

2013

India's Challenge: Preserving Privacy Rights While Implementing an Effective National Identification System

Caroline E. McKenna

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/bjil>

Recommended Citation

Caroline E. McKenna, *India's Challenge: Preserving Privacy Rights While Implementing an Effective National Identification System*, 38 *Brook. J. Int'l L.* (2013).

Available at: <https://brooklynworks.brooklaw.edu/bjil/vol38/iss2/6>

This Note is brought to you for free and open access by the Law Journals at BrooklynWorks. It has been accepted for inclusion in Brooklyn Journal of International Law by an authorized editor of BrooklynWorks.

INDIA'S CHALLENGE: PRESERVING PRIVACY RIGHTS WHILE IMPLEMENTING AN EFFECTIVE NATIONAL IDENTIFICATION SYSTEM

INTRODUCTION

India, with over 1.2 billion inhabitants,¹ is the world's second most populous country² and the world's largest democracy.³ Yet, despite its status as a country with the world's second-fastest growing economy⁴ and a fairly developed system of freedoms and rights,⁵ India has an enormous number of both rural and urban poor.⁶ The Indian government estimates that it has 400 million citizens living in poverty,⁷ a vast number of whom lack governmentally-recognized identities.⁸

The anonymity of these citizens often begins at birth, as many Indians are not issued birth certificates.⁹ The birth reporting system is decentralized, and many births go unrecorded.¹⁰ Although theoretically tallying across the country should

1. CENSUS OF INDIA, *Provisional Population Totals: India Profile* (2011), http://censusindia.gov.in/2011census/censusinfodashboard/stock/profiles/en/IND_India.pdf (last visited Nov. 3, 2012).

2. BBC NEWS: SOUTH ASIA, *India Profile Overview*, <http://www.bbc.co.uk/news/world-south-asia-12557384> (last visited Nov. 3, 2012).

3. *Id.*

4. Lydia Polgreen, *With National Database, India Tries to Reach the Poor*, N.Y. TIMES (Sept. 1, 2011), http://www.nytimes.com/2011/09/02/world/asia/02india.html?pagewanted=all&_r=0; see also BBC NEWS: SOUTH ASIA, *India Profile*, *supra* note 2.

5. Part III of the Indian Constitution guarantees several fundamental rights to Indian citizens. It abolishes "untouchability" and titles, guarantees freedom of speech and religion, provides fair trial provisions which prohibit forcing criminal defendants to testify against themselves, and guarantees protections for minorities. INDIA CONST. arts. 17, 18, 19(1)(a), 20(3), 25, 29, and 30.

6. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4; see also BBC NEWS: SOUTH ASIA, *India Profile Overview*, *supra* note 2.

7. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

8. *See id.*

9. Arun Serrao and Sujatha B.R., *Birth Registration, A Background Note*, CMTY. DEV. FOUND., BANGALORE, (Oct. 23, 2004) at 8–9.

10. *Id.*

be consistent, in reality, birth recording rates vary widely by state, and are as low as 30% in some areas.¹¹ With no national system that records the lives and deaths of Indian citizens,¹² many Indians need to bribe and maneuver their way through bureaucratic morass to obtain basic government documents.¹³ Meanwhile, the rich and middle classes of India have the ability to obtain official identification from the government. Because of this discrepancy, the poor, with their limited means of proving their very existences, often have little access to government aid programs otherwise available to their wealthier counterparts.¹⁴

The rudimentary systems of identification and aid that do exist in India are village-centric.¹⁵ Aid for the poor is administered locally,¹⁶ as individuals are generally known to other locals and so are easily and informally identifiable, particularly in small villages.¹⁷ Villagers are thus likely to be eligible for aid so long as they remain in their small, impoverished towns.¹⁸ If they leave those towns, however, they risk losing access to that aid because they have no documents to identify them as eligible for it elsewhere.¹⁹ Migration within the country is severely curtailed in this way, which in turn has a detrimental effect on the rural poor, and on the economy as a whole.²⁰

These meager identification systems have had other negative impacts on the nation's economy. For example, the lack of identification impairs hundreds of millions of Indians from gaining access to cell phones, lines of credit, or even bank accounts.²¹

11. *Id.*

12. The problems with reporting births also apply to reporting deaths. *Id.* at 9–10.

13. See Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

14. INT'L. FUND FOR AGRIC. DEV., *Plan to Cut Global Poverty by 50% is Failing – Needs of Rural Majority Neglected*, <http://www.ifad.org/poverty/pr.htm> (last visited May 9, 2012).

15. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

16. *Id.*

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.*; see also INT'L. FUND FOR AGRIC. DEV., *Plan to Cut Global Poverty by 50% is Failing – Needs of Rural Majority Neglected*, *supra* note 14 (discussing

Without these rudimentary tools necessary to obtain economic stability and financial freedom, India's millions of poor have few implements with which they may climb out of poverty.

To combat the enormous challenges facing the poor, the Indian government has created a new agency, the Unique Identification Authority of India ("UIDAI").²² The agency is tasked with carrying out an unprecedentedly ambitious²³ plan: to obtain personal information from every Indian, and give each an official ID number, so that every person may obtain a personal bank account into which the government will directly deposit aid and thereby cut out the corrupt local middlemen.²⁴

The program is known as AADHAAR²⁵ ("foundation" in Hindi).²⁶ Its goal is to take both personal information, such as name and date of birth, and also biometric information, such as fingerprints and retina scans, to create a database of every Indian.²⁷ Each citizen will be issued a twelve digit ID number.²⁸ Devices linked to the country's cell-phone network will be able to process an individual's fingerprint and retina information and his or her AADHAAR number to verify his or her identity within eight seconds.²⁹ Ideally, the AADHAAR program could be a tremendous boon for the Indian poor, resulting in millions of Indians directly accessing subsidies for housing, health care, and food directly through deposits in bank accounts³⁰ for the first time. Additionally, the ID numbers will allow them to

the difficulties of rural poor worldwide in accessing markets and technology, and the resulting negative economic effects).

22. The Head of UIDAI is a Cabinet-level executive. *See Background, UNIQUE IDENTIFICATION AUTH. OF INDIA*, http://uidai.gov.in/index.php?option=com_content&view=article&id=141&Itemid=164 (last visited Dec. 20, 2011).

23. The world's current largest biometric database, the US-Visit program for visas, has information for fewer than one tenth of the individuals that UIDAI hopes to obtain. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

24. *Id.*

25. *See id.*

26. AADHAAR, <http://www.aadhaar.nl/> (last visited Dec. 20, 2011).

27. *See* Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

28. *Id.*

29. *Id.*

30. *Id.*

open lines of credit, obtain important technological tools like cell phones, and open banks accounts.³¹

In a country where only 47% of Indian households have bank accounts (compared to 92% of American households), increased access to banking will be an enormous source of growth for the national economy.³² The Indian central bank has agreed to accept AADHAAR numbers as adequate identification to issue bank accounts.³³ In conjunction, banks have introduced outposts at rural grocery shops or other small businesses with enough cash to handle the small deposits and withdrawals that will be made by the rural poor.³⁴ The outposts will have scanners to confirm identities, and in this way rural Indians will have access to rudimentary banking through the AADHAAR initiative.³⁵

There are concerns about the program, however, both economic and political. Leftists, for instance, worry that direct subsidies to the poor will limit support for welfare programs over time.³⁶ Others argue that it is costly and unnecessary, and that there are easier ways to fight the corruption which often stymies the poor in accessing aid programs.³⁷ This Note will focus on one legal issue that could pervert the noble goal of this revolutionary program: privacy rights. India is not known for its strong regime of privacy law,³⁸ and many fear that having one universal ID number will allow any private interactions with businesses, hospitals, or banks to be easily discoverable to perfect strangers, or to the government.³⁹ While its highest

31. *Id.*

32. Vince Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, WIRE (Aug. 19, 2011), http://www.wired.com/magazine/2011/08/ff_indiaid/all/1.

