Australia India Institute Vol.10, October 2018

A VERY SHORT POLICY BRIEF

Making Digital Rights Count in India

Pawan Singh

The Australia India Institute's A VERY SHORT POLICY BRIEF series examines key questions facing contemporary India and the Australia-India relationship. It combines in-depth academic analysis with clarity and policy relevance.

Australia India Institute

THE UNIVERSITY OF MELBOURNE

LA TROBE UNIVERSITY

UNSW AUSTRALIA

www.aii.unimelb.edu.au

The Australia India Institute, based at The University of Melbourne is funded by the Australian Government, Department of Education and Training, the State Government of Victoria and the University of Melbourne.

Summary

In India, a group of experts comprising the Justice B.N. Srikrishna Committee, have created digital rights – pertaining to personal data privacy, protection, processing, access and sharing via digital systems – in its draft bill, the Personal Data Protection Bill, 2018. Personal data privacy concerns arose predominantly in the context of Aadhaar – the Indian government's biometric identity programme – and also around social media technologies like Facebook and WhatsApp. The 2018 draft bill on data protection law identified four digital rights: The Right to Confirmation and Access, Right to Correction, Right to Data Portability and the Right to be Forgotten.

This Very Short Policy Brief identifies key issues in data protection pertaining to digital identity systems in welfare, society and governance, and offers four recommendations to ensure the meaningful exercise of digital rights. These are:

1. Create awareness of the digital rights among marginalized groups (e.g. class, gender, occupation, literacy) with inadequate access to information resources.
2. Develop procedures in regional languages for these rights to be exercised effectively by those with inadequate understanding of digital systems.
3. Include a right to ethical recognition of a welfare beneficiary's claim to entitlements to strengthen the right to be forgotten.
4. Develop a framework of privacy harms for a better understanding of outcomes resulting from the compromise of personal data security.

India's Data Protection Regulation Landscape

In India, regulations governing information technology systems began in 2000 with the growth of e-commerce, business process management industry and national security concerns, and continued to evolve over the next decade. The Indian government passed the first legislation, called the Information Technology Act, 2000 (The IT Act), following the Resolution adopted by the General Assembly of United Nations (UN) regarding the Model Law on Electronic Commerce. During the early 2000s, the government felt the need to regulate the growing e-commerce industry in India. The IT Act governed matters of cybercrime and e-commerce and penalized 1. cyber contraventions (unauthorized access to or downloading data from computer systems) under Section 43 (a)-(h) through civil prosecution and, 2. cyber offences (tampering with computer source code, hacking with intent to cause damage and breach of confidentiality and privacy) under Sections 63-74 through criminal proceedings.[1]

National security concerns around the use of the Internet for terrorist activities and child pornography in India led the Indian Parliament to amend the IT Act in 2008 to introduce Section 66 A. The section penalized sending offensive messages and other provisions related to terrorism, child porn and online voyeurism defined broadly as an illicit viewing/ distribution of someone's private conduct through webcams or digital images.[2]

The IT Amendment Act, 2008 further evolved to respond to the changing regulatory environment globally – particularly the European data protection laws – leading to a major amendment in 2011. Of particular concern was India's thriving business process outsourcing (BPO) industry that dealt with sensitive personal data of individuals. The government passed the amendment to ensure that the BPO sector did not suffer due to a lack of Indian legislation for personal data protection.[3] This amendment laid down explicit rules and provisions applicable to body corporates and persons in India regarding the acquisition, storage and security of sensitive personal data.[4]

Under the amendment, the rules for regulating the handling of sensitive personal data by these entities explicitly addressed privacy and consent. For instance:

Rule 3 listed items that are to be treated as sensitive personal data – passwords, credit/ debit card information, biometrics such as DNA, fingerprints and voice patterns used for authentication of identity. The rule excluded the freely available personal information about the individual in the public domain under this category.

Rule 4 mandated that any body corporate that collects sensitive personal data should publish their privacy policy on their website, along with the type of information, reason for collection and security protocols to maintain the confidentiality of the information.

