Policy Discussion

By SUBHASHIS BANERJEE

4 Feb 2024

Digitalisation, AI and Society

The scale and scope of digitalisation in public life in India are unmatched in the world, especially in large public service applications. The use of digitalisation technologies are not only restricted to the government but are growing rapidly in the private sector as well. While the potential of such digitalisation and AI applications for public good is unquestionable, they do raise some serious social, ethical and legal questions [72, 21, 24, 9] whose mitigation and compliance with regulation pose new challenges for computer science.

In fact, such systems have been difficult to operationalise anywhere in the world. Many attempts at building large public services like national digital identity systems [61], health registries [58, 12, 54, 25], national population and voter registries [71, 50, 64], public credit registries [19, 14], income [67] and tax registries [26] etc. have often been questioned on fairness, privacy and other ethical grounds. The concerns have invariably been related to the need for protective safeguards when large data integration projects are contemplated, and acknowledgment of the bias, exclusion, discrimination, privacy and security problems that these may create. In some situations they have even had to be abandoned altogether as they were unable to deal with these risks [58, 12, 23, 30, 18]. In fact, there are very few examples of successful systems free of controversies. In India too, the use of our national digital identity programme was restricted only to welfare disbursal by the majority judgement on Aadhaar; whereas the minority judgement found it to be unconstitutional in its entirety [60]. Very similar considerations in the respective constitutional courts have led to the halting of the biometric-based national identity programme in Jamaica [30] and Kenya [18]. The concerns around digitalisation and privacy [7, 29, 63, 60] not only require new computer science techniques for design, analysis and implementation, but also require dimensions beyond computer science [41]. In fact, though the much awaited data protection act [37] has recently been passed by the parliament, after several years of debate around the earlier

drafts [62, 56], there still remains considerable doubts about its scope and structure [35, 5, 57].

Digital public goods in India

The unprecedented growth of digitalisation in public life in India has been centred around Aadhaar [69] and welfare delivery, the Unified Payment Interface (UPI) [70], the ongoing efforts towards the Ayushman Bharat Digital Mission (ABDM) for health [42], the Reserve Bank of India's Account Aggregator System [51], and, of course, electronic elections.

India's biometric-based digital identity system, Aadhaar [69], has an enrolment of over 1.3 billion, and is used for a variety of applications, including – but not limited to – welfare disbursal and direct benefit transfers, public distribution systems for ration, deduplication of income tax registries, voters' lists and driving licenses, property registrations, Covid vaccination records and accessing healthcare. It is also used for 'Know Your Customer' (KYC) services for a large number of domains. Several of these applications are backed by law, but several others are not.

The Unified Payment Interface (UPI) [70] system in India is one of the largest transaction systems in the world. Just in January 2024, there were over 12 billion UPI transactions of over ₹ 1.8 million Crores in total value. It has undeniably empowered a vast section of the working population and has enhanced their ease of doing business. Its adoption and penetration even in rural areas have been remarkable. However, the UPI transactions are not anonymous, they leave digital trails, and they do not support a proof of payment independent of the service providers. Hence the issues of privacy and trust are still moot.

The ABDM [42] is not yet fully rolled out, but universal health ids have already been generated for almost all residents of India during digitalisation of Covid vaccination records. The universal health ids have also been linked to Aadhaar. The digitalisation process turned out to be crucial for the supply chain management of Covid vaccines and generation of vaccine certificates. It is envisaged that the ABDM will provide electronic health records (EHR) for every individual in India, sharable and interoperable across hospitals and healthcare providers on the basis of consent. The ABDM certainly has the potential to transform healthcare and clinical research for the better, but there still are open questions related to the exact pathways to public good and risk assessment and mitigation.

The Reserve Bank of India's Account Aggregator framework [51], which went live in September 2021, aims to make financial data more accessible by creating data intermediaries called Account Aggregators (AA) which will collect and share the user's financial information from a range of entities that hold consumer data called Financial Information Providers (FIPs) to a range of entities that are requesting consumer data called Financial Information Users (FIUs) after obtaining the consent of the consumer. This will be one of the largest such systems in the world and the Securities and Exchange Board of India (SEBI) has already joined the programme [52]. The Account Aggregator Framework is based on the Data Empowerment and Protection Architecture (DEPA) of Niti Ayog [46], which however is still at the draft stage.