33. *Id.*

34. *Id.*

35. *Id.*

36. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

37. *Id.*

38. *Id.*

39. There is a joke in which an Indian man, Mr. Singh, calls to order a pizza, and gives his ID number to do so. The pizza vendor welcomes Mr. Singh back from his trip to Japan, because the vendor can access his travel records. He dissuades Mr. Singh from buying a seafood pizza and urges him towards a low-fat pizza option, because medical records indicate that Mr. Singh has high blood pressure and cholesterol. The vendor then refuses to accept Mr. Singh's credit card, and forces him to pay in cash, because he can

court has intimated that the Indian constitution harbors a right to privacy,⁴⁰ the country's aggressive anti-terror efforts are one of many indicators that the government is not highly concerned with protecting the privacy of its 1.2 billion citizens.⁴¹

India must undertake to ensure that the massive data collection does not infringe on the rights of its citizens. The country has not proven to be particularly reliable in making sure that the constitutional rights guaranteed to its citizens are enforced.⁴² For instance, in the last ten years, India has seen a spike in deaths of people who are imprisoned or otherwise held in police custody, with minorities particularly hard hit by the failure of India to enact and protect the fundamental rights provided by its constitution.⁴³ India's human rights watchdog, the National Human Rights Commission ("NHRC"), has come under scrutiny for failing to promote a national conversation about human rights.⁴⁴ In order to ensure that AADHAAR ac-

see that Mr. Singh has reached his credit limit and is in debt to his bank. When Mr. Singh finally becomes annoyed at the pizza man's knowledge about his personal affairs and starts cursing, the vendor gently reminds him to watch his language, noting that Mr. Singh was recently convicted of using abusive language towards a policeman. Usha Ramanathan, *A Unique Identity Bill*, 45 *ECON. & POL. WEEKLY* at 11 (July 24, 2010).

40. See *Rajagopal v. State of Tamil Nadu* (1994) 6 S.C.C. 632, 640–46. Where the autobiography of a prisoner was being published in a magazine, apparently without the prisoner's permission, the Supreme Court of India had to determine whether that was an imposition on the prisoner's privacy. The court indicated that there were two sources of privacy law in India. There is privacy which stems from tort law, and there is also an implicit right to privacy in the Indian Constitution. The court noted that it had looked to American cases like *Griswold v. Connecticut*, 381 U.S. 479 (1965) and *N.Y. Times Co. v. Sullivan*, 376 U.S. 254 (1964) to find that the constitution had an implicit privacy right, although that right was not an absolute one. Where privacy conflicts with other fundamental rights, like freedom of the press, the rights must be balanced. *Id.*

41. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

42. Seema Sengupta, *India's Human Rights Record Makes a Farce of Its Democracy*, *GUARDIAN* (July 22, 2011), <http://www.guardian.co.uk/commentisfree/2011/jul/22/india-human-rights>.

43. *Id.*

44. The United Nations was considering demoting the NHRC's status from that of a participant to that of an observer. Human rights non-governmental organizations and individuals working in the human rights committee submitted an unflattering report on the Commission. Manoj Mitta, *UN May*

completes its goals, India must pass comprehensive privacy legislation that provides for judicial remedies and other enforcement mechanisms for preventing privacy violations, so that what began as a project to help the poor does not become a tool for increasing violations of Indian citizens' privacy.

India should look to the personal data privacy regime of the European Union as a model for its own legal regime. A national privacy law is essential to the success of AADHAAR, and should contain four provisions contained in the EU laws: a prohibition on collecting data about race or caste, the implementation of a role for judicial review as a specific remedy for those whose personal information is improperly used, mechanisms through which individuals can object to the use of certain personal information, and finally, rules for informing individuals how and why their personal information is being used.

Part I of this Note will provide a brief overview of India's government, history, and problems with corruption. It will also discuss the current state of privacy rights in India, and India's proposed solution to the many problems facing the poor: AADHAAR. Part II will discuss the law of data privacy in Europe. Finally, Part III will conclude that AADHAAR is a program with vast potential to enhance the lives of hundreds of millions of people, but that it must be implemented with EU-style privacy protections to ensure that its worthwhile goals are not overwhelmed by the corruption and graft prevalent in Indian government.

I. PRIVACY IN INDIA

A. India's Government, History, and Corruption

"India is a Sovereign, Socialist, Secular, Democratic Republic with a parliamentary system of government" composed of

Downgrade NHRC Status, TIMES OF INDIA (May 23, 2011), http://articles.timesofindia.indiatimes.com/2011-05-23/india/29574012_1_nhrc-chairman-national-human-rights-commission-paris-principles.

Though the NHRC was allowed to maintain its participant status, the U.N. faulted the Commission for, among other things, not engaging with human rights workers in the country sufficiently and not having a credible method for handling complaints regarding human rights violations. Manoj Mitta, *India's Clout Ensures UN Status for NHRC*, TIMES OF INDIA (July 20, 2011), http://articles.timesofindia.indiatimes.com/2011-07-20/india/29793636_1_accreditation-panel-nhrc-paris-principles.

twenty-eight states and seven territories.⁴⁵ The executive branch of the Indian government is headed by the prime minister, assisted by a council of ministers that composes the “Cabinet Ministry” (or “Cabinet”).⁴⁶ The legislative branch of the government is the Indian Parliament (“Parliament”), which has two houses: Rajya Sabha, or the “Council of States,” and Lok Sabha, or the “House of the People.”⁴⁷ The president of India, who is the head of state,⁴⁸ is also part of the legislative arm of the government, and appoints a small number of the members of Parliament (“MPs”), the vast majority of whom are elected.⁴⁹

Parliament’s process for passing legislation is lengthy, with each bill proposed by a Cabinet Minister or an MP requiring four “readings” by Parliament, passage by both houses, and signature by the president to become law.⁵⁰ Parliament does not meet often, and passes few bills, averaging around forty per year since 2009.⁵¹ During a recent session, the legislative body intended to sanction fifteen bills, but only four were passed.⁵²

This tepid pace is exacerbated by the fact that India’s is a coalition government, meaning that the MPs are members of many different parties, not just one or two dominant ones.⁵³ The coalition government operates by reaching consensus, but the parties often have great difficulty reaching that consensus,⁵⁴ making the legislative process slow and unpredictable.⁵⁵

45. *Profile*, NATIONAL PORTAL OF INDIA, <http://india.gov.in/india-glance/profile> (last visited Jan. 28, 2013).

46. *Id.*

47. *Indian Parliament*, NATIONAL PORTAL OF INDIA, <http://india.gov.in/my-government/indian-parliament> (last visited Jan. 28, 2013).

48. *Profile*, NATIONAL PORTAL OF INDIA, *supra* note 45.

49. *Indian Parliament*, NATIONAL PORTAL OF INDIA, *supra* note 47.

50. *How a Bill Becomes an Act*, INDIAN PARLIAMENT, <http://164.100.47.132/LssNew/our%20parliament/Folder04.pdf> (last visited Jan. 28, 2013).

51. Niharika Mandhana and Hari Kumar, *Parliament’s ‘Monsoon’ Season Ends in Washout*, NY TIMES (Sept. 7, 2012), <http://india.blogs.nytimes.com/2012/09/07/parliaments-monsoon-session-ends-in-washout/>.

52. *Id.*

53. *Coalition Politics: Future of Indian Political System*, UPSC PORTAL (May 2012), <http://upscportal.com/civilservices/article/coalition-politics-future-of-indian-political-system>.

54. *Id.*

55. Subhajit Basu, *Policy-Making, Technology, and Privacy in India*, 6 INDIAN J.L. & TECH. 65, 78.

Judicial review over the legislative process is very active, which is another factor slowing the pace of legislation and making the process less predictable.⁵⁶

This sometimes unwieldy system of government came into being on January 26, 1950, when the Constitution of India came into force.⁵⁷ At the time, the nation had only recently gained its independence from British colonial rule in 1947,⁵⁸ partly as a result of an anti-British civil disobedience campaign started by Mahatma Gandhi in the early 1920s.⁵⁹ The country's history as a colonized and subordinated state makes it generally dubious of broad regulatory power.⁶⁰

Furthermore, India is a country with a history of religious strife and the subjugation of persons of "inferior" castes.⁶¹ The government has outlawed discrimination based on the ancient Hindu caste system, which designated each person to a permanent role in the social hierarchy, but it still influences Indian life.⁶² At least some of the popular resistance to the current government initiative to collect personal information stems from this history of discrimination.⁶³ For example, Aruna Roy, an advocate for India's poor, said that she found the idea of AADHAAR "obnoxious and frightening" because of the possibility for increased discrimination.⁶⁴

Even more than discrimination, the greatest impediment to the Indian poor is the nation's culture of corruption, which has resulted in India being ranked as ninety-fourth out of 183 countries in a survey of government transparency, placing it below South Africa and tying it with Colombia.⁶⁵ Given this

56. *Id.*

57. *Constitution of India*, NATIONAL PORTAL OF INDIA, <http://india.gov.in/my-government/constitution-india> (last visited Jan. 28, 2013).