Rule 5 specified that the body corporate should provide a disclosure statement that obtains consent from individuals for collecting their personal information, spells out the reasons for information collection and its use for lawful purposes, and the duration for retaining the person's information. Individuals had the option to review or refuse the information being asked for, and have access to a grievance officer through the website.[5]

The subsequent amendments in 2008 and 2011 to the IT Act, 2000 have shifted the emphasis of original regulation from ensuring the growth of e-commerce and international trade to the introduction of stringent rules for protection of sensitive personal data. The 2011 amendment granted certain exceptions to the use of such data by the Indian

1. See, International Comparative Legal Guides on Data Protection, India. https://iclg.com/practice-areas/data-protection-laws-and-regulations/india Accessed August 18, 2018.
2. Dhwani Pandya. IT Amendment Act 2008 and its Effect on the Indian Enterprise. Computer Weekly. https://www.computerweekly.com/news/1372824/IT-Amendment-Act-2008-and-its-effect-on-the-Indian-enterprise Accessed October 2, 2008.
3. Drafted in 2009 under Section 43A of the IT Act. See Aditi Chaturvedi. GDPR and India. Edited by Amber Sinha, Centre for Internet and Society. https://cis-india.org/internet-governance/files/gdpr-and-india Accessed August 19, 2018.
4. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
5. S.S. Rana & Advocates. 2017. India: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Or Information) Rules, 2011. Mondaq. http://www.mondaq.com/india/x/626190/data+protection/

government under Section 69 leading to concerns around surveillance of citizens.[6] However, it was the introduction of the Indian biometric identity project, Aadhaar, in 2009, that generated an intense national debate among civil society actors, experts and the government regarding the project's potential to create a surveillance state in the absence of stringent laws governing personal data protection.

Aadhaar and Data Protection Regulations

Aadhaar is the Indian government's largest digital project to date, carried out by a specially established organisation called the Unique Identification Authority of India (UIDAI). It enrols individuals by collecting their demographic and biometric information including fingerprints and iris scans, and issues them a Unique ID. The United Progressive Alliance (UPA) government launched Aadhaar in 2009 as an optional scheme to deliver welfare benefits to the poor, especially those who lacked access to proper identity infrastructures and, as a result, could not access government benefits.[7]

Since 2012, various legal petitions challenged Aadhaar for its potential to create a surveillance state as well as for the mandatory linkage of the central biometric database to databases of subsidies and services like banking and mobile communications. The potential violation of citizen privacy through the interlinking of Aadhaar with other databases became the rallying cry of the movement against Aadhaar, led by civil society actors, lawyers and privacy activists. These actors raised concerns about the accuracy of biometric technology given that many legitimate beneficiaries whose biometric authentication failed, were excluded from their benefits, leading in several instances, to their death due to starvation. In case the ration card of a beneficiary remained unlinked to Aadhaar for reasons beyond their control, it led to exclusion as well.[8]

As these petitions were being heard, the National Democratic Alliance (NDA) government passed Aadhaar as a Money Bill (Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016). A money bill contains provisions for taxes, appropriation of funds and other financial matters. This led to other legal petitions opposing the passage of Aadhaar as a money bill in the Indian Supreme Court (SC).

The national debate on data privacy took shape around Aadhaar's perceived potential for mass surveillance and denial of benefits to legitimate beneficiaries due to technological failures of identity authentication and ration cards not linked to Aadhaar. The SC debated Aadhaar's validity as a matter of balance between the marginalized sections' socioeconomic rights including the right to government welfare through a legitimate digital identity and a reasonable restriction on their individual privacy. The exclusion of the welfare-dependent beneficiaries from benefits due to system failures in Aadhaar's biometric authentication or linking of ration cards (which allows beneficiaries to access government-subsidized food and cooking gas) violates the Article 14 (equality) and Article 21 (life and liberty) of the Indian Constitution. Moreover, the mandatory Aadhaar linkage to various service databases potentially violates individual privacy given that such a linkage can lead to social profiling of individuals.[9]

6. The section enables the Indian Government to intercept, monitor or decrypt information if it is satisfied that it is necessary in the interest of national security and sovereignty, defence, security, public order, friendly relations with foreign states and prevention and investigation of crimes. See, Vijay Pal Dalmia. 2017. Data Protection Laws in India. Mondaq. http://www.mondaq.com/india/x/655034/data+protection/Data+Protection+Laws+in+India Accessed August 19, 2018.

7. R.S. Sharma. 2010. "Identity and the UIDAI: A Response." Economic and Political Weekly. 45 (35).

8. Aadhaar's Graveyard – Aadhaar Deaths. https://aadhaar.fail/category/aadhaar-exclusions/aadhaar-deaths/ Accessed October 2, 2018.