The digitalisation efforts such as the above undeniably are great examples of software development and project management at scale, though they may in some aspects lack

the sophistication of contemporary computer science. They also have had great impact on society. Data collection and analysis is one of the biggest aims of such digitalisation. In fact, Nandan Nilekani, who pioneered the vision of digitalisation of public services in India [44], famously said that "Indians will be data rich before they're economically rich". However, converting a speculative data-driven theory of public good to a rigorous, safe and effective theory will require considerable research and due diligence, and the pitfalls are many [47, 21, 59, 72, 24, 9]. Required now are comprehensive academic enquiries into these digitalisation and analytics efforts, to learn from the experience, from the points of view of sociology, economics, ethics and computer science.

Design considerations for digital systems

While all digitalisation come with some inherent risks of exclusion, increased transaction costs and loss of privacy, the theory of social good based on digitalisation are often not fully developed [9]. It is undeniable that in addition to facilitating superior record keeping and audit, digitalisation also offers the possibility of using modern data analytics techniques for finding large scale correlations in data that may facilitate improved design of social policy strategies and early detection and warning systems for anomalies. For example, it may be tremendously insightful to be able to correlate education levels, family incomes and nutrition across the entire population; or disease burden with income, education, nutrition and lifestyle, work environment and exposure to environmental stress. More generally, it may enable carrying out econometric analysis, epidemiological studies, automatic discovery of latent topics and causal relationships across multiple domains of the economy [68, 31, 65, 66, 33, 6, 34, 17].

However, realising such potential requires identifying and understanding the diverse data sources and their complexity. This may involve understanding the constraints of personnel, resources and equipment at various data generation and consumption points, understanding their primary functions and ensuring that they are not hampered in any way. It also requires an understanding of the frequency of data generation, error models, access rights, interoperability, sharing, data analysis, dissemination and other usage requirements, and designing the data organisation and application programming interfaces appropriately. Most importantly, it requires the necessary due diligence to ensure that the AI and data analytics techniques are reliable and they indeed deliver what they promise [9]. Developing tools and techniques for validating and evaluating the reproducibility and reliability of AI algorithms is an active area of research that requires multidisciplinary inputs.

The following are the specific areas that require particular attention.

Use case analysis

The most problematic aspect of digitalisation in large public service applications is incomplete modelling and analysis of use cases. Such inadequate analysis may not only result in the digitalisation use cases failing to achieve their intended purposes, but may also result in harms like exclusion, denial of service and increased transactional costs for users [15, 39]. For example, it becomes imperative to analyse whether digital identity and authentication systems are sound, implying that nobody is incorrectly authenticated, and complete, implying there are no authentication failures for true users. Even if

these guarantees are probabilisitic, the probabilities need to be quantified and the consequences of the probabilistic errors – especially for their potential for denial of service and exclusion – completely analysed. The use cases also need to be analysed for fairness, their potential for discrimination and their privacy and security threat models. Developing formal techniques for use case specification, modelling and analysis is an open research problem.

Privacy and security

The biggest concern is large digital applications usually is privacy. Computer science has traditionally conflated privacy with secrecy. Privacy, however, has other connotations as well, including but not limited to loss of informational self-determination, breaking silos by linking of information across multiple domains, function creep, unfair assessment using out-of-context data, public or selective disclosure resulting in unwanted attention or social stigma, defamation, unfair and discriminatory treatment etc. [55, 63, 56]. Most of these harms result from lack of effective purpose limitation, for which security against insider attacks is an important necessary condition [55, 4]. Most large public service applications fail to engender trust due to inadequate articulation of what precise privacy problems are being addressed, and how exactly do the adopted measures address the privacy concerns.

Any digitalisation will necessarily entail some privacy risks. The problem then is to precisely model the risks and develop tools and techniques to mitigate them to the extent possible. This requires rigorous modelling of the limits of anonymisation [40, 53], data security, data hiding – including differential privacy [16] – and encryption. We also require a framework to precisely articulate a privacy threat model and capture the minimum unavoidable privacy risks of an ideal functionality of an application (assuming perfect security), and clearly articulate the trust requirements.

