Article

Uncertainty and Insecurity in Privacyless India: A Despotic Push towards Digitalisation

P. Arun

Department of Political Science, University of Hyderabad, India.
arun.p@uohyd.ac.in

Abstract

In November 2016, an unexpected imposition of a demonetisation policy in India by Modi's government changed the role of digital technologies in mundane lives. It was unfolded with a discourse of its potential to generate a trail of long-term benefits; such as reduced corruption, enhanced governance and greater digitizing of the economy which could eventually lead to development of the nation. This road to development was radical, coercive and even authoritarian as it drove individuals to adopt digital technologies.

Such a despotic push in one of the world's largest democracies had consequential effects on individuals' privacy and altered the nature of surveillance. The grand digitalisation project was veiled and fanatically endorsed with a tunnel vision while any robust privacy legislation to protect the flow of data was absent. This article intends to investigate the political dimensions and consequences. It will trace the contours of a despotic and authoritarian push by the government to digitise mundane lives. Therefore, it will unravel the nature of governance under the new emerging technologies, legalities, and interlinking policies to understand the persistent uncertainty and perpetual fear of insecurity under this Privacyless India.

*Everyone is breathless and choking up. Here deaths are not mourned anymore.
Rather the death of privacy is celebrated and jubilation can be seen even at the graves.*

Introduction

Is it a gimmick or sorcery? It would be inappropriate to regard the novel developments in digital technologies as such because they have rather unleashed a kind of grandeur experience to human senses which essentially assists in their mundane lives. Digitising has significantly enhanced our capacities and means to collect, store, process and communicate information. These advancements got immensely interwoven into our mundane lives which is observed as digitalisation. Unknowingly, this has unleashed a thread of unforeseen effects on individuals' privacy due to the creation and sharing of data. Therefore, the burgeoning issue in this age of information revolves around privacy. Despite being one of the fundamental concerns in our modern lives, it is still crawling around the cradle. And it is quite evident from India as the

right to privacy is not a constitutional right.¹ Though there had been efforts to legislate over the right to privacy bill, not just once but twice, in 2011 and 2014, yet it could not acquire statutory existence (Greenleaf 2014a, 2014b). The bill is stalled as it is undergoing the process of drafting and it is still lingering around the inter-ministerial consultation (Rajya Sabha Debates 2016). This is because the biggest impediment was to address the suggestion from Ministry of Home Affairs about the blanket exemption to the Law Enforcement Agencies and government's intelligence units.²

Despite the fact that India is under the ambit of lackadaisical privacy framework, which superficially resembles a data protection law. The journey to establish a legal framework for privacy originated from the 1997 Resolution adopted by the General Assembly which drove India to frame laws for Electronic Commerce in the global arena. After three years, it led to the formulation of Information Technology (IT) Act (2000) with which India embarked into the 21st century. Though there was selective patchwork in the following years with subsequent amendments which aimed to address the growing concern with data protection and privacy (Section 43, 43A, 72A of IT Act 2000 (2008)); the most recent one was the Draft IT (Security of Prepaid Instruments) Rules, 2017 which is supposed to address the issues surrounding electronic payment transactions and it is still under deliberations (MeitY 2017). In contrast to that, the Indian state also amassed the power to surveil and intercept personal data from private entities through major amendments in legal regimes, along with technological innovations in surveillance techniques (Abraham and Hickok 2012: 302-315; SFLC 2014). The provisions under the legal regime comprise both extraordinary laws and ordinary laws to address different situations respectively (Singh 2007, 2014). These laws equip the state with not merely proactive (routine and periodic disclosure) and reactive surveillance (disclosure on specific request by state), but they are also used to transforming itself with an apparatus of systematic surveillance (state's real-time access to information). The latter involves surveillance techniques such as Central Monitoring System (CMS), National Intelligence Grid (NATGRID), Network Traffic Analysis (NETRA) (Xynou and Hickok 2015). It also includes the grand biometric identification programme known as Aadhaar³ or Unique Identification Number (UID); though introduced to streamline governance, it is also interlaced with the surveillance apparatus, which provides a real-time access to information about individuals (discussed below).

