: http://indianexpress.com/article/opinion/columns/privacy-after-aadhaar-money-bill-rajya-sabha-upa/ Accessed on 14.10.2016
[xiii] Monika Halan, "Coming on a Screen Soon All Your Money", The Livemint, September 7, 2016 Available at: http://www.livemint.com/Money/GpUnXkfU5ELaHNre2Ov2UP/Coming-on-a-screen-soon-all-your-money.html Accessed on 14.10.2016
[xiv] "MP Cop Mull Aadhaar Link to Track Criminals", Times of India, October 7, 2016 Available at: http://timesofindia.indiatimes.com/city/bhopal/MP-cops-mull-Adhaar-link-to-track-criminals/articleshow/54727211.cms Accessed on 14.10.2016
[xv] Pratap Bhanu Mehta, "Privacy After Aadhaar", The Indian Express, March 26, 2016 Available at: http://indianexpress.com/article/opinion/columns/privacy-after-aadhaar-money-bill-rajya-sabha-upa/ Accessed on 14.10.2016
[xvi] "In One Quote Edward Snowden Summed Up Why Our Privacy is Worth Fighting For", Tech.Mic, May 29, 2015 Available at: https://mic.com/articles/119602/in-one-quote-edward-snowden-summed-up-why-our-privacy-is-worth-fighting-for#.0kmjlK1GO Accessed on 14.10.2016
[xvii] Executive director of Bengaluru based-research organisation The Centre for Internet & Society
[xviii] "Aadhaar Cards Have More Details Than Any US Surveillance", Business Insider, March 16, 2016 Available at: http://www.businessinsider.in/Aadhaar-cards-more-intrusive-than-US-surveillance/articleshow/51426959.cms Accessed on 14.10.2016
[xix] Chinamyi Arun, "Privacy is a Fundamental Right", March 18, 2016 Available at: http://www.thehindu.com/opinion/lead/lead-article-on-aadhaar-bill-by-chinmayi-arun-privacy-is-a-fundamental-right/article8366413.ece Accessed on 14.10.2016
[xx] Section 2(g), Aadhaar (Targeted Delivery of financial And Other Subsidies, Benefits and Services) Act, 2016
[xxi] Refer to question no. 9. Available at: http://ccis.nic.in/WriteReadData/CircularPortal/D2/D02adm/FAQ-21062016.pdf Accessed on 8.9.2016
[xxii] Btihaj Ajana, "Surveillance and Biopolitics", Electronic Journal of Sociology (2005)
[xxiii] Eben Moglen and Mishi Choudhary, "Yahoo!: A Cautionary Tale", The Hindu, October 19, 2016 Available at: http://www.thehindu.com/opinion/columns/yahoo-a-cautionary-tale/article9235740.ece Accessed on 24.10.2016
[xxiv] Bhairav Acharya, "Privacy in Peril", Frontline, July 12, 2013 Available at: http://www.frontline.in/cover-story/india-privacy-in-peril/article4849211.ece Accessed on 14.10.2016
[xxv] Jean Dreze, "The Aadhaar Coup", The Hindu, March 15, 2016 Available at: http://www.thehindu.com/opinion/lead/jean-dreze-on-aadhaar-mass-surveillance-data-collection/article8352912.ece Accessed on 14.10.2016
[xxvi] "Big Brother is Watching You", The Hindu, January 3, 2014 Available at: http://www.thehindu.com/opinion/op-ed/big-brother-is-watching-you/article5530857.ece Accessed on 14.10.2016
[xxvii] "Privacy Debate on Aadhaar", The Telegraph, November 26, 2016 Available at:

http://www.telegraphindia.com/1131127/jsp/nation/story_17616903.jsp#.WACmI_l97IU Accessed on 14.10.2016

[xxviii] Bhairav Acharya, "The Battle for a Right to Privacy Has a Long Way to Go", August 2, 2015 Available at: https://bhairavacharya.net/2015/08/06/the-battle-for-a-right-to-privacy-has-a-long-way-to-go/ Accessed on 04.10.2016

[xxix] "Aadhaar and Right to Privacy", The Livemint, July 28, 2015 Available at: http://www.livemint.com/Opinion/3kjHJ0Z7cwhuBgxETejCAI/Aadhaar-and-the-right-to-privacy.html Accessed on 14.10.2016

[xxx] Arun Jaitely, " My Call Detail Records and a Citizen's Right to Privacy" Available at: http://www.bjp.org/index.php?option=com_content&view=article&id=8683:article-shri-arun-jaitley-on-qmy-call-detail-records-and-a-citizens-right-to-privacyq&catid=68:press-releases&Itemid=494 Accessed on 14.10.2016

[xxxi] Article 21 provides- No person shall be deprived of his life or personal liberty except according to procedure established by law. In the landmark case of Maneka Gandhi versus Union of India (1978) the Supreme Court observed that the 'procedure established by law' needed to be just, fair and reasonable to deprive a person of his life or personal liberty.

[xxxii] "Policy Recommendations for Surveillance Law in India", Centre for Internet and Society Available at: http://cis-india.org/internet-governance/blog/policy-recommendations-for-surveillance-law-in-india-and-analysis-of-legal-provisions-on-surveillance-in-india-and-the-necessary-and-proportionate-principles.pdf Accessed on 14.10.2016

[xxxiii] "The Battle for Privacy Still has a Long Way to Go", The Wire, August 8, 2015 Available at: http://thewire.in/7685/the-battle-for-a-right-to-privacy-still-has-a-long-way-to-go/ Accessed on 15.10.2016

[xxxiv] "Policy Recommendations for Surveillance Law in India", Centre for Internet and Society

[xxxv] "FISA Court Oversight: a Look Inside a Secret and Empty Process", The Guardian, June 19, 2013 Available at: https://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy Accessed on 16.10.2016

[xxxvi] "Identity Cards and National Identity Register to be Scrapped", May, 2010 Available at: https://www.gov.uk/government/news/identity-cards-and-national-identity-register-to-be-scrapped Accessed on 28.10.2016