Ethics of AI

Threats to privacy and liberty also arise from big-data analytics or machine learning algorithms, which are important reasons for collecting and recording high frequency, real-time and non-aggregated transactional data in the first place. In recent times, several commentators have pointed out the fairness risks associated with big data analytics. It is forcefully argued by O'Neil [47] that big-data analytics, by the very fact that they are designed by the privileged and often for profit, increases inequality and threatens democracy. O'Neil illustrates with a series of examples that they reinforce inequality and reward the rich and punish the poor. The bias is either present in the algorithm or in the data and sometimes even in both. The common traits of such poor fallout of predictive analytics usually are opacity, scale, and damage. They also often exacerbate inequality [21]. Thatcher et al. [59] argue that "As algorithms select, link, and analyse ever larger sets of data, they seek to transform previously private, unquantified moments of everyday life into sources of profit." Similar concerns have also been raised by Zuboff [72].

There are also theoretical results that suggest that fairness and non-discrimination with big data analytics may be impossible to achieve unless the data is actually well-behaved and lies in a narrow manifold [13, 32, 8]. Poor AI ethics is also often reflected in shoddy and careless design of unreliable data analytics [9].

Developing techniques to model and mitigate

risks of discrimination in AI algorithms, eliminate biases, ensure fairness, or even test them effectively are open research questions. The social realities and the inequities in India add new dimensions to the problem.

Digitalising elections

Electronic voting

End-to-end verifiable (E2E-V) cryptographic voting systems [10] have been around for some time. However, their adoption in large public elections is poor, seemingly because of the inaccessibility of their underlying complex cryptography to the general electorate. Moreover, the ruling of the German Constitutional Court [43] – which ruled that elections should be publicly verifiable without any special knowledge – makes relying on pure electronic elections untenable. Meanwhile, risk-limiting audits based on voter-verified paper records (VVPR) or Voter Verified Paper Audit Trails (VVPAT) [10] may be effective in bringing easy-tounderstand verifiability and recoverability to electronic voting if carried out properly, but they generally require the electorate to trust the post-election custody chain of the paper trail.

Despite decades of research it is still an open problem to design an electronic voting protocol that combines cryptographic security with VVPRs in a principled way, and provides sound and efficient methods of recovering from errors without re-running the entire election in case an election fails verification. The secret ballot requirement makes the problem harder.

A variety of proposals on internet and blockchain based voting add yet another dimension to electronic voting which requires careful and rigorous analysis.

Also, eligibility verification and ensuring that only and all eligible voters can vote, is still an open problem in voting, and it is particularly hard in a country like India.

Securing the electoral rolls and other public registries

With the rapid digitalisation of electoral rolls all around the world, it is now well understood that securing the electoral rolls is the most crucial aspect of securing elections [27, 48, 28].

On the one hand, conventional wisdom – and also election laws in most countries – require the electoral rolls to be publicly displayed, and all additions, deletion and other updates to be made available for public scrutiny. Traditionally, such public verifiability has been considered essential for the integrity of the electoral rolls (for example, see the Registration of Elector Rules [38] under the Representation of the People Act [2]). On the other hand, free access to digitised electoral rolls make profiling of individuals and groups easier, which in turn increases the possibility of targeting or even coercion of voters in closely fought constituencies. In fact, digital profiling of voters and communities are becoming common, and democracies have to soon decide the extent to which it should be allowed.

Protecting individual privacy in electoral rolls and yet making all changes publicly verifiable is as yet an open research problem. Similar considerations also apply to other public registries as well, including citizen registries, registries of social and economic status, tax registries, wealth and property registries, land records, etc.

Tools for digital governance

Recently, there have been a plethora of proposals towards using blockchain and similar other technologies to build trustworthy digital platforms for governance [45, 36], and cryptocurrencies form a special case.

