# THE RIGHT TO PRIVACY IN THE ERA OF SMART GOVERNANCE: CONCERNS RAISED BY THE INTRODUCTION OF BIOMETRIC-ENABLED NATIONAL ID CARDS IN INDIA

*Sheetal Asrani-Dann*[*]

> Once a civilization has made the distinction between the "outer" and the "inner" man, between the life of the soul and the life of the body, between the spiritual and the material, between the sacred and the profane, between rights inherent and inalienable, and rights that are in the power of the government to give and take away, between public and private, between society and solitude, it becomes impossible to avoid the idea of privacy by whatever name it may be called – the idea of a private sphere in which man may become and remain himself.
>
> - Samuel Warren and Louis Brandeis:
> *4 Harvard Law Review 193 (1890).*

## Introduction

WHILE THE right to privacy has many dimensions, the main concerns of the author in this paper are the right to privacy of personal data and right to territorial privacy. In Part I, the foundations of the concept of privacy in two Western democracies, namely, Germany and the US, and the framework of legal protection it enjoys, have been examined. This has been compared with the right of privacy as understood and defined by the courts in India. In Part II, the proposal for a biometric National ID Card in India has been discussed, and then the nature of objections levelled against nationwide identity systems in general has been examined. In Part III, some fundamentals of the working of biometric technology have been explained and the serious privacy implications of the adoption of a biometric enabled ID card have been described. Even assuming that the privacy risks related to biometric ID cards should be disregarded or are outweighed by the compelling public interest in national security, the claims relating to the effectiveness of

* Legal Associate, The World Bank; B.A.L., LL.B. (Bangalore University Law College), LL.M. (Harvard Law School).

the technology are entirely unsubstantiated. In Part IV, a critical evaluation of the proposal for a biometric National ID Card in India, from a procedural and substantive standpoint, against the backdrop of discussions in the two previous parts has been made. Finally, in Part V, the available policy alternatives and possible legal safeguards and a model for a data privacy law in India have been proposed.

## I The Right to Privacy

### (a) Privacy as conceived in the West

In the 1890s, Louis Brandeis J articulated a concept of privacy that argued that it was the individual's *right to be let alone*. This article, wherein Brandeis J urged that privacy was the most cherished of freedoms in a democracy, profoundly shaped the development of the law of 'privacy'.[1] However, the philosophical foundations of the right to privacy in the US and Germany – to take as examples two countries in which privacy concepts are relatively advanced – are rooted in a profound distrust of the state. In the US, the witchunts and anti-communist hysteria of the McCarthy era led to great excesses including widespread surveillance and government repression of a wide array of citizens engaging in completely lawful activity. Likewise, the German *Gestapo,* or secret state police created under the *Third Reich* enjoyed unrestricted authority for surveiling and rounding up 'subversive elements' considered a threat to the German state. Thus, both in the US and in Germany, there are historic and political reasons for a strong privacy consciousness, which grew out of mass abuses committed by state agencies like the FBI and the *Gestapo*.

It is difficult to define privacy in strictly legal terms. It's meaning has varied with the times, the historical context, the state of culture and the prevailing judicial philosophy.[2] The development of sophisticated technology going as far back as the invention of the telephone and the telegraph, and more recently expressed by computers, wiretap devices and electronic surveillance techniques, has led to a conceptual shift

1. Samuel Warren and Louis Brandeis, "The Right to Privacy", 4 *Harvard Law Review* 193-220 (1890). The motivation for this seminal article was the growing concern of these two Bostonian lawyers over the rapid growth of communications and imaging technology – instantantaneous photography and newspapers – invading the sacred precincts of private life. See Albert J. Marcella Jr. and Carol Stuki (ed.), *Privacy Handbook: Guidelines, exposures, policy implementation and international issues*, 302 (2003). See also Daniel J. Solove and Marc Rotenberg, *Information Privacy Law*, 3-16 (2003).

2. Gross Hyman, *Privacy – Its Legal Protection* (Introduction to the 2nd ed.) ix-x (1976).

from a physical and property-based common law notion of privacy, to a personal liberty basis understanding of the right. In the US, this conceptual shift also forced a re-examination and re-interpretation of the Constitution, especially Fourth Amendment protections.[3] The fundamental issues of personal freedom against state interest in regulating individual behaviour form the consistent theme in privacy cases. Privacy may thus be described as the interest that individuals have in sustaining a 'personal space' free from interference by other persons or organizations. In a free society, the balancing of privacy claims of the individual and the societal interest sought to be protected by the state results in a dynamic tension. Whether the specific question involves freedom of speech, the right to have an abortion, or to wear one's hair at any desired length, there is usually a question of whether a compelling public interest should prevail over personal choice, or whether personal liberties should control over an asserted state interest.