58. *Profile*, NATIONAL PORTAL OF INDIA, *supra* note 45.

59. BBC NEWS: SOUTH ASIA, *India Profile Timeline* (Jan. 9, 2013), <http://www.bbc.co.uk/news/world-south-asia-12641776>.

60. Basu, *supra* note 55, at 77–78.

61. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

62. BBC NEWS: SOUTH ASIA, *India Profile Overview*, *supra* note 2.

63. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

64. *Id.*

65. *2012 Corruption Perceptions Index*, TRANSPARENCY INTERNATIONAL, available at <http://cpi.transparency.org/cpi2012/results/> (last visited Jan. 20,

culture, even if the impoverished stay in their villages, the rampant corruption of local officials in India results in a substantial portion of any government aid lining the pockets of local bureaucrats and politicians instead of reaching the intended recipients.⁶⁶

The corruption in India is not limited to local officials, but reaches the higher echelons of national government as well. Recent national scandals include a "cash for votes" scheme, the fraudulent selling of mobile phone licenses which cost the country nearly forty billion dollars, the misappropriation of homes intended for war widows, and financial irregularities that beset the Commonwealth Games.⁶⁷ Perhaps most telling, the chief of India's anti-corruption watchdog was forced to step down as he himself faces corruption charges.⁶⁸

Anger over the severe culture of corruption has been known to boil over; in some instances, officials in charge of meting out the significant government money intended for aid are attacked or even murdered.⁶⁹ For example, in Uttar Pradesh, one of the most corrupt provinces in India, three doctors were murdered, each of whom had at one point been in charge of spending the government money that was given to the province as part of a national government effort to improve the health of citizens.⁷⁰

2013). It has moved up one spot since 2011, when it ranked ninety-fifth out of 183 countries, below Colombia, South Africa, and Liberia. *2011 Corruption Perceptions Index*, TRANSPARENCY INTERNATIONAL, available at <http://cpi.transparency.org/cpi2011/results/> (last visited Jan. 28, 2013).

66. Many Indians took to the streets in August and September of 2011 to support the hunger strike of Anna Hazare, an Indian activist protesting the rampant corruption permeating the government. There is growing opposition to graft, as young Indians become more invested in the economy and concerned about the human rights practices of their country. See Dipankar Gupta, *Waving the Flag Against Corruption*, NY TIMES (Sept. 17, 2011), <http://india.blogs.nytimes.com/2011/09/17/waving-the-flag-against-corruption/>.

67. *India's Corruption Scandals*, BBC NEWS SOUTH ASIA (Aug. 19, 2011), <http://www.bbc.co.uk/news/world-south-asia-12769214>.

68. *Id.*

69. See Lydia Polgreen, *Health Officials at Risk as India's Graft Thrives*, N.Y. TIMES (Sept. 17, 2011), <http://www.nytimes.com/2011/09/18/world/asia/graft-poisons-uttar-pradeshs-health-system-in-india.html?pagewanted=all>.

70. *Id.*

Compounding the citizenry's distrust of government is the perception that it is not taking the plight of the poor sufficiently seriously.⁷¹ For instance, the recent declaration by the government that any urban citizen who spends more than thirty-two rupees a day, the equivalent of approximately sixty-five American cents, is not poor has caused many Indian citizens to feel that the government has unrealistic views of how much money it takes to survive in India.⁷²

The slowness of enacting legislation, a historical and cultural resistance to broad regulatory regimes, corruption, and distrust of the government are all potential roadblocks for the implementation of effective and broad privacy protections for the AADHAAR program.

B. Privacy Rights in India

While the Parliament has historically displayed a reluctance to implement personal data privacy laws, judicial officers in India have been less averse to bolstering notions of privacy.⁷³ The Indian constitution guarantees fundamental rights,⁷⁴ and makes the supreme court the protector of those rights.⁷⁵ In the 1964 case of *Kharak Singh v. State of U.P.*,⁷⁶ the supreme court

71. See *id.*; see also Nikhila Gill, *Delhi on 32 Rupees a Day*, N.Y. TIMES (Sept. 26, 2011), <http://india.blogs.nytimes.com/2011/09/26/delhi-on-32-rupees-a-day/#more-2875>. Many citizens are dubious of such governmental declarations, especially when members of Parliament recently underwent a pay raise. The government has a credibility problem with those struggling to survive on urban streets in India. Ajit, a twenty-eight year old entrepreneur with a new business and finance degree, said "thirty-two rupees is not sufficient for anyone, not even for a beggar. If someone's going to buy food from a store then [thirty-two rupees] isn't going to afford him much. If they're going to pick from a garbage bin, then maybe." *Id.*

72. See Nikhila Gill, *Delhi on 32 Rupees a Day*, *supra* note 71.

73. Basu, *supra* note 55, at 77.

74. INDIA CONST. arts. 17–35, *supra* note 5.

75. *Id.*

76. *Kharak Singh v. State of UP*, (1964) 1 SCR 332, 359 (India). Plaintiff challenged local police regulations which allowed for monitoring and surveillance of him and his home as violative of his constitutional rights to freedom of movement and personal liberty. The court held that surveillance occurring via visits to his home violated Article 21 of the constitution of India. While the court noted that privacy was not a fundamental right laid out in the constitution, it did explain that privacy is central to personal liberty, especially as it concerns privacy against arbitrary intrusion into one's home by the state.

of India recognized that there is an implied right to privacy in Article Twenty-One of the Indian constitution.⁷⁷ The supreme court and other courts within India have more recently expanded on this notion.⁷⁸

Traditionally, the Indian conception of privacy has centered more on personal and domestic privacy, and less on data and information privacy.⁷⁹ Prior to the advent of the AADHAAR program, India's main concern with data protection was economic.⁸⁰ Due to its enormous outsourcing industry,⁸¹ a staggering amount of data from foreign lands streams into India.⁸² Until recently, the only privacy protection for all of this data was self-regulation.⁸³ The information technology industry formed its own self-regulatory body, the Data Security Council of India, operating on the idea that the industry was in the best place to create a regulation regime for data privacy because of its substantial expertise in the area.⁸⁴ The enormity of the economic interests at stake, however, compelled the government to get involved in the realm of data protection and data privacy for businesses.⁸⁵

In 2000, the Parliament passed information technology legislation to assuage foreign companies' reluctance to outsource to

77. Basu, *supra* note 55, at 79.

78. See *Rajagopal v. State of Tamil Nadu*, *supra* note 42. See also *People's Unions for Civil Liberties v. Union of India*, (1997) 1 S.C 1203 (India) (holding that improper wiretapping violates the Article 21 of the Indian Constitution because the right to personal liberty includes the right to privacy).

79. See Basu, *supra* note 55, at 69–74; however, a national Do Not Call Registry has also been formed, which indicates that Indians are growing more interested in the notion of privacy as the right to be let alone. Latha R. Nair, *Data Protection Efforts in India: Blind Leading the Blind*, 4 INDIAN J.L. & TECH. 19, 24–26 (2008).

80. See Basu, *Policy-Making, Technology, and Privacy in India*, *supra* note 55, at 81.

81. The information technology and outsourcing industries generate more than sixty billion dollars a year for the Indian economy. James Fontella-Kahn, *IT Outsourcing Drives India's Economic Ascent*, FIN. TIMES (July 27, 2010), <http://www.ft.com/intl/cms/s/0/227120e2-9994-11df-a852-00144feab49a.html#axzz1hDCXYBQ4>.