Cryptocurrencies

A crucial property of cash is that transactions are anonymous, which provides a safety net in any democratic society. The basic principle of privacy demands that one should be able to transact without leaving an electronic trail, unless required by law [22]. While cryptocurrencies like bitcoin are supposed to be anonymous by design, and hence even highvalue transactions are difficult to regulate or tax, the extant UPI system in India does leave an electronic trail. It also requires a trust assumption on the providers, as opposed to a blockchain transaction which may provide a proof of the transaction validity. In view of this, there is a demand for a Central Bank Digital Currency (CBDC) in India which may support anonymous transactions [3, 20] and be zero-trust. However, how such an anonymous digital currency tied to a fiat currency may be realised and how cryptocurrencies may be regulated are still very much open questions in computer science, political science and economics.

Governance

While blockchain is a fascinating data structure, it is still unclear what exact roles do consensus and immutability – the two defining properties of blockchain – play to realise the required safety properties in governance, and precisely which aspects of the privacy and security threat models of governance do they address. For example, in most registry applications there usually is only one authority, so consensus is inapplicable. Exact requirement specification of governance related registries, understanding the suitability of blockchains for such registries, and rigorous and formal analysis of the use cases and the threat models of blockchain applications are open research questions.

Social media

Perhaps the most difficult challenges of rapid digitalisation come from the social media systems. On the one hand, they have unleashed hitherto unknown opportunities for ordinary individuals to freely communicate and express themselves without let or hindrance, thereby promoting free speech. On the other hand, the same freedom has led to negative manifestations like creating alternate realities with fake news, illegal profiling and targeting, brainwashing political campaigns, targeted and predatory advertisements, and even shaping public opinion and morality [49]. The problem of fake news has been so overwhelming in India that it has forced the government to demand traceability in end-to-end encrypted communication platforms like WhatsApp [7, 11]. While the court is seized with the traceability issue, the question of how to bring the much needed safety elements into social media and communication systems remain an open problem. It is not even clear whether social media should be regulated or not, and bringing order to social media will require thoughtful and multidisciplinary research.

Conclusion

The digitalisation of society has happened too fast, especially in India where digital literacy is still rather low. This has raised new problems of hitherto unknown dimensions. If we bring digitization to public life, we cannot leave the rigours of computer science behind.

References

1. The Registration of Electoral Rules, 1960, 1960.

2. Act of Parliament. The Representation of the People Act. https://legislative.gov.in/sites/default/files/04representation%20of%20the%20people%20act%2C%201951.pdf, [Online; 1951].

3. Surabhi Agarwal and Romit Guha. Digital rupee should remain anonymous, Nandan Nilekani says. https://economictimes.indiatimes.com/tech/informationtech/digital-rupee-should-remain-anonymous-nandan-nilekani-says/ articleshow/89439300.cms?from=mdr, [Online February 21, 2022].

4. Shweta Agrawal, Subhashis Banerjee, and Subodh Sharma. Privacy and Security of Aadhaar: A Computer Science Perspective. Economic and Political Weekly, Vol. 52(Issue No. 37), 16 2017.

5. Apar Gupta. An Act to cement digital authoritarianism. https://www.thehindu.com/ opinion/lead/an-act-to-cement-digital-authoritarianism/article67202493.ece, [Online; Accessed September 1, 2023].

6. Susan Athey and Guido W. Imbens. Machine learning for estimating heretogeneous casual effects. Technical report, Stanford University, April 2015. https://www.gsb.stanford.edu/faculty-research/working-papers/machinelearning-estimating-heretogeneous-casual-effects.

7. Varsha Bansal. WhatsApp's Fight With India Has Global Implications. https://www. wired.com/story/whatsapp-india-traceability-encryption/, [Online May 27, 2021].

8. Solon Barocas, Moritz Hardt, and Arvind Narayanan. Fairness and Machine Learning. fairmlbook.org, 2019. http://www.fairmlbook.org.

9. T. Bergstrom and J.D. West. Calling Bullshit: The Art of Skepticism in a DataDriven World. Random House Publishing Group, 2020.

10. Matthew Bernhard, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach. Public evidence from secret ballots. In Electronic Voting – Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, October 24-27, 2017, Proceedings, pages 84–109, 2017.