With the abovementioned massive apparatus, India's surveillance state aspires to create an atmosphere of security and safety. Paradoxically, they have also unleashed a kind of uncertainty and insecurity in this age of information. The following section will focus on the spiral events and despotic push towards digitalisation.

'Digital India': Leveraging Technology and Empowering Society

On July 10, 2014, the government proposed to launch a pan-India programme named "Digital India" in its Union Budget 2014-2015. In order to address the "imminent need to further bridge the divide between digital haves and have-nots" several policies and schemes were proposed. It was called a clarion call for E-Kranti (Electronic Revolution) in government service delivery and governance (Budget Speech 2014). Though this is not the first instance of a transformative decision—in 2006 the National e-Governance Plan was also launched under the UPA (United Progressive Alliance) regime—however, the 2014 BJP led NDA (Bharatiya Janata Party led National Democratic Alliance) regime launched Digital India to give greater

¹ A constitutional bench is looking into the matter on infringement of right to privacy due to Aadhar and also whether privacy is a constitutional right or not in Justice K.S. Puttaswamy (Retd.) & Another vs. Union of India (WPC) 494/2012.

² *Indian Express*. "Policy paralysis? Privacy and false claims laws caught in the crossfire." March 6, 2017. Accessed April 28, 2017. <http://www.newindianexpress.com/nation/2017/mar/06/policy-paralysis-privacy-and-false-claims-laws-caught-in-the-crossfire-1578328.html>.

³ The word Aadhaar means foundation.

thrust towards e-governance. The plan aims to “build a digitally empowered society and knowledge economy by leveraging Information Technology as a growth engine of new India” (PIB 2014). Until now it was merely a novel push by the government towards Digital India, as a panacea to transform India, by harnessing digital technologies and making it accessible to people in order to empower them through digital services.

However, there was a perceptible change, as the technology was leveraged as a rational and efficient approach for social organisation, administration and management. Following the same rationale, a 12-digit biometric identification programme named ‘Aadhaar’ was launched in order to facilitate the efficient delivery of welfare services. It all commenced under the UPA regime not through statutory law but with a notification in 2009. After two years, there was an effort to give it a statutory backing. However, the Parliamentary Standing Committee on Finance rejected the National Identification Authority of India (NIAI) Bill 2010. The committee pointed out the absence of data protection legislation, dangers and issues like access and misuse of personal information, surveillance, profiling, linking and matching of databases and securing confidentiality of information (PSC 2010). Later, the BJP led NDA government, in March 2016, passed Aadhaar Act in parliament as a money bill despite severe furore in the parliament, several apprehensions in public domain and its own criticism while being in opposition during UPA regime. The programme was held to provide good governance and enable efficient and transparent delivery of entitlements to individuals.

Digital technologies were gradually being harnessed in common livelihood. However, a sudden outbreak of demonetisation policy by the Reserve Bank of India (RBI) on November 8, 2016, accelerated the cash-crunch Indian economy to forcibly adopt non-cash methods or cashless methods (credit or debit cards, mobile wallets and electronic fund transfer mechanisms and many more) for monetary transactions.⁴ As the flow of cash and lower denomination notes in the circulation deteriorated, the government initiated a despotic push towards digital currency again under the Digital India campaign. Eventually there was a sudden surge of consumer base and amount of transactions through E-wallet Apps (such as Paytm, Mobikwik, Freecharge etc.) as India’s central banking institution RBI did not restrict the electronic means of payments (RBI 2016b). Prior to demonetisation, in August 2016, the government launched its own mobile digital payment application named Unified Payments Interface (UPI),⁵ similarly later in December 2016 another app was launched named as BHIM (Bharat Interface for Money).⁶ In order to promote digital transactions, it also launched promotional schemes⁷ to entice individuals to adopt digitalisation.

⁴ According to the Government, demonetisation was unleashed to tackle three issues; the circulation of fake currency notes, black money, financing terrorism and economic security (MoF 2016). However, its goalposts shifted towards cashless economy and promoting benefits of Digital India.

⁵ *The Hindu*. “Change the way you pay with Unified Payments Interface.” April 13, 2016. Accessed April 29, 2017. <http://www.thehindu.com/business/Economy/Change-the-way-you-pay-with-Unified-Payments-Interface/article14235265.ece>.