82. Basu, *supra* note 55, at 81.

83. *Id.*

84. Nair, *supra* note 79, at 24.

85. See Basu, *supra* note 55, at 81.

India.⁸⁶ The amendment requires businesses to keep up reasonable security practices for sensitive data.⁸⁷ The amendment deals only with corporate, and not state, actors.⁸⁸ Though it leaves many holes,⁸⁹ the law is at least an indication that Indian regulators are taking notice of the need for protection of data.

Just as with the data privacy laws for corporations, economic concerns also spurred the creation of AADHAAR,⁹⁰ and those same concerns should cause the federal government to create laws which protect the personal information of Indian citizens.⁹¹ The government has already enacted laws to prevent private actors from abusing personal information, adopting piecemeal regulations that are meant to protect data.⁹² These regulations allow for individuals to contract so that data transactions are as secure as they wish. For example, the Indian Contract Act of 1872⁹³ allows for companies importing data to contract to ensure that high standards of data protection are met.⁹⁴ Other rules fill niches of data privacy. For instance, there is an act which codifies the tradition of "maintaining confidentiality in bank transactions."⁹⁵ Another act recognizes the privacy of those using credit lines, acknowledging that credit information must be collected according to privacy regulations.⁹⁶

86. The Information Technology Act, No. 21 of 2000, INDIA CODE (2000) *amended by* The Information Technology Amendment Act, No.10 of 2009, INDIA CODE (2009). Basu, *supra* note 55, at 84.

87. *Id.*; *see also* Basu, *supra* note 55, at 84.

88. Nair, *supra* note 79, at 23.

89. The amendment does not deal with personal data processing, or provide precautions to be taken while collecting data, etc. *Id.*

90. AADHAAR is an important part of India's quest to include its hundreds of millions of poor in its economy. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

91. *See* R. Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, THEHINDU.COM (Dec. 16, 2011), <http://www.thehindu.com/news/national/article2698907.ece>.

92. *See* Basu, *supra* note 55, at 82.

93. The Indian Contract Act, No. 9 of 1872, INDIA CODE (amended 1972).

94. Basu, *supra* note 55, at 82.

95. The Recovery of Debts Due to Banks and Financial Institutions Act, No. 51 of 1993, INDIA CODE (1993); *see* Basu, *supra* note 55, at 82.

96. The Credit Information Companies Regulation Act, No. 30 of 2005, INDIA CODE (2005); *see* Basu, *supra* note 55, at 82.

Piecemeal as they are, these Indian data privacy laws reflect the Indian reluctance to enact broad regulations.⁹⁷ While the laws do reflect India's recognition of the need to protect personal data in some situations, the Indian laws are less comprehensive than those of the European Union.⁹⁸ Some would argue that Indian notions of privacy are very different from Western ones,⁹⁹ and therefore that sweeping, Western-style privacy laws are ill-suited to fit the needs of India.¹⁰⁰ However, in an undertaking as vast as AADHAAR,¹⁰¹ privacy concerns cannot rely on a patchwork of rules that is a mix of "constitutional, customary, and common law rights scattered across various legal fields."¹⁰² Instead, India should take its cues from those Western laws that have addressed data privacy more comprehensively, so that it can ensure the success and credibility of the AADHAAR program.¹⁰³

C. AADHAAR

The AADHAAR program, by using biometric information, hopes to weed out the corruption, fraud, and graft that dominate the Indian welfare system.¹⁰⁴ Under the program, a fingerprint or retina scan will be necessary for identification purposes.¹⁰⁵ Lawmakers hope that, by requiring not just a physical card but also matching biometric information, fraud will de-

97. See Basu, *supra* note 55, at 77–78.

98. *Id.* at 82.

99. *Id.* at 69–74.

100. *Id.* at 86–88.

101. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

102. Basu, *supra* note 55, at 77.

103. Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, *supra* note 91 (noting that the Parliament will not pass an establishing bill unless a national data privacy law is passed). The laws need to be easy to navigate, and largely devoid of loopholes. *Id.*

104. Baba Umar, *The Trouble with Big Brother's Eye*, TEHELKA MAG. (May 21, 2011), http://www.tehelka.com/story_main49.asp?filename=Ne210511TROUBLE.asp. Even in the United States, some public assistance is lost to fraud when criminals steal or fraudulently obtain a number of different identification cards. See generally James A. Killerlane III, Note, *Finger Imaging: A 21st Century Solution to Welfare Fraud at Our Fingertips*, 22 FORDHAM URB. L.J. 1327, 1327 (1995). Killerlane argues that implementing biometric information will easily identify those in need and keep criminals from defrauding the system, resulting in greater efficiency overall. *Id.*

105. Umar, *The Trouble with Big Brother's Eye*, *supra* note 104.

crease¹⁰⁶ and aid programs will be able to be administered to the poor more efficiently.¹⁰⁷ The program is federally administered and, in fact, the head of UIDAI is a member of the Cabinet.¹⁰⁸ By placing the administration of AADHAAR at the highest level of executive government, the government has ensured that the public and the press will keep a watchful eye on the program, subjecting it to close scrutiny.¹⁰⁹

Making the program a "poster child" for good governance could instill confidence, but it is a risky move for the government.¹¹⁰ On the one hand, enacting the program shows the public that the government is making a serious attempt to combat corruption within India, and especially that corruption which most hurts the poor. On the other hand, should the program fail by becoming corrupt itself or by failing to protect the privacy of the Indian public, it will only add to the notion that the Indian government cannot function efficiently and fairly. The stakes for the UIDAI system are high, and therefore, the privacy regulations that India enacts for the program should be strong enough to reflect its importance.¹¹¹

Enrolling in AADHAAR is voluntary.¹¹² It might be difficult to persuade poor Indian citizens to have their irises scanned, as millions of them have never even seen a computer.¹¹³ However, it is important for them to enroll, because as the AADHAAR system is increasingly utilized, it would be increasingly difficult for citizens to function without having an ID number.¹¹⁴ Therefore, the government needs to create the right incentives

106. See generally Killerlaine III, *Finger Imaging: A 21st Century Solution to Welfare Fraud at Our Fingertips*, *supra* note 104.

107. For example, one Indian woman, Kiran, and her three children were scanned and received ID numbers. She said she planned to first use the AADHAAR number to obtain a city card that would authorize her to receive subsidized groceries. "I've tried very hard to get one before, but they wouldn't give it to me because I couldn't prove I live in Delhi" she said. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

108. See *Background*, UNIQUE IDENTIFICATION AUTH. OF INDIA, *supra* note 22.

109. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

110. *Id.*

111. *Id.*

112. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32, at 5.

113. *Id.* at 1.

114. *Id.* at 5.

so that people will see that the benefits of the program override the potential negative effects.¹¹⁵ As noted, national legislation will create a greater sense that the risks associated with joining the program are small, while the potential payoff, especially for the poor, is substantial. So far, however, the Parliament has failed to enact legislation to govern AADHAAR and thereby legitimize it.

1. Enacting Legislation

UIDAI has been operating under an executive order in India.¹¹⁶ The AADHAAR program it administers is thus operating without legislative backing.¹¹⁷ On September 24, 2010, the Cabinet approved the *National Identification Authority of India Bill, 2010* ("Bill") for introduction to Parliament,¹¹⁸ which was then formally introduced to that body on December 3, 2010.¹¹⁹ Because one of the main arguments against UIDAI and AADHAAR is that both are operating in the executive branch, without having been sanctioned or appropriately supervised by the legislative branch of government,¹²⁰ it is very important that Parliament approve the Bill.

Unfortunately, the Parliamentary Standing Committee on Finance ("SCOF") dealt a blow to the passage of the Bill by recommending that Parliament reconsider it.¹²¹ SCOF cited sever-

115. *Id.* at 1.

116. *See Background*, UNIQUE IDENTIFICATION AUTH. OF INDIA, *supra* note 22.

117. R. Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, *supra* note 91.

118. *Indian Cabinet Approves Introduction Of National Identification Authority of India Bill, 2010 in Parliament*, MEDIANAMA.COM (Sept. 25, 2010), <http://www.medianama.com/2010/09/223-indian-cabinet-approves-introduction-of-national-identification-authority-of-india-bill-2010-in-parliament/>.