11. Subimal Bhattacharjee. Traceability issue in WhatsApp-Govt spat. https://www.thehindubusinessline.com/opinion/traceability-issue-in-whatsappgovt-spat/article34683085.ece, [Online December 6, 2021].

12. Robert N. Charette. Australians Say No Thanks to Electronic Health Records. https://spectrum.ieee.org/riskfactor/computing/it/australianschoosing-to-optout-of-controversial-my-health-record-system, [Online July 27, 2018].

13. Alexandra Chouldechova. Fair prediction with disparate impact: A study of bias in recidivism prediction instruments. Big Data, 5(2):153–163, 2017. PMID: 28632438.

14. Beni Chugh and Malavika Raghavan. The RBI's proposed Public Credit Registry and its implications for the credit reporting system in India. https://www.dvara. com/blog/2019/06/18/the-rbis-proposed-public-credit-registry-and-itsimplications-for-the-credit-reporting-system-in-india/, [Online; posted 18-June-2019].

15. Jean Dr`eze, Nazar Khalid, Reetika Khera, and Anmol Somanchi. Aadhaar and Food Security in Jharkhand: Pain without Gain? Economic and Political Weekly, Vol. 52(Issue No. 50), 16 2017.

16. Cynthia Dwork. Differential Privacy. In Proceedings of the 33rd International Conference on Automata, Languages and Programming – Volume Part II, ICALP'06, pages 1–12, Berlin, Heidelberg, 2006. Springer-Verlag.

17. Liran Einav and Jonathan D. Levin. The data revolution and economic analysis. Working Paper 19035, National Bureau of Economic Research, May 2013.

18. Rachel England. Kenya halts biometric ID scheme over discrimination fears. https://www.engadget.com/2020-02-03-kenya-halts-biometric-id-schemediscrimination-fears.html, Online, February 3, 2020.

19. org. Equifax Data Breach. https://epic.org/privacy/data-breach/equifax/, 2019. [Online accessed 3-November-2019].

20. ET Now Digital. Central Bank Digital Currency may have an anonymity feature for low-value transactions. https://www.timesnownews.com/business-economy/ personal-finance/central-bank-digital-currency-may-have-an-anonymityfeature-for-low-value-transactions-article-90888256, [Online April 17, 2022].

21. Virginia Eubanks. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press, Inc., USA, 2018.

22. Hugo Godschalk. Right to anonymous payments. https://paytechlaw.com/en/ anonymous-payments-2/, [Online November 8, 2018].

23. UK Press Release. National identity register destroyed as government consigns ID card scheme to history. https://www.gov.uk/government/news/nationalidentity-register-destroyed-as-government-consigns-id-card-scheme-tohistory, 2011. [Online posted 10-February-2011].

24. Yuval Noah Harari. Yuval Noah Harari: the world after coronavirus. https://www. ft.com/ content/19d90308-6858-11ea-a3c9-1fe6fedcca75, [Online; posted 20-March-2020].

25. Jeff Hecht. The future of electronic health records. https://www.nature.com/ articles/ d41586-019-02876-y, [Online September 25, 2019].

26. Kimberly Houser and Debra Sanders. The Use of Big Data Analytics by the IRS: Efficient Solution or the End of Privacy as We Know it? Vanderbilt Journal of Entertainment & Technology Law, 19(4), April 2017.

27. Philip N. Howard and Daniel Kreiss. Political Parties and Voter Privacy: Australia, Canada, the United Kingdom, and United States in Comparative Perspective. First Monday, 15(12), 2010.

28. Christopher Hunter. Political privacy and online politics: How e-campaigning threatens voter privacy. First Monday, 7(2), 2002.

29. Reetika Khera. Dissent on Aadhaar: Big Data Meets Big Brother. Orient BlackSwan, 2019. Edited volume.

30. Ashok Kini. Jamaica SC Follows Justice Chandrachud's Aadhaar Dissent To Declare Its National Identification System (NIDS) Unconstitutional. https://www.livelaw.in/ top-stories/jamaica-sc-declares-nids-unconstitutional-144256, Online, April 13, 2019.