⁶ *Indian Express*. “People can now bank with thumb using BHIM app: PM Modi at Digi Dhan Mela.” December 30, 2016. Accessed April 29, 2017. <http://indianexpress.com/article/india/bhim-app-narendra-modi-digi-dhan-mela-demonetisation-4452004/>.

⁷ Lucky Grahak Yojana (Lucky Consumer Scheme) and Digi Dhan Vyapar Yojana (Digi Money Business Scheme) (PIB 2016).

Figure 1: Advertisement to go Cashless and Digital⁸

The government claims that their Digital India programme is a tactical tool to fight against corruption, promote financial inclusion of poor, bring financial accountability, and also to provide digital convenience and accessibility. The following section will critically explore the previously mentioned massive surveillance apparatus and the frequent iteration of digitalisation as how it all leads to state authoritarianism, and consequentially alters the nature of privacy and surveillance in India.

Trails of Uncertainty and Insecurity in India's Surveillance State

The extensive utilisation of digital technologies was advocated for administrative expediency, and here the biometric identification system became a harbinger for governance through Digital India. In contrast to its purpose of streamlining governance architecture, it also contains the provision of disclosure of information (identity information or authentication records) for national security. Instead of giving a blanket exemption, the act offers protection from any sort of blatant misuse, as it lays out an oversight committee (consisting of the cabinet secretary and the secretaries of the Department of Legal Affairs and the Department of Electronics and Information Technology, Government of India).⁹ This committee would act as a channel to

⁸ "Pamphlets." *Digital Jagriti*. Accessed April 30, 2017.

https://s3.amazonaws.com/DFIAA/Cashless_payment_banner_blue_V13.jpg.

⁹ Clause 33 (2) says "any disclosure of information, including identity information or authentication records, made in the interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorised in this behalf by an order of the Central Government: Provided that every direction issued under this sub-section, shall be reviewed by an Oversight Committee consisting of the Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology, before it takes effect: Provided further that any direction

review any unlawful surveillance by the government. However, if we look at the legacy of the oversight committees, especially in anti-terror legislation in India it shows that there is a sheer absence of political will to deliver transparency and accountability (Singh 2007: 153-154).

It all occurred as an aftermath of 26/11 Mumbai terror attacks in India. Instead of employing the technologies for an exclusive purpose, there were widespread interlinking technologies. This is because it serves a range of desires—verification of identity, or for prevention, detection, investigation transparency, accountability, surveillance, and much more. By interlocking biometric identification system with Intelligence Grid and the National Population Register,¹⁰ the colossal database can be shared with various other intelligence agencies and government departments for national security and surveillance (Singh 2014: 53-54). For governance, the government is interlinking Jan Dhan,¹¹ Aadhaar and Mobile (JAM Trinity), which aims to implement direct transfer of benefits through banks in an efficient, leakage-proof, well-targeted and cashless manner (ES 2017). Furthermore, it has also interwoven biometrics with many more policies and practices. Despite a series of judgements where the Supreme Court¹² clearly stated enrolment to Aadhaar to be voluntary and prohibited denial of service to any individual who could not obtain the Aadhaar card,¹³ the state blatantly violated the court order and released a series of notifications in which it made the card mandatory to avail various essential services and basic amenities.¹⁴ The state even went a step further and manipulated the interpretation of the court judgement; by regarding the biometric authentication ‘not mandatory’ to ‘compulsory’ for obtaining a new telephone connection and also update connection with Aadhar (Krishna 2017b). It completely defeats the idea of limited government and rule of law in a democratic governance.

Under the Digital India programme, it was avowedly claimed that the new technologies contain appropriate provisions of informational privacy and digital security. But it was hogwash, as prior to demonetisation, there had been two biggest financial data breaches in the banking history of India.¹⁵ Whereas in the post-demonetisation period there have been regular data leaks; also there is publicly available data of not merely Aadhaar related information, but also other categories of sensitive personally identifiable information of

issued under this sub-section shall be valid for a period of three months from the date of its issue, which may be extended for a further period of three months after the review by the Oversight Committee. (Aadhaar Act 2016).