119. Gopal Krishna, *National Identification Authority of India Bill Introduced in Parliament*, MEDIAVIGIL.COM (Dec. 3, 2010), <http://mediavigil.blogspot.com/2010/12/national-identification-authority-of.html>.

120. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4; Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, *supra* note 91.

121. *Blow to AADHAAR project as Bill is rejected*, THE HINDU.COM (Dec. 8, 2011), <http://www.thehindu.com/news/national/article2698907.ece>; *see also* Standing Committee on Finance, Fifteenth Lok Sabha, *Forty-Second Report* (Dec. 2011), *available at* <http://www.prsindia.org/uploads/media/UID/uid%20report.pdf>.

al reasons why it disapproved of the Bill, including privacy concerns,¹²² and asked the Cabinet to bring forth alternative legislation on the issue.¹²³ Notably, SCOF took issue with the government for trying to implement AADHAAR without first enacting a national data privacy law.¹²⁴

UIDAI and AADHAAR are not doomed yet, as SCOF will still need to present its report to the entire Parliament.¹²⁵ Additionally, it is not clear that UIDAI would stop administering the program even if the Bill is eventually rejected by Parliament.¹²⁶ However, the SCOF report has led at least some commentators to call for the end of the program,¹²⁷ and it has certainly not given more credibility to the massive undertaking. As there is some discussion in India that AADHAAR does not pass constitutional muster without legislative sanctioning,¹²⁸ and because the program is seen by some as a giant executive regulation with little oversight by democratically elected Parliament members,¹²⁹ passage of the legislation is essential to the program's success. Placing control of this massive program solely

122. The report criticizes the executive branch of the government for starting to enroll people in AADHAAR before Parliament approved the Bill. Parliament rejected the government's contention that there was no legal barrier to the executive running the program without legislative approval. The cost of the program concerned SCOF, which also had national security concerns and concerns about the safety of the personal information of those possessing AADHAAR numbers. A sticking point was the program's stated goal to register every "resident," not every "citizen." Finally, SCOF questioned the general safety of the use of biometrics, calling it "untested, unreliable technology." Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, *supra* note 91; *see also* Standing Committee on Finance, *supra* note 121.

123. Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, *supra* note 91.

124. *Blow to AADHAAR project as Bill is rejected*, *supra* note 121.

125. It is not clear that Parliament will in fact reject the Bill. At least one member of SCOF, Rashid Alvi, submitted a note of dissent with the report, saying that while recommendations should be made to the government, the Bill should not be rejected outright. *Blow to AADHAAR project as Bill is rejected*, *supra* note 121.

126. The government can choose to overrule the SCOF report if it chooses. Chokkapan S., *Will AADHAAR see the light of the day?*, CIOL.COM (Dec. 20, 2011), <http://www.ciol.com/News/News/News-Reports/Will-Aadhaar-see-the-light-of-the-day/158046/0/>.

127. *See generally* Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, *supra* note 91.

128. *See id.*

129. *See id.*

in the hands of a Cabinet-level office, while neglecting both the judiciary and the legislature, is unsavory for many Indians.¹³⁰

In order to most effectively address the concerns raised by the SCOF report, the government must pass a national data protection law which ensures the privacy of individuals whose information is collected by AADHAAR. The Cabinet displayed a troubling lack of concern about such a privacy law when it submitted the Bill to SCOF, opining simply that “collection of information without a privacy law in place does not violate the right to privacy of the individual.”¹³¹ Only with the appropriate privacy controls, however, will Parliament be likely to pass the Bill and allow the government to continue its mission of helping India’s poor access economic channels in a manner that most Indians find legitimate.¹³²

2. Privacy Controls

Thus far, the main privacy control on UIDAI is that the number of people working on its implementation has been kept surprisingly small for such an enormous project.¹³³ There are detailed guidelines for admitting volunteers to work in UIDAI on the AADHAAR project.¹³⁴ The guidelines include a detailed code of conduct, which stipulates, among other things, that volunteers are prohibited from revealing any information from or about UIDAI¹³⁵ and from interacting with the media.¹³⁶ UIDAI guidelines also mandate screening of volunteers for conflicts of interest,¹³⁷ and allow for their dismissal if their skills are no longer necessary to the project.¹³⁸

130. *See id.*

131. *Id.*

132. *Id.*

133. Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4; UIDAI headquarters take up “a couple of floors,” and the atmosphere of the office is “more like a start-up than a government ministry.” Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32, at 1.

134. *See* UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UIDAI), *Guidelines for Recruitment of Volunteers*, available at http://uidai.gov.in/images/FrontPageUpdates/volunteer_guidelines_2011.pdf (last visited Dec. 21, 2011).

135. *Id.* at 5(a)(2).

136. *Id.* at 5(a)(4).

137. *Id.* at 4(a)(2).

138. *Id.* at (6)(1).

These guidelines demonstrate that UIDAI is, at the least, paying attention to its reputation for privacy and trustworthiness.¹³⁹ This is prudent, as it wants to encourage as many people as possible to take part in the voluntary program.¹⁴⁰ Yet the national unrest about corruption¹⁴¹ makes it likely that any privacy concerns the program raises are likely to become controversial. Therefore, privacy implementations far beyond personnel guidelines are necessary to make the program a viable one.

II. EUROPEAN UNION PRIVACY LAWS

The European Union, comprised of twenty-seven nations and with twenty-three official languages,¹⁴² is in some ways akin to

139. There are also guidelines on hiring volunteers who wish to move from employment in the private sector in India to work in the government, for hiring individuals on sabbatical from their usual jobs, and for taking on interns who wish to work in the public sector. See UNIQUE IDENTIFICATION AUTHORITY OF INDIA, *Guidelines for Recruitment of Personnel on Sabbatical/Secondment*, available at http://uidai.gov.in/images/FrontPageUpdates/sabbatical_guidelines_2011.pdf (last visited Dec. 21, 2011) and UNIQUE IDENTIFICATION AUTHORITY OF INDIA, *Internship Guidelines 2011*, available at http://uidai.gov.in/images/FrontPageUpdates/internship_guidelines_8_march_2011.pdf (last visited Dec. 21, 2011).

140. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

141. See Gupta, *Waving the Flag Against Corruption*, *supra* note 66 (regarding the aforementioned street protests in support of the hunger strike of Anna Hazare). In response to the protests, the Cabinet introduced anti-graft legislation. However, the legislation fell short of the protesters' demands. The proposed legislation creates a body for hearing complaints but, in Hazare's and his followers' opinions, did not do enough to give the body any "teeth" to conduct investigations. Hazare has threatened to begin another strike and protesters have sworn to take to the streets again unless a strong anti-graft bill is passed. Andrew MacAskill and Bibhudatta Pradhan, *Indian Cabinet's Anti-Graft Bill Brings Vow of Further Protests*, BLOOMBERG BUSINESSWEEK (Dec. 21, 2011), <http://www.businessweek.com/news/2011-12-21/indian-cabinet-s-anti-graft-bill-brings-vow-of-further-protests.html>.

142. *Countries*, EUROPA, http://europa.eu/about-eu/countries/index_en.htm (last visited October 21, 2012). There are also many more minority and regional languages and dialects in Europe. Press Release, European Union, 10th European Day of Languages: What's Happening Near You (Sept. 23, 2011), available at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1065&format=HTML&aged=0&language=EN&guiLanguage=en>.

India. More than 300 languages or dialects are spoken in India. The cultures of India include “everyone from Himalayan mountain villagers to Bangalorean call-center workers, from Rajasthan desert nomads to Mumbai street beggars.”¹⁴³ Also similarly to India,¹⁴⁴ the EU’s legislative approach to data privacy stemmed from business considerations, not from anxiety about the government’s data-gathering. The European Parliament, with members elected by European citizens, and the Council, made up of representatives of the national governments of EU member nations, pass legislation to ensure that goods and services move freely throughout the Union.¹⁴⁵ The regulations and directives of the EU are enforced by the European Commission and the European Court of Justice.¹⁴⁶ The EU’s privacy controls were born in response to concerns about multinational companies exchanging data across Europe without uniform regulation.¹⁴⁷

Unlike in India, however, the European Union privacy law followed an omnibus approach,¹⁴⁸ meaning that it created a comprehensive law which reflects the belief that data privacy is a fundamental human right.¹⁴⁹ The fierce belief in, and protection of, an individual’s right to privacy is both a feature of the civil law tradition¹⁵⁰ and a remnant of the horrors caused by the use of personal information by former domestic, despotic

143. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

144. Nair, *supra* note 79, at 20.

145. *Basic Information on the European Union*, EUROPA, http://europa.eu/about-eu/basic-information/index_en.htm (last visited Jan. 28, 2013).