31. Jon Kleinberg, Jens Ludwig, Sendhil Mullainathan, and Ziad Obermeyer. Prediction policy problems. American Economic Review, 105(5):491–95, May 2015.

32. Jon M. Kleinberg, Sendhil Mullainathan, and Manish Raghavan. Inherent trade-offs in the fair determination of risk scores. CoRR, abs/1609.05807, 2016.

33. Rashmi Krishnamurthy and Kevin C. Desouza. Big data analytics: The case of social security administration. Information Policy, 19:165–178, May 2014.

34. Linden McBride and Austin Nichols. Improved poverty targeting through machine learning: An application to the usaid poverty assessment tools. Technical report, Economics That Really Matters, Charles H. Dyson School of Applied Economics and Management at Cornell University, January 2015. http://www.econthatmatters. com/wp-content/uploads/2015/01/improvedtargeting21jan2015.pdf.

35. Mihir R. Digital Personal Data Protection Act, 2023: A missed opportunity for horizontal equality. https://www.scobserver.in/journal/digital-personal-dataprotection-act-2023-a-missed-opportunity-for-horizontal-equality/, [Online; Accessed September 1, 2023].

36. Ministry of Electronics and Information Technology. National strategy on blockchain: towards enabling trusted digital platforms. https://www.meity.gov.in/ writereaddata/files/NationalBCTStrategy.pdf, 2021. [Online; Accessed May 13, 2022].

37. Ministry of Law and Justice, Government of India. The Digital Personal Data Protection Act, 2023. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf, [Online; Accessed September 1, 2023].

38. Ministry of Law, Government of India. The Registration of Electors Rules, 1960. https://legislative.gov.in/sites/default/files/%281%29THE%20REGISTRATION%20OF%20ELECTORS%20RULES%2C%201960.pdf, [Online; November 10, 1960].

39. Karthik Muralidharan, Paul Niehaus, and Sandip Sukhtankar. Identity verification standards in welfare programs: Experimental evidence from india. Working Paper 26744, National Bureau of Economic Research, February 2020.

40. Arvind Narayanan and Vitaly Shmatikov. Robust De-anonymization of Large Sparse Datasets. In Proceedings of the 2008 IEEE Symposium on Security and Privacy, SP '08, pages 111–125, Washington, DC, USA, 2008. IEEE Computer Society.

41. National Academies of Sciences, Engineering, and Medicine. Fostering Responsible Computing Research: Foundations and Practices. The National Academies Press, Washington, DC, 2022.

42. National Health Authority, Ministry of Health and Family Welfare. Ayushman Bharat Digital Mission. https://abdm.gov.in, [Online; Accessed May 13, 2022].

43. The Constitutionality of Electronic Voting in Germany. https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf, 2019. [Accessed June 8, 2019].

44. Nilekani and V. Shah. Rebooting India: Realizing a Billion Aspirations. Penguin Books, 2015.

45. Niti Ayog. Blockchain: The India Strategy. Towards enabling ease of business, ease of living, and ease of governance. https://www.niti.gov.in/sites/default/files/2020-01/BlockchainTheIndiaStrategyPartI.pdf, 2020. [Online; Accessed May 13, 2022].

46. Niti Ayog. Data Empowerment and Protection Architecture: A Secure ConsentBased Data Sharing Framework To Accelerate Financial Inclusion (Draft for discussion). https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf, [Online; Posted August, 2020].

47. Cathy O'Neil. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing Group, New York, NY, USA, 2016.

48. Petervan Onselen and Wayne Errington. Electoral Databases: Big Brother or Democracy Unbound? Australian Journal of Political Science, 39(2):349–366, 2004.

49. Jeff Orlowski, Davis Coombe, and Vickie Curtis. The Social Dilemma. https://www.thesocialdilemma.com, [Online; Accessed May 13, 2022].

50. Monica Pal. Are citizens compromising their privacy when registering to vote? https://gcn.com/articles/2018/12/11/voting-data-privacy.aspx, [Online; posted December 11, 2018].

51. PIB, Ministry of Finance. Know all about Account Aggregator Network- a financial data-sharing system. https://pib.gov.in/PressReleaseIframePage.aspx?PRID= 1753713, [Online; posted 10-September-2021].