Drilling down to a deeper level, the right to privacy has several dimensions: it encompasses the privacy of person,[4] privacy of personal communications,[5] territorial privacy[6] and privacy of personal data.[7] The adoption of biometric National ID Cards has very serious implications for territorial privacy and privacy of personal data. It is these two aspects of privacy that will be the focus of this paper.

*Privacy as a legal right in Germany*

While the German Constitution does not create a general right of privacy, three of its provisions do, however, protect privacy interests.

3. *Id.* at 90-95. The US Supreme Court recognized that the Fourth Amendment's proscription against unwarranted search and seizure protects not only against physical intrusion on a man's premises, but rather any intrusion without proper authority, physical or otherwise. See *infra* note *24*, *Katz* v. *US*, 386 US 954 (1967).

4. Bodily privacy or privacy of person concerns issues affecting the integrity of the individual's body, including compulsory sterilization, immunization and testing; compulsory provision of body fluids, etc.

5. Communicational privacy implies that individuals have an interest in being able to communicate using various media, without the monitoring of their communications by other persons or organizations.

6. Territorial privacy concerns the setting of limits on intrusion into domestic and other environments, such as the workplace or public spaces. It includes searches, video surveillance and ID checks.

7. Data privacy connotes that personal information should not be automatically available to other persons and organizations, and that, even when another party possesses data, the individual must be able to exercise a substantial degree of control over such data's use and disclosure. Data privacy relates to the protection of all kinds of information, especially sensitive data like political activities, religious affiliations, etc.

The first is article 2, which guarantees the right to the free development of personality.[8] The second is article 10, which protects the privacy of posts and telecommunications. [9] The third, finally, is the guarantee of the inviolability of the home under article 13.[10]

The year 1983 marked a watershed moment in the privacy jurisprudence of the Federal Republic of Germany. It was the year in which the German Federal Constitutional Court, in a remarkable display of judicial activism, suspended the execution of a census under the Federal Census Act of 1983 pending a decision on the Act's constitutional validity.[11] In what was to become a landmark decision,[12] the constitutional court formally acknowledged an individual's *right of informational self-determination* that derived from the textual authority of Articles 1(1) and 2(1) of the German Constitution, which make human dignity and personality inviolable.

In the court's evolving human dignity jurisprudence, the human person was seen as more than the sum of his parts. Rather, he is a spiritual-moral being. The state, therefore, cannot inventory the individual with respect to every aspect of his being without threatening his personal autonomy. The standard primarily applied by the court to carve out an area of inviolable human interiority was the general right to the free development of one's personality protected in article 2(1), in conjunction with article 1 of the Constitution, which protects human dignity.[13] The personality right includes the authority of the individual to decide for himself, when and within what limits facts about his personal life shall be disclosed in his social environment. Without such decisional authority, an individual's right to act freely without being influenced by others is

8. German Constitution, art 2 states: "(1) Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law. (2) Every person shall have the right to life and to physical integrity. The liberty of the individual shall be inviolable. These rights may be interfered with only pursuant to a law."

9. For the text of art 10 of the German Constitution, see http://www.bundestag.de/htdocs_e/info/gg.pdf

10. For the text of art 13 of the German Constitution, see *ibid.*

11. The Census Act provided for the collection of comprehensive data on the Federal Republic's demographic and social structure. In addition to a total population count and the collection of basic personal information (*e.g.,* name, address, sex, marital status, *etc*.), the Act required citizens to fill out detailed questionnaires relating to their sources of income, occupation, supplementary employment, educational background, hours of work, mode of transportation to and from work and related matters. Sections of the statute provided for the transmission of the statistical data to local governments for purposes of regional planning, surveying, environmental protection and redrawing election districts.

12. *Census Injunction Case*, 64 BVerfGE 67 (1983).