146. *Id.*

147. ILMR Editors, *International Data Privacy Laws and the Protectors of Privacy*, 5 B.Y.U. INT’L L. & MGMT. REV. 173, 177–78 (2008).

148. This is in contrast to the U.S. approach. Rather than create an omnibus privacy law, the legislature has created several laws, like the Fair Credit Reporting Act, to protect data privacy. Perhaps because the United States is more concerned with free speech and the free flow of information than with individual privacy, and is generally distrustful of government intervention in the private sphere, it is less protective of data privacy than the EU. Deborah Roach Gaut and Barbara Crutchfield George, *Offshore Outsourcing to India by U.S. and E.U. Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business*, 6 U.C. DAVIS BUS. L. J. 13 (2006).

149. So important is the right to data privacy in the EU that several countries have explicitly included it in their constitutions. *Id.*

150. *Id.*

regimes of EU member states.¹⁵¹ While in the early 1980s there was indifference to data privacy on the parts on many EU nations, by the later years of the decade disputes among nations regarding data privacy were on the rise.¹⁵² France in particular blocked the transfer of personal data to Italy and Belgium due to their lax data privacy laws.¹⁵³ Faced with these disputes between member nations, the EU gave increased power to privacy regulators and harmonized privacy protection within Europe¹⁵⁴ by enacting a directive on privacy (the "EU Directive").¹⁵⁵

Establishing a body of privacy regulators and imposing stringent set of primary regulations, the EU Directive is a strong law for data privacy protection.¹⁵⁶ This greater power meant that the privacy regulators could control market access and restrict access to EU markets to companies that had adequate privacy protection.¹⁵⁷ The EU Directive also imposed three serious requirements on EU members.¹⁵⁸ First, each country must enact legislation for both the public and private sectors.¹⁵⁹ Second, each must create a government agency responsible for enforcing the directive.¹⁶⁰ Third, each country must ensure that non-member countries with which it does business have data

151. Most notably Germany's. *Id.*

152. ILMR Editors, *International Data Privacy Laws and the Protectors of Privacy*, *supra* note 147.

153. *Id.*

154. *Id.* at 178.

155. Directive 1995/46 of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (EC) ("EU Directive"). The Preamble of the EU Directive notes that right to privacy is one of the fundamental rights of living in the EU and a general principle of the EU Community, and the EU Directive is intended to protect data at a high level.

156. See Gaut and George, *supra* note 147.

157. Article 25 of the EU Directive requires that European data transfers only occur with those countries with adequate data privacy laws. By EU standards, the United States does not have strong enough privacy protection. The United States, however, was able to negotiate a deal in which American companies were allowed to transfer data from their European business partners if the companies complied with EU standards. ILMR Editors, *International Data Privacy Laws and the Protectors of Privacy*, *supra* note 147, at 178.

158. *Id.*

159. *Id.*; Directive 1995/46, *supra* note 156, at art. 4(1).

160. ILMR Editors, *International Data Privacy Laws and the Protectors of Privacy*, *supra* note 147 at 178; Directive 1995/46, *supra* note 156, at art. 28.

protection laws that are up to EU standards.¹⁶¹ Because it is such a huge market, the EU is able to exert its data privacy rules on extraterritorial countries who depend on access to the European market.¹⁶²

The EU's data privacy concerns have spread beyond the business context into the realm of collection and retention of information by governments.¹⁶³ As one of the strongest data privacy laws in the world,¹⁶⁴ the EU Directive contains strict rules for data collection by governments,¹⁶⁵ laying out specific prerequisites for making any personal data collection legitimate.¹⁶⁶ For instance, personal data may only be processed if the person from whom it being taken unambiguously consents.¹⁶⁷ No data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, or a subject's health and sex life may be processed.¹⁶⁸ While terrorist attacks in Spain and the United Kingdom loosened this tight regulatory scheme somewhat in 2005,¹⁶⁹ the EU was

161. ILMR Editors, *supra* note 149; Directive 1995/46, *supra* note 156, at art. 29.

162. ILMR Editors, *International Data Privacy Laws and the Protectors of Privacy*, *supra* note 147 at 178, 180.

163. *Id.*

164. Basu, *Policy-Making, Technology, and Privacy in India*, *supra* note 55, at 87.

165. *See* Directive 1995/46, *supra* note 156, at rec. 7 (noting the economic importance of free movement of data and the problems caused by disparate member country laws regarding data protection).

166. *See id.*

167. *Id.* at art. 7 (1). Article 7 of the EU Directive provides a few other baselines for when data may be collected other than when the subject consents. For instance, data may be collected if the subject has a legal or contractual obligation which requires it.

168. There are exceptions for consent, and the legitimate use of such information. *Id.* at art 8. Such a rule is an important one for AADHAAR to adopt in some fashion. In a country where caste and religion have been causes of strife, there are fears that collection will make it easier for government actors to discriminate. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

169. ILMR Editors, *International Data Privacy Laws and the Protectors of Privacy*, *supra* note 147, at 184–85. The changes made in the law in response to terrorist attacks in the United States, Spain, and England were not as drastic as those enacted in the United States. However, the fact that the law was changed at all demonstrates that privacy and data protection are, even in the EU, balanced against other concerns, such as national security. *Id.* at 184–85.

still able to maintain strict control on governments' ability to maintain data privacy, limiting the use of retained data to issues "directly related to international criminality."¹⁷⁰

The EU Directive allows individuals to exercise control over their personal information. Importantly, the Directive calls for the availability of remedies to those whose information has been improperly taken or used.¹⁷¹ Each member state is required to provide a judicial remedy for those whose privacy rights, as guaranteed by the national data privacy laws, have been breached.¹⁷² People who have been damaged as a result of improper data collection are entitled to receive compensation from those who control the collected data.¹⁷³ Additionally, each member country is obligated to impose sanctions on those who infringe on privacy rights in violation of the EU Directive.¹⁷⁴

Further, the EU Directive requires that collectors of personal information communicate with the subjects from whom they collect personal data,¹⁷⁵ and mandates that those subjects have access to it¹⁷⁶ and object to its use.¹⁷⁷ The data collector must identify himself to the subject, tell the subject who will see the data, and inform the subject of how his personal information will be used.¹⁷⁸ Furthermore, an EU citizen must be able to obtain responses to questions about whether and how such personal information is being used, and must be able to do so quickly and cheaply.¹⁷⁹ Finally, data subjects must be able to object to the use of their personal information for direct marketing purposes,¹⁸⁰ and to object, for compelling reasons, to the use of information for other purposes.¹⁸¹

170. *Id.* at 184.

171. Directive 1995/46, *supra* note 156, arts. 22–24.

172. These judicial remedies are without prejudice to administrative remedies at the EU level. *Id.* art. 22.

173. Provided that responsibility on the part of the collector can be shown. *Id.* art. 23.

174. *Id.* art. 24.

175. *Id.* arts. 10, 11.

176. *Id.* art. 12.

177. *Id.* art. 14.

178. Collectors must also inform the subject as to whether his responses are voluntary or mandatory. *Id.* art. 10.

179. Subjects should also be able to change or erase data that has been collected improperly. *Id.* at art. 12.

180. *Id.* art. 14(b).

181. *Id.* art. 14(a). What these "other purposes" might be is unclear.

These are just some of the ways in which the EU Directive provides protection of personal information from private and public actors alike.¹⁸² The strong protections in the EU are substantially influenced both by cultural notions of privacy and by notions of the government's role in protecting it.¹⁸³

The European culture is obviously quite different from that of India, and for this reason it is unlikely that a wholesale adoption of the rules of the EU Directive would be feasible or effective in India.¹⁸⁴ However, India should look to some of the provisions of the EU Directive, highlighted here, as it attempts to create a national privacy law that will make AADHAAR sustainable.