¹⁰The pilot project UID commenced to provide universal identity and remove ghost-beneficiaries, now it is being linked with NPR data to find out ghost residents. See Indian Express. “Government out to match Aadhaar, NPR data.” July 6, 2016. Accessed April 28, 2017. <http://indianexpress.com/article/india/india-others/government-out-to-match-aadhaar-npr-data/>.

¹¹ Pradhan Mantri Jan-Dhan Yojna (Prime Minister’s People Money Scheme) aims to bring financial inclusion of poor by opening their bank accounts.

¹² For more details on court rulings see Krishna (2017a).

¹³ Though it restricted its voluntary usage to only six government schemes, (Cooking Gas (LPG), Public Distribution System (PDS), Employment Guarantee Scheme, Jan Dhan accounts, Employees’ Provident Fund, and National Social Assistance Programme) and even held that no person would be denied access to any service, until the final verdict is delivered by the apex court which is going to evaluate constitutional existence of privacy and privacy violations in Aadhar.

¹⁴ For more information about the list notifications (SFLC 2017).

¹⁵ *Economic Times*. “3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit.” October 20, 2016. Accessed April 28, 2017. <http://economictimes.indiatimes.com/news/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms>.

beneficiaries or subjects¹⁶; digital fraud through the BHIM app,¹⁷ and also via the e-Wallet app,¹⁸ collectively all of them indicate the amount of insecurity persistent in the emerging technologies. In response to these attacks, the government aims to establish the Computer Emergency Response Team for Financial Sector (CERT-Fin) (Budget Speech 2017). Still, the degree of insecurity is much higher as both the RBI circular (RBI 2016a) and recent Draft IT Rules 2017 framed by MeitY (2017) stressed that the private entities are supposed to provide adequate data security, but they did not emphasise any kind of liability and penal provisions if they fail to do so. Under this debilitated situation, it creates serious uncertainty and insecurity to individuals' personal information and informational privacy.

Another major insecurity arises from the dangers of state surveillance. The Indian state intends to have proactive or real-time access to the humungous flow of data in the technologies developed by private entities. Unlike the encryption dispute between Apple vs. FBI in United States, in India, Blackberry was compelled by the state in 2010, to either provide access to security agencies to monitor their services or face a ban. And the company finally agreed to provide access to partial services.¹⁹ Later, the state again intended to acquire blanket and real-time access to encrypted data as it released a Draft National Encryption Policy in 2015, making it mandatory to store data in plain text (unencrypted) format for 90 days (DNES 2015). Later it released an addendum (ADES 2015) by giving exemptions to social media platforms like WhatsApp, Facebook, Twitter, payment gateways, e-commerce and many more. After severe apprehensions against a policy to establish a surveillance state, later it was withdrawn.

Information is under siege not merely due to state, but even from the private entities. Since the post-demonetisation campaign of Digital India, the state has been constantly pushing people to move ahead with digitalisation. However, private entities are waiting to exploit personal data to expand their business through Big Data analytics. Unlike the traditional currency which leaves no trail, the digital payment holds the potential to leave its trail as individuals in their mundane lives drop their digital footprints in every digital transaction and movement. It is quite visible as people are bombarded with frequent mails, popups and SMS (text) messages of advertisements and solicitations.

Under this ubiquitous digital governance, individuals need to interlace themselves to surveillance and keep their identity visible and transparent. Here, interlocking and bringing synergy between technologies is encompassing, penetrating and even governing individual democratic rights and liberties through digitalisation, and it raises severe apprehensions of expansive state authoritarianism. The apprehension is not coming from luddites who are trying to undermine the role of cutting-edge digital technologies. Rather it is germinating from the prevailing janus-faced nature of governance in India; 'allocative governance' and 'authoritative governance.' The roadmap for development is being laid out with the help of modern

¹⁶ For more information about data leaks see: Centre for Internet & Society report on Information Security Practices of Aadhaar (CIS 2017); *Scroll*. "Jharkhand, Chandigarh Govt Websites Leak Aadhaar Data of Lakhs of People. Is Aadhaar Really Secure?" April 25, 2017. <https://scroll.in/article/835546/the-centres-casual-response-to-aadhaar-data-breaches-spells-trouble>.