13. For the text of art 1 of the German Constitution, see *supra* note 9.

crucially inhibited. The psychological pressure of public awareness will make him avoid engaging in certain kinds of behavior so as not to attract attention.[14] This would not only impair his chances of development, but would also damage the common good, because self-determination is an elementary functional condition of a free democratic community, based on its citizen's capacity to act and to participate. The court, moreover, recognized that the individual's decisional authority needs special protection in view of the present and prospective conditions of automatic data processing by which the possibilities of acquiring, storing and retrieving personal information have increased to a degree hitherto unknown.[15] With remarkable prescience, Ernst Benda CJ has noted: "Today, man's dignity is not endangered by totalitarian tools of suppression, but rather by the potential invasion of an ever-present welfare state into almost all aspects of private life." [16]

In a momentous decision, the constitutional court struck down the sections of the census law empowering the combination of statistical data and a personal registry, which could lead to the identification of persons and violate the core of the personality right. While most of the Act's provisions were sustained, the court stressed the need to close all loopholes in the census law, which might lead to abuses in the collection, storage, use and transfer of personal data.[17]

Germany has the distinction not only of having a well founded 'right of informational self-determination', but also of being a pioneer in the field of data privacy legislation. Germany today has one of the

---

14. For instance, if an individual expects that the state will officially register his attendance at a meeting, and believes personal risks might result from this, he may refrain from exercising his right of association guaranteed under the German Constitution (arts 8 and 9). See generally, Donald P. Kommers, *The Constitutional Jurisprudence of the Federal Republic of Germany* 332-36 (1st ed.1989).

15. From the standpoint of human autonomy, the court feared that information gathering would threaten human liberty, making it easier to control individuals, either by manipulation or outright coercion as the government seeks desired norms of behavior. This carries the specter of big brother, as predicted by George Orwell in his book *1984*, ironically the date of the *Census Act* decision. From the Kantian perspective, information gathering carries the danger of converting human beings into mere objects of statistical survey, depersonalizing the human element. See Edward J. Eberle, *Dignity and Liberty: Constitutional Visions in Germany and the United States*, 87-92 (2002).

16. "Fundamental Rights: A Comparative Analysis" (Lecture presented at the Center for Contemporary German Studies, Johns Hopkins University, Washington, D.C., 23.9. 1987, 6, as quoted in Kommers, *supra* note 14 at 336.

17. The court noted that the right of informational self-determination might be limited for reasons of compelling public interest. Balancing the individual right against the legitimacy of a general census for social planning, the court directed the legislature to specify the purposes and conditions of data gathering and adopt organizational and procedural safeguards to protect individual privacy.

strictest data protection laws in the European Union. In fact, the world's first data protection law was passed in the German state of Hesse in 1970. In 1977, a Federal Data Protection Law followed, which was amended in 2002 to conform to the EU Data Protection Directive.[18] The general purpose of this law is "to protect the individual against violations of his personal rights by handling person-related data." The law covers collection, processing and use of personal data collected by public federal and state authorities (where there is no state regulation), and by non-public offices, if they process and use data for commercial or professional aims. The implementation of the Federal Data Protection Act is supervised by an independent federal agency called the Federal Data Protection Commission. The commission's chief duties include receiving and investigating complaints, as well as submitting recommendations to parliament and other governmental bodies.[19]

*Privacy as a legal right in the US*

The situation is slightly different in the US. The 'right to privacy' is not explicitly mentioned in the US Constitution. However, the US Supreme Court has ruled that several of the Bill of Rights' guarantees protect the privacy interest and create a *penumbra* or *zone of privacy*. *Griswold* v. *Connecticut*[20] was one of the earliest privacy cases before the US Supreme Court involving a challenge to the constitutionality of a state law forbidding the use of contraceptives. In this historic case, the court found that even if the right to privacy is not expressly mentioned in the Constitution, it emanates from the Fourth Amendment's ban on unreasonable searches,[21] as well as the protections under the First, Third, Fifth and Ninth Amendments.[22] Collectively, these amendments establish a zone in which privacy is protected from governmental intrusion.

While most decisions have dealt with the right to privacy predominantly in the context of marriage, abortion, contraception, family

18. Federal Act on Data Protection, 14.1.2003 (*Bundesgesetzblatt*, Part I, No 3, 66. Jan. 2003) available at http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg03.htm.

19. A description of the duties of the Federal Data Protection Commissioner is available at http://www.bfd.bund.de/information/datprotec_en.html.

20. 381 US 479 (1965). The impugned statute was ultimately struck down by the Court.