III. ANALYSIS

AADHAAR could be a breakthrough for the nameless poor of India, giving identities to those who are all but invisible and granting access to credit markets, bank accounts, government aid, cell phones, and other benefits that were previously out of reach.¹⁸⁵ However, if strict privacy controls and regulations are not enacted the system could become yet another of India's notoriously corrupt government projects, helping only already-corrupt government officials. The anti-corruption movement¹⁸⁶ in India may be the harbinger of a future with less corruption and less stolen funding, but even as the government enacts an anti-graft bill¹⁸⁷ it is clear that that day has not yet come.¹⁸⁸ While it endeavors to create a potentially stronger anti-graft

182. *See id.* for the many other provisions.

183. *See* Gaut and George, *supra* note 147.

184. *See* Basu, *supra* note 55, at 86–87.

185. *See generally* Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4; *see also* Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

186. *See* Craig Jeffrey, *India's Vibrant Anti-Corruption Activists*, BBC NEWS MAGAZINE (Dec. 3, 2011), <http://www.bbc.co.uk/news/magazine-16003576>; *see also* Gupta, *Waving the Flag Against Corruption*, *supra* note 66.

187. Parliament passed an anti-graft bill in December 2011. *Lower House Passes Anti-graft Bill in India*, CNN (Dec. 27, 2011), <http://www.cnn.com/2011/12/27/world/asia/india-corruption-bill/index.html>.

188. Anna Hazare has threatened further strikes and protests over what he considers to be a watered-down anti-graft bill being debated in India's Parliament. Frank Jack Daniel, *Anna Hazare Vows New Protests Over Lokpal Bill*, REUTERS (Dec. 22, 2011), <http://in.reuters.com/article/2011/12/22/anna-hazare-vows-new-protests-over-lokpa-idINDEE7BL0B020111222>.

and anti-corruption culture, India requires strong privacy protections for AADHAAR.

The recent SCOF report, discussed in Part I.C.1, demonstrates the importance of a national privacy law for the long-term prospects of AADHAAR.¹⁸⁹ While the report lists several privacy concerns, SCOF cited two complaints of specific importance: first, that the data collected by AADHAAR would not be sufficiently safe for national security purposes, and second, that there is no preexisting national data privacy law to protect Indian individuals from government misuse.¹⁹⁰ A data privacy law could address security of information for national security purposes and also for personal privacy purposes,¹⁹¹ thus addressing both major concerns and potentially preventing the parliament's disavowal of AADHAAR. A data privacy bill modeled on the EU Directive could encourage free business practices¹⁹² while maintaining the privacy of individuals.

India's general reluctance to implement sweeping data privacy laws,¹⁹³ and its piecemeal privacy legislation,¹⁹⁴ reflects differences between Indian and Western notions of privacy.¹⁹⁵ Conceptions of privacy in India relate more to personal privacy and modesty¹⁹⁶ than to the notions of inherent rights that inform European ideas of "owning" or being entitled to personal information.¹⁹⁷ The Indian people are not as concerned as their European counterparts with privacy as it relates to their personal data¹⁹⁸ and therefore there is less political pressure in forming national privacy laws in India than in Western countries.¹⁹⁹ Moreover, India's move in the early 1990s from a highly regulated, state-run economy to one driven more by the pri-

189. See Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, *supra* note 91.

190. *Id.*

191. As the EU Directive does. See Directive 1995/46, *supra* note 156.

192. As AADHAAR aims to do. See Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

193. Basu, *supra* note 55, at 77.

194. *Id.*

195. *Id.* at 69–74.

196. *Id.*

197. See Gaut and George, *supra* note 147.

198. Basu, *supra* note 55, at 69–74.

199. *Id.* The political pressures may be changing, as evidenced by both the anti-corruption movement and the introduction of the anti-graft bill, as well as the SCOF report's criticism of the lack of a data privacy law.

vate sector has made the Indian people even more skeptical of far-reaching regulatory regimes.²⁰⁰

Whatever the difficulties facing the implementation of legislative protection for the personal information collected by AADHAAR, the passage of such legislation remains essential. The consequences of inadequate privacy protections could be devastating for constitutional and human rights in India.²⁰¹ Even if many Indians do not feel strongly about their right to safe personal data, unprotected personal information can smooth the road for the government to track and monitor people, resulting in the sorts of privacy invasions unpalatable to most Indians.²⁰²

Opponents of AADHAAR are concerned that the ID cards will make it easier for discrimination to occur.²⁰³ Although AADHAAR has a rule against collecting information about race and caste, local governments are allowed to ask questions about these personal traits and link such information to the AADHAAR number,²⁰⁴ creating serious concerns for human rights activists.²⁰⁵ While the negative feelings about regulatory action may be strong,²⁰⁶ the need for strong protection of personal information is at its greatest when a government implements a program as unique, and as massive, as AADHAAR.

The erosion of civil liberties is a concern for many of those in opposition to UIDAI and AADHAAR.²⁰⁷ One opponent notes that national ID cards or ID numbers have only been adopted in a small number of countries worldwide, largely because of the fears that the numbers will be misused.²⁰⁸ Even in the

200. Basu, *supra* note 55, at 77–78.

201. See Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, *supra* note 91; see also Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

202. See Polgreen, *With National Database, India Tries to Reach the Poor*, *supra* note 4.

203. *Id.*

204. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

205. *Id.*

206. See, e.g. Basu, *supra*, note 55 at 86–87; Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, *supra* note 91.

207. See Ramakumar, Opinion, *Aadhaar: Time to Disown the Idea*, *supra* note 91.

208. Ramakumar notes that the first proposals for national ID cards in India came from a right-wing government group wishing to restrict illegal im-

United States, where the use of Social Security numbers is well established, the use of national ID cards raises constitutional concerns.²⁰⁹ The fear of “functionality creep,”²¹⁰ which occurs when an ID card or number is used for purposes other than for which it was intended, especially for purposes of profiling along lines of race, drives some of the skepticism behind the UIDAU project.²¹¹ Opponents have also noted the absence of meaningful discussion of possible privacy and human rights violations in UIDAI documents detailing the project.²¹² The system was introduced with an eye toward making access available to private enterprises, toward the creation of “pay-as-you-go” systems, and toward the maintenance of health records. Many are skeptical of a government taking private information and storing it, fearing the potential involvement of private organizations in its use of the information.²¹³ The promises to respect privacy so far have been rudimentary,²¹⁴ and are not likely to reassure citizens who are fearful that the program will be used improperly.

Another source of opposition to the project is its reliance on technology.²¹⁵ The collection of biometric information has been particularly troubling to some who feel that there is too much

migration to the country. R. Ramakumar, *The Unique ID Project in India: A Skeptical Note*, 6005 ETHICS & POLY BIOMETRICS: LECTURE NOTES IN COMPUTER SCI., 153, 156–67 (2010). The difference between that proposal and this is the expressed purpose of UIDAI, which is to provide for India’s poor.

209. See Daniel J. Steinbeck, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 Fla. L. Rev. 697, 724 (2004). The prospect of mass checkpoints around sensitive areas, easily used both for pedestrians and in traffic stops, is one concern among many that arises when the question of a national ID card arises in America.

210. Ramakumar, *The Unique ID Project in India: A Skeptical Note*, *supra* note 208, at 157.

211. *Id.* (noting that such ID cards were instrumental in the Rwandan genocide of 1995). These concerns should be somewhat alleviated by the fact that religion, caste, language, and income will not be recorded. Ramanathan, *A Unique Identity Bill*, *supra* note 39, at 10.

212. See Ramakumar, *supra* note 208, at 157–58.

213. *Id.*

214. *Id.* at 158. This is likely to change because of the SCOF report.