¹⁷ *Outlook*. "50 People Pull out Rs 6.14 Cr Using UPI Lacuna; BoM Files Case." March 11, 2017 Accessed April 28, 2017. <http://www.outlookindia.com/newscroll/50-people-pull-out-rs-614-cr-using-upi-lacuna-bom-files-case/1005177>.

¹⁸ 15 people allegedly done fraudulent refunds worth Rs 6.15 lakh from a payment gateway of e-wallet company Paytm. See *Indian Express* "CBI Steps in to Probe Rs 6-lakh Paytm 'fraud'." December 17, 2016. <http://indianexpress.com/article/india/cbi-to-probe-paytms-rs-6-lakh-fraud-complaint-4430853/>.

¹⁹ The company responded by providing lawful access to BlackBerry Messenger (BBM) and BlackBerry Internet Service (BIS) email, but it denied decoding of its intranet facility in BlackBerry Enterprise Service. *Daily Mail*. "No secrets on Blackberry: Security services to intercept information after government gets its way on popular messenger service." April 7, 2012. Accessed April 29, 2017. <http://www.dailymail.co.uk/indiahome/indianews/article-2126277/No-secrets-Blackberry-Security-services-intercept-data-government-gets-way-messenger-service.html>.

technological paraphernalia in which the former is used to enhance individual livelihood. Whereas the latter one reflects a disguised political surveillance which is guided to induce state's ideological and developmental discourse. The presence of such political surveillance turned out as a dragnet to surveil and prevent oppositions, movements and counter dissenting voices against the State.

It was quite apparent by the authoritative actions, in three notable incidents: when tribal activist Gladson Dungdung's passport was impounded in 2016,²⁰ in 2015 a look out circular was issued on Greenpeace activist Priya Pillai and prevented her from travelling abroad,²¹ and in 2014 Amnesty International's Christian Mehta was deported.²² Evidently, the investigating agencies had been surveilling their actions and movements. It was not any random sorting; rather it was an intentional and purposeful sorting. Here it was their personal details which were utilized to monitor and restrain their right to travel. The abstract data was manipulated for a particularly defined authoritative purpose. It became possible when data collection became material, and also when the analysis of information about populations could be done in order to govern their activities. Apart from being benevolent, the state has been expanding its measures, mechanisms and technologies of surveillance which are operational to purposefully monitor, observe, control, and influence the counter dissenting voices against the state. It characterises a strong central power of the state, whereas individual receives limited political freedoms.

Conceptually privacy and surveillance itself is not a self-defining phenomenon, rather, it dwells around the deeply muddy terrain of an array of interrelated social and policy issues. And historically, they were moulded to suit varying interests and agendas. Here the prescribed policy of digitalisation contains state's primordial interest and agenda of adopting a model of privatization and neoliberal economy. For this the state is accruing private investments (PIB 2017a) and they even roped in New York-based consultancy firm McKinsey & Company to lay the roadmap to reap more investments (PIB 2017b). Secondly, it also involves the expansion of state's surveillance through the benign and despotic push towards digitalisation.

Conclusion

The despotic push towards digitalisation brought out drastic changes in the policy framework of governance as it circumscribed privacy and made surveillance ubiquitous in India. Despite India being one of the largest democratic states, it could not do away with the authoritarian surveillance practices which have proliferated over the last two decades. Though surveillance is not a new phenomenon in India, because it has the chequered history of telephone tapping and political snooping. However, the surveillance regime in the present scenario is instilled with a novel push towards massive digitalisation. Here digitalisation cannot be circumscribed as merely a technological development, rather it also includes ethical and political dimensions—the janus-faced nature of governance, along with interlinking of policies—it basically contains the state's primordial interests and agenda to establish an authoritarian surveillance regime.