21. The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."

22. For the text of the Bill of Rights, see http://www.house.gov/Constitution/Amend.html. See also Solove and Rotenberg, *supra* note 1, *Constitutional Law Roots of Privacy*, 20-21.

relationships, child rearing and education,[23] the court has also articulated a right to privacy against government surveillance in an area where a person has a "reasonable expectation of privacy". [24] It is impossible to discuss privacy in America without referring to the *Watergate* scandal. *Watergate* unveiled events in which the US government itself violated the most basic prohibitions against invasion of privacy by authorizing bugging, wiretapping and illegal entry. These were later sought to be justified by citing 'national security' as an overriding state interest. The years since *Watergate* have seen more judicial activity in the area of enlarging the concept of privacy to include legal actions involving electronic surveillance, databanks, credit reporting, and other related concerns. Interestingly, however, there is no independent privacy oversight agency in the US, and no comprehensive privacy law for the private sector.[25] The US has taken a sectoral approach to privacy regulation so that a patchwork of federal laws covers some specific categories of personal information like financial records, health information, credit reports, video rentals, etc.[26]

---

23. See *e.g.*, *Eisenstadt* v. *Baird,* 405 US 438 (1972); *Roe* v. *Wade,* 410 US 113 (1973); *Paul* v. *Davis,* 424 US 714 (1976). Scholars have used the term 'decisional privacy' to describe the interest protected by the court in cases relating to birth control, procreation, abortion, child-rearing, sexual intimacy, and so on which concern the freedom to make decisions about one's body and family. Decisional privacy is at the center of a series of Supreme Court cases often referred to as "substantive due process". It is contrasted with 'informational privacy', which concerns the collection, use and disclosure of personal information.

24. The court has held that the Fourth Amendment "protects people, not places" and said the police must obtain a warrant even when a search takes place in a public payphone on a public street, in *Katz* v. *US,* 386 US 954 (1967). The Court has recognized a right of anonymity in *McIntyre* v. *Ohio Elections Commission,* 514 US 334 (1995) and the right of political groups to prevent disclosure of their members' names to government agencies in *NAACP* v. *Alabama,* 357 US 449 (1958).

25. The US approach is not a reluctance to confront privacy issues, but more a product of differing perceptions amongst Americans regarding the role of government. Americans mistrust big brother and any regulation that touches their personal lives – evidence that normative values and expectations of privacy are highly context-sensitive. In 1977, the US Privacy Protection Study Commission, an independent study group, rejected the notion of an omnibus privacy statute establishing authority to regulate the flow of personal data, concluding that the danger of government control, the greater influence of economic incentives on the private sector to adopt voluntary privacy guidelines, and the difficulty in legislating a single standard for widely-varying information-keeping practices all argued for rejecting any attempt to develop a comprehensive regulatory scheme of protection. See Marcella and Stuki, *supra* note 1 at 302-04.

26. Today, there are roughly 600 federal and state laws that deal with the handling of personally identifiable information. See Privacy International, *Privacy and Human Rights* (2003) International Survey ('PI Survey') available at http://www.privacyinternational.org/survey/phr2003/countries/unitedstates.htm

Records held by US government agencies are, however, protected under the Privacy Act of 1974.[27] In practice, the Act's effectiveness is significantly weakened by administrative interpretations of a provision allowing for disclosure of personal information for a "routine use" compatible with the purpose for which the information was originally collected. In recent years, limits on the use of the social security number (SSN) have also been undercut because Congress has approved new purposes for the identifier and because the private sector employs the identifier for many purposes with virtually no safeguards for the individual.

The closest American constitutional case, in a substantive way, to the German concept of informational self-determination is *Whalen* v. *Roe*.[28] Decided seven years before the *Census case* in Germany, *Whalen* involved a challenge to a statute empowering the government to accumulate vast amounts of information on prescription drug usage in centralized computer banks. The US Supreme Court found that the privacy interest of the prescription drug users in not having the state gather information on their drug usage was outweighed by the state's interest in gathering this data.[29] While textually, the US Constitution seems as illuminative of the right of privacy[30] as the German Constitution, as a matter of comparative law, it is worth observing that the German Constitutional Court has addressed this aspect of the computer age in a more rights-protective manner than the US Supreme Court.[31]

In sum, whereas both in Germany and the US, the foundations of the notion of privacy lie in a deep distrust of government power, both

---

27. Privacy Act, Pub. L. No. 93-579 (1974), codified at 5 USC § 552a, text available at http://www.usdoj.gov/04foia/04_7_1.html

28. 429 US 589 (1977).

29. See Schachter, *Informational and Decisional Privacy*, 288-89 (2003) "The scope of the informational privacy protection delimited in *Whalen* has been regarded as inchoate, or, perhaps as in a nascent stage."