9. Madhav Khosla and Anand Padhmanabhan. 2018. The Aadhaar Challenge: 3 Features that Put Constitutional Rights at Risk. The Print. https://theprint.in/opinion/the-aadhaar-challenge-3-features-that-put-constitutional-rights-at-risk/75576/ Accessed August 20, 2018.

Aadhaar's Constitutional Validity and Digital Rights

The Aadhaar privacy debate gave way to important legislations and a regulatory framework to govern data privacy in India. In 2017, the Indian Supreme Court declared privacy to be a fundamental right subject to certain limitations.[10] Subsequently, the government appointed a ten-member expert committee headed by the retired Supreme Court Justice B.N. Srikrishna to identify personal data protection issues and draft a data protection law for India.[11] The report was submitted to the Supreme Court in November 2017, followed by the draft bill in July 2018.[12] In September 2018, the SC ruled that Aadhaar was constitutionally valid for government welfare schemes as well as for filing taxes, but not mandatory for banking or mobile phone communications.[13] The ruling implies that the marginalized sections of society must share their biometric information under Aadhaar to avail of benefits because their access to welfare is defined as a matter of their empowerment, and broadly, a public good.

The Srikrishna Report follows the spirit of the 2017 privacy judgment to reinforce individual autonomy and self-determination with respect to information. It recognizes a right to informational privacy that makes an individual the owner of their data and have the freedom to share that data or retain it as part of this right. However, the report recognizes the limitations on such rights to advance national interest and collective values. These pertain to a free and fair digital economy that runs on personal data. The report constructs the individual control over their personal data and the growth of a digital economy as mutually compatible.

The report defines individuals who share their data with entities as data principals, who are fundamentally in a relationship of trust with those entities. In turn, the entities that collect individual data, are defined by a duty to protect and process such data with care in line with individual expectations. They are data fiduciaries who must use and share the data in a manner that fulfils the expectations of the data principal while furthering the common public good of a free and fair digital economy.[14]

The findings from the Srikrishna Report translated into a set of rights covered by the draft Personal Data Protection Bill, 2018. These include:

> *Right to confirmation and access* that enables the data principal to seek confirmation of what data has been processed by the data fiduciary and the processing activities undertaken;
>
> *Right to correction* that enables the data principal to correct, update and complete any data that needs to be modified;
>
> *Right to data portability* that enables the data principal to obtain and transfer their data to other entities and the,
>
> *Right to be forgotten*, which enables the data principal to stop further disclosure of their information by the data fiduciary but not the ability to have their digital data erased, or object to its processing, as provided by the European regulations under the General Data Protection Rules (GDPR).

Together, the SC ruling on Aadhaar's constitutionality for welfare and the Srikrishna Committee Report lay down the scope of digital rights in India. While digital rights of information pertain to everyone, their implications for the poor are significant. Due to inadequate access to informational resources and lack of control over their personal data,

10. K. S. Puttaswamy v. Union of India, Writ Petition (Civil) No. 494 of 2012 (Sup. Ct. India Aug. 24, 2017).
11. See http://www.prsindia.org/parliamenttrack/report-summaries/white-paper-on-data-protection-framework-for-india-4986/ Accessed Aug 5, 2018.
12. A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. Committee of Experts Under the Chairmanship of Justice B.N. Krishna. http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf Accessed August 24, 2018.
13. Murali Krishnan. 2018. Supreme Court Upholds Aadhaar, Strikes Down Some Provisions. Bar & Bench. https://barandbench.com/aadhaar-verdict-supreme-court-upholds/ Accessed October 2, 2018.
14. Ibid.

the marginalized sections of Indian society face greater data-related vulnerabilities. They bear the burden of proving their identity in transactions with the government which holds their demographic and biometric information. Failures of Aadhaar authentication could result in civil exclusion or actual death, particularly if they are unable to access food entitlements.[15]

Making Digital Rights Count

The Srikrishna Report has undertaken some important steps for data protection to empower citizens. However, for these rights to be effectively exercised, data protection policies need to address information asymmetries – access to, and understanding of information – among the government, expert stakeholders like lawyers, activists and policymakers and individual users within their social, cultural and economic contexts.

The rights proposed in the draft Personal Data Protection Bill are an important step in setting up a regulatory framework for user-centric data protection. However, they need to be further refined in the context of the 2018 SC judgment that predominantly creates vulnerabilities of personal data for the poor who constantly bear the burden of proving their identity in their transactions with the state. For instance, the draft Bill proposes that the exercise of digital privacy rights requires a written request to the data fiduciary (except for the right to be forgotten) along with proof of data principal's identity. It also suggests that a fee may be charged to exercise some of these rights.