Here the recurrent changes in governance policies through demonetisation and despotic push towards digitalisation unleashed a trail of uncertainties and insecurities. Under this digitalisation mission, everyone

²⁰ Dungdung was supposed to give a presentation at a workshop on "Environmental History and Politics of South Asia," to be held on May 10, 2016 at the Centre for World Environmental History, University of Sussex. Dungdung, Gladson. "Ask no questions." *Indian Express*, May 16, 2016. Accessed April 29, 2017. <http://indianexpress.com/article/opinion/columns/jharkand-advansi-forest-rights-act-human-rights-environment-activist-2802460/>.

²¹ *The Hindu*. "Greenpeace campaigner Priya Pillai offloaded at airport." January 11, 2015. Accessed April 29, 2017. <http://www.thehindu.com/news/national/greenpeace-campaigner-priya-pillai-offloaded-at-airport/article6777773.ece>.

²² Mehta, Christine. "How I was deported from India." *The Hindu*, July 2, 2015. Accessed April 29, 2017. <http://www.thehindu.com/opinion/op-ed/christine-mehta-writes-on-how-she-was-deported-from-india-for-her-report-on-afspa/article7375878.ece>.

became visible and transparent under its ambit. Its manifold effects are quite apparent, especially due to the non-existence of a robust data protection regime. The mobilisation of new technologies by the state to deliver government services, in contrast, is veiled with the dangers of surveillance, privacy violations and abuse of civil liberties. India clearly lacks democratic control over surveillance, which led to the establishment of a centralised surveillance apparatus, without establishing robust principles of reasonable regulation along with firm publicness for action. Here the idea of limited government and constitutionalism seems to be under siege, and the Orwellian Indian state is deeply penetrating and carving out new surveilling space as it taps out the prospects of emerging new technologies.

Acknowledgements

I would like to thank my supervisor, Professor Vasanthi Srinivasan, for thought provoking discussion on issues surrounding privacy and surveillance. I would also like to thank the Editor and the anonymous reviewers for their serious and critical feedback on the article.

References

- Aadhaar Act. 2016. *Unique Identification Authority of India*. Accessed April 28, 2017. https://uidai.gov.in/images/the_aadhaar_act_2016.pdf.
- Abraham, Sunil, and Elonnai Hickok. 2012. "Government access to private-sector data in India." *International Data Privacy Law* 2(4): 302-315. Accessed April 28, 2017. <https://doi.org/10.1093/idpl/ips028>.
- ADES. 2015. "Proposed Addendum to The Draft Encryption Policy 2015." Accessed April 30, 2017. http://naavi.org/uploads/wp/clarification_nep_v1.pdf.
- Budget Speech. 2014. Arun Jaitley, Minister of Finance July 10, 2014 Accessed April 28, 2017. <http://indiabudget.nic.in/budget2014-2015/ub2014-15/bs/bs.pdf>.
- Budget Speech. 2017. Arun Jaitley Minister of Finance, February 1, 2017 Accessed April 28, 2017. <http://indiabudget.nic.in/ub2017-18/bs/bs.pdf>.
- CIS 2017. "Information Security Practices of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar Numbers with sensitive personal financial information." *The Centre for Internet & Society*. Accessed June 13, 2017. <http://cis-india.org/internet-governance/clarification-on-information-security-practices-of-the-aadhaar-report/view>.
- DNES. 2015. "Draft National Encryption Policy 2015." Accessed April 30, 2017. <https://netzpolitik.org/wp-upload/draft-Encryption-Policyv1.pdf>.
- ES. 2017. "Economic Survey 2016-17". *Government of India, Ministry of Finance, Department of Economic Affairs*, Accessed April 28, 2017. <http://indiabudget.nic.in/es2016-17/echapter.pdf>.
- Greenleaf, Graham. 2014a. "India's Data Protection Impasse: Conflict at All Levels, Privacy Absent." *Privacy Laws & Business International Report* 127 no. 23-24. Accessed April 30, 2017. <https://ssrn.com/abstract=2438366>.
- Greenleaf, Graham. 2014b. "India's Draft the Right to Privacy Bill 2014 – Will Modi's BJP Enact it?" *Privacy Laws & Business International Report* 129 no. 21-24. Accessed April 30, 2017. <https://ssrn.com/abstract=2481796>.
- Krishna, Gopal. 2017a. "Defying Fundamental Rights with Impunity." *Economic and Political Weekly* 52 No. 12 (March 2017). Accessed April 29, 2017.
- Krishna, Gopal. 2017b. Did the Supreme Court Support The Mandatory Use Of Aadhaar In Non-Welfare Schemes? *Live Law* March 28, 2017. <http://www.livelaw.in/supreme-courts-support-mandatory-use-aadhaar-non-welfare-schemes-inappropriate/>.
- MeitY. 2017. "Draft IT (Security of Prepaid Payment Instruments) Rules." *Ministry of Electronics and Information Technology, Government of India*. Accessed March 30, 2017. <http://meity.gov.in/writereaddata/files/draft-rules-security%20of%20PPI-for%20public%20comments.pdf>.
- MoF. 2016. Notification, *Ministry of Finance, Department of Economic Affairs*. November 8, 2016. Accessed April 28, 2017. <http://finmin.nic.in/172521.pdf>.
- PIB. 2014. "Digital India—A programme to transform India into digital empowered society and knowledge economy." *Press Information Bureau*. August 20, 2014. Accessed April 28, 2017. <http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926>.
- PIB. 2016. "NITI Aayog Announces Launch of the Schemes—Lucky Grahak Yojana and Digi-Dhan Vyapar Yojana - for Incentivising Digital Payment." *Press Information Bureau*. Accessed April 30, 2017. <http://pib.nic.in/newsite/PrintRelease.aspx?relid=155418>.
- PIB. 2017a. "A Digital Friendly Budget aimed at accelerating India's Transformation into a Digitally Empowered Society": Ravi Shankar Prasad" *Press Information Bureau*. Accessed June 13, 2017. <http://pib.nic.in/newsite/PrintRelease.aspx?relid=158376>.
- PIB. 2017b. "Modi's 3 years: Government receives Rs 1.43 lakh crore of investment in electronics sector." *Press Information Bureau*. Accessed June 13, 2017. <http://pib.nic.in/ndagov/3YearsOfNDAGovernment/nda25.pdf>