30. The First Amendment plausibly bestows certain rights to knowledge of how information, especially personal information, is to be gathered or used. The Fourth Amendment confers certain rights of privacy against discovery of personal information, especially that over which one has a 'reasonable expectation' of privacy. The due process clause protects against arbitrary intrusion into matters of personal security and liberty. Human dignity too has been a theme of the Bill of Rights, including especially its cognates of self-determination and autonomy. Together, these rights would seem to convey a certain zone of privacy, which, it might be argued, covers informational privacy. Yet, for various reasons, American law has not developed along these lines. See Eberle, *supra* note 15 at 93-94, 110.

31. For a probing of the divergences in German and American law over the idea of inner freedom most notably manifested in the concept of informational self-determination, see *id.* at 110.

countries differ in their respective approaches to privacy protection – a comprehensive law in Germany versus a sectoral and self-regulatory approach in the US.[32] Additionally, in Germany federal law provides the framework of an independent oversight agency in the form of a Data Protection Commission, but there is no comparable institution in the US. However, what unites both systems is their recognition of the significance of the right and the value of protecting it, especially against governmental intrusion. While the right of privacy has many components, it is the aspects of territorial privacy and data privacy which are seriously implicated in the context of the biometric National ID project.

**(b) Tracing the contours of the right to privacy in India**

In marked contrast to the two systems described above, in India, there is to date no comprehensive or sectoral privacy legislation, or any independent oversight agency. Neither does the Constitution of India expressly recognize the right to privacy.[33] In fact, curiously enough, some scholars have even questioned whether privacy is, after all, a value somewhat alien to Indian culture.[34] While one of the main rationales for the adoption of comprehensive privacy laws in many countries, especially in Central Europe and South America, has been to remedy privacy violations that occurred in past authoritarian regimes, interestingly, the recent push for data protection legislation in India is

32. The omnibus approach adopted by European countries establishes privacy standards independent of technological and market considerations. By establishing broad standards, Europeans ensure that privacy is considered in the planning stages of new technology or activities, rather than at a less efficient and less effective time in the process. The US is rarely, if ever, able to anticipate technology with privacy laws or policies. See Robert M. Gellman, "Can Privacy be regulated effectively on a national level? Thoughts on the Possible Need for International Privacy Rules", 41 *Vill. L. Rev.* 129, 146-47 (1996).

33. During the Constituent Assembly debates, K.S. Karimuddin moved an Amendment on the lines of the US Constitution. However, as B.R. Ambedkar gave it only reserved support, it did not secure the incorporation of the right to privacy in the Constitution. See VII *Constituent Assembly Debates*, 794 and 976.

34. See Upendra Baxi, (ed.), *Introduction to K.K. Mathew on Democracy, Equality and Freedom, The New Domain of Personal Liberty: Privacy*, 73-75 (1978). Baxi has expressed doubts about the evolution of privacy as a value in human relations in India. Everyday experiences in the Indian setting (from the manifestation of good neighborliness through constant surveillance by next-door neighbours, to unabated curiosity at other people's illness or personal vicissitudes) suggests otherwise. See *also* S.K. Sharma, *Privacy Law: A Comparative Study*, 344 (1994) commenting on the problems in the development of the law of privacy in India, and Arnold Simmel, *Privacy, International Encyclopedia of Social Sciences*, 481, for an examination of the cultural, socio-historic and situational differences in the understanding of the notion of privacy.

business-driven. The National Association of Software and Service Companies (NASSCOM) has been urging the Indian government to pass a data privacy law for some years now.[35] The absence of such legislation has proved to be a handicap for European and American companies seeking to outsource their business processes to Indian companies. This is because EU and US laws mandate stringent privacy safeguards to protect the transborder flow of personal data.[36]

While the right to privacy is not explicitly enumerated in the Indian Constitution, historically, judicial pronouncements of the Supreme Court of India provide the basic resources for both the purposes and the content of the right to privacy. It took a quarter of a century of the functioning of the Constitution before the right to privacy received the status of a constitutional right. The main issues relating to the recognition of privacy have confronted the state power of searches and surveillance. In the first case wherein the right to privacy was invoked in the context of search and seizure,[37] the Indian Supreme Court adopted a narrow and formalistic approach, pointing to the absence of a specific constitutional provision analogous to the Fourth Amendment of the US Constitution, to protect the right of privacy of Indians from unlawful searches.[38] This disappointing decision was followed nearly a decade later by *Kharak Singh* v. *State of U.P.*,[39] wherein the right to privacy was again invoked to challenge police surveillance of an accused person. In a pedantic fashion, the court held that as privacy is not a guaranteed fundamental right under the Constitution, an attempt to ascertain the movements of a person, while it invades his privacy, does not infringe any fundamental right. On this reasoning, the impugned provisions empowering police 'watches' were upheld. The majority rejected the petitioner's plea that freedom of movement under article 19(1)(d) connotes a wider freedom transcending mere physical restraints and includes psychological inhibitions caused by surveillance. In a forceful and oft-cited dissent,