Such conditions for the exercise of the digital rights assume an ideal data principal with informational and economic resources at their disposal. They do not account for varying levels of social vulnerability, digital literacy and informational resources accessible to the data principal for redress under the proposed data protection regime.

A regulatory framework that addresses the data protection needs of Indian citizens is a necessary and important step in ensuring the safety and proper use of personal data and the functioning of a robust digital economy. However, the formulation of rights is only the first step in the implementation of a system of checks and balances. As the draft bill continues to be debated, privacy-oriented digital rights need to be understood in the material contexts of their application.

The following recommendations contribute to the ongoing debate and development of the regulatory framework for data protection in India.

Recommendation 1. Create awareness of the digital rights among marginalized groups with inadequate access to information resources (e.g. class, gender, occupation, literacy)

For the effective exercise of digital rights in India, it is important to undertake initiatives to bridge the digital divide that encompasses digital literacy and informational asymmetry among other issues. In India, 40% of the population lives below the poverty line, the illiteracy rate is 25-30%. Digital literacy is almost non-existent for more than 90% of the population.[16] Raising digital literacy is vital for digital rights proposed under the data protection regime to be meaningfully exercised.

15. Praavita. Aadhaar Doesn't Work. Supreme Court's Judgment Cannot Change this Reality by Denying the Facts. Scroll.in https://scroll.in/article/896374/aadhaar-doesnt-work-supreme-courts-judgement-cannot-change-this-reality-by-denying-the-facts Accessed September 30, 2018.

The National Democratic Alliance (NDA) government's 2018 National Digital Literacy Mission seeks to impart IT training to 52.5 lakh persons in the informal sector who lack basic knowledge of computer and the Internet.[17] As the data protection bill takes shape with further deliberations, it is imperative that education about data systems and digital rights is incorporated in digital literacy programmes to create awareness among the lower socio-economic strata populations. Such education will have to cater to the contextual specificities of class, gender, occupation, literacy and education keeping in mind the distribution of vulnerabilities across material experience. This may be a long and difficult process but awareness about digital rights has to go hand-in-hand with digital literacy.

Recommendation 2. Develop procedures in regional languages for these rights to be exercised effectively by those with inadequate understanding of digital systems.

In addition to raising digital literacy and access to information technology infrastructures, there is a need to provide multiple options in regional languages for the same procedures to be followed. The ability to correct and update personal data with the data fiduciary effectively will depend on the ease of procedures and access to appropriate informational resources. The procedures should not be burdensome on the data principal and ought to be proportionate to the resources at their disposal for them to follow it efficiently.

An obligatory aspect of ease of procedures is the requirement for access to informational and redressal resources so that the data principal can exercise their right to correction. This may be undertaken through an online service or a paper form and, in cases where the data principal is not familiar with digital systems, with the assistance of a literate assistant who can facilitate the process of initiating a request. Further, it is absolutely vital to offer exemptions to persons who cannot afford the fees that may be charged for exercising their right to correction.[18]

Recommendation 3. Include a right to ethical recognition of a welfare beneficiary's claim to entitlements to strengthen the right to be forgotten.

Data privacy is a context-specific formulation as already noted by scholars,[19] and a right to ethical recognition must be included in the bill to prevent exclusion from benefits. The data protection regulatory framework must acknowledge that digital rights, no matter, how inclusively and comprehensively formulated, will likely not work in certain situations. This dynamic has already been evident in the case of Aadhaar-Based Biometric Authentication (ABBA) which requires beneficiaries to authenticate their claim on food rations using their fingerprints.

Various scenarios can lead to exclusion from benefits. For example, a successful transaction for the delivery of welfare through Aadhaar authentication requires not only internet connectivity and the linkage of ration card to Aadhaar but also the biometric authentication to match the fingerprints captured at the time of enrolment. If either of these fail, it may result in welfare recipient being excluded or denied their legitimate benefits. Such exclusions, in certain cases, have led to deaths of individuals owing to starvation along with an exacerbation of their social and economic vulnerabilities.[20]

16. Digital Empowerment Foundation. https://defindia.org/national-digital-literacy-mission/ Accessed August 24, 2018.

17. National Digital Literacy Mission. http://beta.nielit.gov.in/calicut/content/national-digital-literacy-mission-ndlm Accessed August 24, 2018.