- PSC. 2010. "Parliamentary Standing Committee on Finance, National Identification Authority of India (NIAI) Bill." Accessed June 13, 2017. <http://www.prsindia.org/uploads/media/UID/uid%20report.pdf>.
- Rajya Sabha Debates. 2016. "Right to Privacy Bill." responded by Dr. Jitendra Singh. Minister of State, 5 May, 2016. Accessed April 28, 2017. http://rsdebate.nic.in/bitstream/123456789/659936/2/PQ_239_05052016_U1380_p248_p248.pdf#search=PRIVACY.
- RBI. 2016a. "Master Circular—Policy Guidelines on Issuance and Operation of Pre-paid Payment Instruments in India." *Reserve Bank of India*. Accessed April 28, 2017. <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=10510&Mode=0>.
- RBI. 2016b. "Notification, Withdrawal of Legal Tender Character of existing 500/- and 1000/- Bank Notes." *Reserve Bank of India*. Accessed April 28, 2017. <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI11270CF2F17E86E4C5F92FEDFFDF8820934.PDF>.
- SFLC. 2014. "India's Surveillance State: Report on Communications Surveillance in India." *Software Freedom Law Centre*. Accessed April 28, 2017. <http://sflc.in/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf>.
- SFLC. 2017. "No Aadhaar, no service- Notifications making Aadhaar mandatory." *Software Freedom Law Centre*. Accessed April 28, 2017. <http://sflc.in/no-aadhaar-no-service-notifications-making-aadhaar-mandatory/>.
- Singh, Ujjwal Kumar. 2007. *The State, Democracy and Anti-Terror Laws in India*. New Delhi: SAGE.
- Singh, Ujjwal Kumar. 2014. "Surveillance Regimes in Contemporary India," In: *Surveillance, Counter-Terrorism and Comparative Constitutionalism*, edited by Fergal Davis, Nicola McGarrity, and George Williams. London: Routledge.
- Xynou, Maria and Elonnai Hickok. 2015. "Security, Surveillance and Data Sharing Schemes and Bodies in India." *The Centre for Internet & Society*. Accessed June 13, 2017. <https://cis-india.org/internet-governance/blog/security-surveillance-and-data-sharing.pdf>.