215. Fear is heightened because the head of the project is not a lifelong, humble government servant, but rather Nandan Nilekani, a billionaire ex-businessman who has a professed interest in technology. *Id.* at 160. For more about Mr. Nilekani, see Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

faith placed in a biometric system that could malfunction and misidentify individuals, or confuse their identities.²¹⁶ Additionally, the fact that fingerprints can change over time, particularly for people who engage in manual labor for a living, like many of the rural Indians who will benefit from UIDAI, can make fingerprint data accuracy more of a concern.²¹⁷ It is also worth noting that China recently dropped its own plans to issue ID cards and take biometric information from its citizens after determining that the technology was likely to result in too many misidentifications when faced with a population as large as China's²¹⁸—a concern that should be equally important in India given its own large population. And because national ID cards are often proposed with the goal of maintaining national security, they are seen as inherently tied to surveillance and policing.²¹⁹

There is also concern that UIDAI will be able to form “bridges” between different groups that already hold information about an individual.²²⁰ This is termed “convergence.”²²¹ The fear is that the collection of one's number by different businesses or government programs will result in each of those entities having information about that individual's unrelated activities in which he has used the ID number. For instance, if a person provided their identification number to a hospital and then was later required to provide their identification number to a prospective employer, convergence would occur if both the potential employer was then able to view the person's private hospital information and the hospital could access their professional information. In this way, compartmentalization of personal information disappears, and every entity using the ID

216. Ramakumar, *The Unique ID Project in India: A Skeptical Note*, *supra* note 208, at 157.

217. *Id.* But see Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32. It is true that the biometric system is not infallible. But with a combination of fingerprint scanning, which alone correctly IDs someone about 95% of the time, and iris scanning, correct identification rates reach 99%.

218. Ramakumar, *The Unique ID Project in India: A Skeptical Note*, *supra* note 208, at 161.

219. David Lyon, *National IDs in a Global World: Surveillance, Security, and Citizenship*, 42 CASE W. RES. J. INT'L L. 607, 607 (2010).

220. Ramanathan, *A Unique Identity Bill*, *supra* note 39, at 11–12.

221. *Id.* at 11.

number has access to a wealth of an individual's personal data.²²²

Given these legitimate fears, the Indian government should take serious action to make sure that the immense good the project can work is not undone by popular unrest regarding the administration of the program. It should also do so to ease the privacy concerns of those who work in the human rights field, and those observers who find the very notion of a national identification card suspect. Paramount among possible actions is to enact a national law and enforcement regime to give an air of seriousness to the lip service that has thus far been paid to privacy.

In taking cues from the EU Directive, the Indian government should include in its national privacy law a prohibition on the collection of information regarding race or caste.²²³ Information about caste or race will not serve the core purposes of the AADHAAR program, as it will not help to identify individuals any more certainly than the biometric information already will.²²⁴ Importantly, information about race or caste is not relevant to accessing bank accounts, subsidized groceries, or the many other programs that AADHAAR hopes to facilitate. If India is to take seriously its abolishment of the caste system²²⁵ and its commitment to include the poor in its economy,²²⁶ collecting information about caste as part of information linked to an individual's ID card has no place. The current rules allowing local officials to ask AADHAAR ID recipients about race or

222. As illustrated by the joke above at note 39. *Id.* UIDAI's silence on many of these issues adds to the concerns of academics like Ramakumar. A detailed discussion of how the technology will be utilized would help alleviate fears. See, e.g., Ramakumar, *The Unique ID Project in India: A Skeptical Note*, *supra* note 208, at 161 (commenting on the vagueness of the privacy protections in the UIDAI proposals). It is not clear that average Indians, especially poor rural ones, share these data privacy concerns as notions of, for instance, identity theft are foreign to people who do not have credit cards or access the Internet. See Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

223. See Directive 1995/46, *supra* note 156, art. 8. India would be free to include similar exceptions to this rule, as the EU has done.

224. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

225. INDIA CONST. art. 17, *supra* note 5 (particularly doing away with the caste system designation of "untouchability").

226. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

caste should be tightened as part of the privacy law, and only allowed insofar as absolutely necessary to accomplish AADHAAR's goals, if at all.

Next, the privacy law should, like the EU Directive, explicitly include provisions for judicial review of citizen complaints.²²⁷ The judiciary would serve as a sort of third party "enforcer" to ensure that the government administrators of AADHAAR are accountable to those people whom it is meant to protect. Like a European citizen,²²⁸ an Indian who felt he had been damaged by AADHAAR's improper use of his personal information could bring a claim for damages. The threat of lawsuits resulting from improper use of personal data would incentivize UIDAI to take care that it used the collected information only for its intended purposes. Because there is already a very active judicial review process in India,²²⁹ this type of regulation is one that fits the Indian regulatory culture²³⁰ and would likely garner support.

When Indians go to sign up for AADHAAR, they should be told exactly the intended purpose and usage of their personal information. A national data privacy law must mandate that the government clearly explain to individuals (1) who will have access to the information, (2) the intended use of that information, and (3) what rights of access to that information they maintain.²³¹ Doing so will alleviate confusion and make it clear to ID recipients both exactly how AADHAAR will help them and exactly who is able to access their information in order to help them.²³² Such a provision will instill confidence in recipients and encourage them to use their IDs to maximize their benefits, confident that their information will not be used in ways that will harm them.

227. See Directive 1995/46, *supra* note 156, art. 22.

228. *Id.*

229. Basu, *supra* note 55, at 79. However, because many of the participants are quite poor, they would likely be without legal resources. This does not necessarily remove the incentive power of a judicial remedy, however. AADHAAR applies to all citizens, not only the poor, and at least some of them will have the resources to bring suits.

230. *Id.*

231. See Directive 1995/46, *supra* note 156, art. 10.

232. It is possible that this will add a few minutes to the current ten minute AADHAAR sign-up process. Beiser, *Massive Biometric Project Gives Millions of Indians an ID*, *supra* note 32.

Finally, the Indian privacy law must also include mechanisms by which individuals can object to the uses being made of their personal information.²³³ Citizens with legitimate, compelling reasons should be able to quickly indicate that they do not agree with their information being disseminated for certain purposes.²³⁴ This provision would tie in with the provision mandating disclosure to recipients of the intended use of their information, because when the use of the data exceeds that disclosed scope, a citizen will have a cause for complaint. This provision will further serve as a check on AADHAAR's ability to misappropriate personal information, because the ability to object will create administrative costs for UIDAI and create political pressures to ensure that personal data is being used only for the purposes intended.

CONCLUSION

In order to live up to its title of the world's largest democracy, India must value the dignity and identity of even the poorest of its 1.2 billion citizens. In creating the AADHAAR system, the country has shown that it takes the plight of its poor, many of whom live in the most hopeless circumstances, seriously. It also demonstrates that the highest levels of federal government are focused on reigning in the rampant corruption and graft harming the people of India. But in order to maintain its democratic ideals, India must ensure that the massive amount of information it collects through AADHAAR is used only for the limited purposes for which it is collected.

Federal legislative solutions are the most effective way to lend credence to the program. They will create national standards that will make it easier for the very disparate governments of the different states of India to administer the program, and ensure that rural and urban, rich and poor, are treated alike as to how the government uses their information. A law passed with the Parliament's seal of approval will create an air of legitimacy around a project that has thus far been viewed as an executive enactment with little appropriate oversight.

Creating rules for data sharing, and enforcement mechanisms for realizing those rules, will give average Indians a

233. See Directive 1995/46, *supra* note 156, at art. 14.

234. *Id.*

sense of control and will incentivize them to take part in AADHAAR. National privacy laws modeled particularly on the EU Directive will ease one of SCOF's major concerns: that the data collected through AADHAAR will not be kept private or properly protected. Taking such precautions will, in turn, make it more likely that the Parliament will approve the program, and therefore more likely that the hundreds of millions of Indian citizens who could benefit from the program will have a chance to access banks, credit, and technology, and thus be better equipped to function in the modern economy.

*Caroline E. McKenna**

* B.A. Pennsylvania State University, Schreyer Honors College (2009); J.D. Brooklyn Law School (Expected 2013); President of the Brooklyn Law School Moot Court Honor Society. I am grateful to my parents Patrick and Kathleen, my sisters Siobhan and Madeline, and Jeremi Roux for their love and patience. I am grateful also to the staff of the *Brooklyn Journal of International Law* for their efforts in the publication of this Note. All errors and omissions are my own.