18. Amba Kak, Jochai Ben-Avie, & Naomi Shiffman. 2018. Mozilla Weighs in on India's Draft Data Protection Bill. moz://a. https://blog.mozilla.org/netpolicy/2018/07/27/indian-draft-data-protection-bill/ Accessed August 24, 2018.

19. Helen Nissenbaum. Privacy in Context: Technology, Policy and the Integrity of Social Life. Stanford: Stanford University Press.

The right to be forgotten must, therefore, be re-conceptualized as a separate right to contextually-appropriate or ethical recognition. This is specifically needed for poor people who must bear the greatest burden of identification to access welfare, given that their ability to identify themselves remains contingent upon the accuracy of biometrics.

Recommendation 4. Develop a framework of privacy harms for a better understanding of outcomes resulting from the compromise of personal data security.

One key means through which data protection regulation can be made more effective is through the development of a framework of privacy harms related to data misuse and undue disclosure. This may be accomplished through a risk-cognizant approach to data protection, which classifies data-related risks and vulnerabilities in certain sectors.[21] A comprehensive documentation of case studies of data breaches (undue disclosures) in various public databases linked to Aadhaar[22] and a rigorous theorization of privacy harms, not just related to data breaches but other kinds of information mishaps, will be critical to a meaningful framing and implementation of the data protection bill in India.

The data protection regulatory frameworks in both countries are new and will continue to evolve over the next few decades or so. In Australia, the Privacy Amendment (Notifiable Data Breaches) Bill 2016 was passed in 2017 and came into force in February 2018. The new law lays down the procedures and penalties for data breaches including requirements to notify various stakeholders. The Srikrishna Report and the Draft Personal Data Protection Bill 2018 provide the basis for imminent regulation in India.

India and Australia

The Australia-India relationship is of strategic importance[23] and provides significant opportunities for collaboration on the issue of digital protection and privacy. Both countries hold an important geopolitical position within the Asia-Pacific. Given the need in India to understand data privacy, digital rights and digital literacy from a materially grounded perspective, Australian academics can extend support to Indian policymakers, activists and scholars in undertaking a study of data privacy issues across different social, cultural, economic and regional contexts.

A study called, 'Digital Rights in Australia', conducted by the University of Sydney offered significant findings about data privacy concerns of Australian citizens in the context of their use of digital platforms, digital rights and responsibilities in Asia and Australia and identification of governance models for the platforms.[24] This is an important and timely study that needs to be replicated in the Indian context as well.

Collaborations between Indian and Australian scholars, policymakers, activists and institutions hold enormous potential to offer concrete research findings for robust models of digital rights that are relevant beyond the two contexts to the rest of the Asia-Pacific.

20. Anmol Somanchi, Srujana Bej & Mritunjay Pandey. 2017. Well Done ABBA? Aadhaar and the Public Distribution System in Hyderabad. Economic & Political Weekly. 52 (7).

21. Beni Chugh, Malavika Raghavan, Nishanth Kumar & Sansiddha Pani. 2018. Effective Enforcement of a Data Protection Regime: A Model for Risk-Based Supervision Using Responsive Regulatory Tools. Dvara Research.

22. Varun Aggarwal. 2017. Aadhaar Data Leak Exposes Cyber Security Flaws. The Hindu Business Line. https://www.thehindubusinessline.com/info-tech/

23. Peter N. Varghese, 'An India Economic Strategy to 2035: Navigating from Potential to Delivery', 2018.

24. Gerard Goggin, Ariadne Vromen, Kimberlee Weatherall, Fiona Martin, Adele Webb, Lucy Sunman and Francesco Bailo. 2017. Digital Rights in Australia. The University of Sydney. https://ses.library.usyd.edu.au//bitstream/2123/17587/7/USYDDigitalRightsAustraliareport.pdf Accessed Aug 25, 2018

References

Aadhaar's Graveyard – Aadhaar Deaths. https://aadhaar.fail/category/aadhaar-exclusions/aadhaar-deaths/ Accessed October 2, 2018.

Aggarwal, V. 2017. Aadhaar Data Leak Exposes Cyber Security Flaws. The Hindu Business Line. https://www.thehindubusinessline.com/info-tech/aadhaar-data-leak-exposes-cyber-security-flaws/article9677360.ece Accessed Aug 24, 2018.

Chaturvedi, A. GDPR and India. Edited by Amber Sinha, Centre for Internet and Society. https://cis-india.org/internet-governance/files/gdpr-and-india Accessed Aug 19, 2018.