52. Sebi joins RBI's account aggregator ecosystem. https://economictimes. indiatimes.com/markets/stocks/news/sebi-joins-account-aggregatorecosystem/articleshow/93663850.cms?from=mdr, 2022. [Online; Posted August 19, 2022].

53. Bruce Schneier. Why 'Anonymous' Data Sometimes Isn't. https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/, 2007. [Online December 12, 2007].

54. Siddarth Shrikanth and Benjamin Parkin. India plan to merge ID with health records raises privacy worries. https://www.ft.com/content/4fbb2334-a864-11e9-984cfac8325aaa04, July 2019. [Online; posted 17-July-2019].

55. Daniel J. Solove. The Digital Person: Technology And Privacy In The Information Age. New York University Press, New York, NY, USA, 2004.

56. N. Srikrishna, Aruna Sundararajan, Ajay Bhushan Pandey, Ajay Kumar, Rajat Moona, Gulshan Rai, Rishikesha Krishnan, Arghya Sengupta, and Rama Vedashree. White Paper of the Committee of Experts on a Data Protection Framework for India, 2017. [Online; Accessed January 9, 2018].

57. Subhashis Banerjee. Data protection Bill: Hiding behind consent. https://indianexpress.com/article/opinion/columns/hiding-behind-consent8834780/, 2023. [Online; Accessed September 1, 2023].

58. James Temperton. NHS care. Data scheme closed after years of controversy. https://www.wired.co.uk/article/care-data-nhs-england-closed, [Online July 6, 2016].

59. Jim Thatcher, David O'Sullivan, and Dillon Mahmoudi. Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data. Environment and Planning D: Society and Space, 34(6):990–1006, 2016.

60. K S Puttaswamy and Another v Union of India (2018): Writ Petition (Civil) No 494 of 2012, Supreme Court judgment dated 26 September. https://www.scobserver.in/cases/puttaswamy-v-union-of-indiaconstitutionality-of-aadhaar-act-case-background/, [Accessed March 29, 2019].

61. The London School of Economics and Political Science. The Identity Project: An assessment of the UK Identity Cards Bill and its implications. http://eprints.lse. ac.uk/726/, June 2005.

62. The Planning Commission: Government of India. Report of the group of experts on privacy chaired by Justice A P Shah. http://planningcommission.nic.in/reports/genrep/rep-privacy.pdf, December 2011.

63. K S Puttaswamy v Union of India (2017): Writ Petition (Civil) No 494 of 2012, Supreme Court judgment dated 24 August. https://www.scobserver.in/courtcase/fundamental-right-to-privacy, [Accessed January 9, 2018].

64. Purnima S. Tripathi. Concerns over linking Aadhaar to voter ID and social media accounts. https://frontline.thehindu.com/the-nation/article29407553.ece, September 2019. [Online; posted 27-Septeber-2019].

65. Big data for development: Challenges and opportunities. http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopmentUNGlobalPulseMay2012.pdf, May 2012.

66. Data for development: Challenges and opportunities. http://www.unglobalpulse. org/, August 2016.

67. Yle Uutiset. Launch of Incomes Register dogged by data security concerns. https://yle.fi/uutiset/osasto/news/launch-of-incomes-register-dogged-by-data-security-concerns/10576057, 2018. [Online posted 30-December-2018].

68. Hal R. Varian. Big data: New tricks for econometrics. Journal of Economic Perspectives, 28(2):3–28, May 2014.

69. Wikipedia. Aadhaar. https://en.wikipedia.org/wiki/Aadhaar, 2022. [Online; Accessed May 13, 2022].

70. Wikipedia. Unified Payments Interface. https://en.wikipedia.org/wiki/Unified-Payments-Interface, 2022. [Online; Accessed May 13, 2022].

71. Kim Zetter. Voter Privacy Is Gone – Get Over It. https://www.wired.com/2008/ 01/voter-privacy-i/, [Online January 31, 2008].

72. Shoshana Zuboff. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. 1st edition, 2018.

© 2023. All Rights Reserved.