Chugh, B. Raghavan, M. Kumar, N & Pani,S. 2018. Effective Enforcement of a Data Protection Regime: A Model for Risk-Based Supervision Using Responsive Regulatory Tools. Dvara Research.

Dalmia, V. 2017. Data Protection Laws in India. Mondaq. http://www.mondaq.com/india/x/655034/data+protection/Data+Protection+Laws+in+India Accessed 19 Aug, 2018.

Goggin, G., Vromen, A., Weatherall, K., Martin, F. Webb, A., Sunman, L. and Bailo, F. 2017. Digital Rights in Australia. The University of Sydney. https://ses.library.usyd.edu.au//bitstream/2123/17587/7/USYDDigitalRightsAustraliareport.pdf Accessed Aug 25, 2018.

Kak, A., Ben-Avie, A. & Shiffman, N. 2018. Mozilla Weighs in on India's Draft Data Protection Bill. moz://a. https://blog.mozilla.org/netpolicy/2018/07/27/indian-draft-data-protection-bill/ Accessed Aug 24, 2018.

Khosla, M. and Padhmanabhan, A. 2018. The Aadhaar Challenge: 3 Features that Put Constitutional Rights at Risk. The Print. https://theprint.in/opinion/the-aadhaar-challenge-3-features-that-put-constitutional-rights-at-risk/75576/ Accessed Aug 20, 2018.

Kini, A. 2018. [Aadhaar] Read the Summary of Majority (4:1) Judgment. LiveLaw. https://www.livelaw.in/aadhaar-read-the-summary-of-majority-41-judgment/ Accessed Sept. 30, 2018.

Krishnan, M. 2018. Supreme Court Upholds Aadhaar, Strikes Down Some Provisions. Bar & Bench. https://barandbench.com/aadhaar-verdict-supreme-court-upholds/ Accessed October 2, 2018.

Mandhani, A. 2018. Govt. Releases Justice Srikrishna Committee Report and Draft Personal Data Protection Bil, 2018. Live Law. https://www.livelaw.in/justice-srikrishna-committee-releases-report-and-personal-data-protection-bill-2018/ Accessed October 2, 2018.

Nissenbaum, H. 2009. Privacy in Context: Technology, Policy and the Integrity of Social Life. Stanford: Stanford University Press.

Pandya, D. 2009. IT Amendment Act 2008 and its Effect on the Indian Enterprise. Computer Weekly. https://www.computerweekly.com/news/1372824/IT-Amendment-Act-2008-and-its-effect-on-the-Indian-enterprise Accessed October 2, 2018.

Praavita. Aadhaar Doesn't Work. Supreme Court's Judgment Cannot Change this Reality by Denying the Facts. Scroll.in https://scroll.in/article/896374/aadhaar-doesnt-work-supreme-courts-judgement-cannot-change-this-reality-by-denying-the-facts Accessed September 30, 2018.

Sharma, R.S. 2010. "Identity and the UIDAI: A Response." Economic and Political Weekly. 45 (35).

Somanchi, A., Bej, S. & Pandey, M. 2017. Well Done ABBA? Aadhaar and the Public Distribution System in Hyderabad. Economic & Political Weekly. 52 (7).

S.S. Rana & Advocates. 2017. India: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Or Information) Rules, 2011. Mondaq. http://www.mondaq.com/india/x/626190/data+protection/formation+Technology+Reasonable+Security+Practices+And+Procedures+And+Sensitive+Personal+Data+Or+Information+Rules+2011 Accessed August 18, 2018.

Also from the A Very Short Policy Brief series:

Promoting Off-Grid Solar Energy in India

Promoting Healthy Food Environments in India

Strategies to Expand Hindi Education in Australia

Making 'Climate-Smart' Indian Cities

India's New Goods and Services Tax: Implications and Opportunities

Promoting India's Panchayats as Vanguards of Local Climate Adaptation

Australia's India Choice: Navigating Strategic Competition between India and China

Sustainable Skill Development in India

Engaging with India's Higher Education Sector: Pathways to Improved Market Access

Australia India Institute
147 - 149 Barry Street
Carlton, Victoria 3053 Australia

Australia India Institute @ Delhi
B3/70, Safdarjung Enclave
New Delhi,110029 India

Australia India Institute

aii.unimelb.edu.au australiaindiainstitute @aiiinstitute