35. The aim is to allow India to be officially designated by the European Commission as a country that can be assumed to ensure an adequate level of protection, as required under the EU Data Protection Directive (art 25). This would clear the path for any data processing operations involving personal data originating in the EU to be carried out by companies established in India, as they would have to meet the same requirements as EU-based companies. See *infra* note 124 for the text of the directive.

36. See generally, Eduardo Ustaran, *Data Protection Update: Destination India*, October 2003 at 1-3.

37. *M.P. Sharma* v. *Satish Chandra*, (1954) SCR 1077.

38. For a critique of *M.P. Sharma*, see Anirudh Prasad, "New Dimensions of the Right to Privacy under the Indian Constitution", in Verinder Grover (ed.), *The Indian Constitution*, 160-61 (1989).

39. AIR 1963 SC 1295.

two judges of the court conceded that while privacy is not an express fundamental right, it is an essential ingredient of personal liberty under article 21, which reads: "No person shall be deprived of his life or personal liberty except according to procedure established by law." Taking a more holistic view of the scheme of protection afforded by part III, the minority found that all acts of surveillance under the impugned Regulations offended articles 21 and 19(1)(d), as movement under the shroud of police surveillance cannot be described as free movement within the meaning of the Constitution.

Finally, in 1975 came a decision with far-reaching constitutional implications. In *Govind* v. *State of M.P.,*[40] the Supreme Court again confronted the question of the constitutional validity of police surveillance, challenged by the petitioner as violating his right to privacy. Neatly sidestepping the ratio of the larger benches in *Sharma* and *Kharak Singh*, the three-judge bench unanimously gave the right to privacy a new lease of life.[41] Tracing the origin of the right in the presumed intention of the framers of the Constitution, the court, speaking through Mathew J. said:[42]

> There can be no doubt that the makers of our Constitution wanted to ensure conditions favorable to the pursuit of happiness. They certainly realized, as Brandeis, J. said in his dissent in Olmstead v. US, the significance of man's spiritual nature, of his feelings and his intellect […]. They sought to protect [individuals] in their beliefs, their thoughts, their emotions and their sensations. Therefore they must be deemed to have conferred upon the individual as against the government a sphere where he should be let alone – the most comprehensive of rights and the right most valued by civilized men.

The Supreme Court accepted that the unifying principle underlying the concept of privacy is the assertion that the fundamental nature of the right is implicit in the concept of ordered liberty.[43] Fortified by recent American decisions,[44] the court laid the basis for the doctrine that a

---

40. AIR 1975 SC 1378.

41. F.S. Nariman, "The Right to be let alone – A Fundamental Right", 17 *The Indian Advocate*, 76-83 at 81 (1977).

42. Mathew J. quoting from *Olmstead* v. *US*, 277 US 438 at 478 (1928).

43. "Rights and freedoms of citizens are set forth in the Constitution in order to guarantee that the individual, his personality and those things stamped with his personality shall be free from official interference except where a reasonable basis for intrusion exists. In this sense, many of the fundamental rights of citizens can be described as contributing to the right to privacy," Mathew, J. in *Govind.*

44. *Griswold* v. *Connecticut*, 381 US 479 (1965); *Roe* v. *Wade*, 410 US 113 (1973).

*penumbra* or *zone of privacy* is created by the various guarantees in part III of the Indian Constitution. The right to personal liberty (article 21), the right to move freely throughout the territory of India (article 19(1)(d)), and the freedom of speech (article 19(1)(a)) create an independent right of privacy as an emanation from them, which might also be characterized as a fundamental right. The court firmly anchored the right of privacy in constitutional jurisprudence, but noted that it would necessarily have to go through the process of a "case-by-case development". [45] It held that if a claimed right were entitled to protection as a fundamental privacy right, any law infringing it would have to satisfy the test of furthering a compelling state interest.[46] *Govind* has been hailed as an example of judicial creativity at its best, a case wherein the court exercising its constituent power has not only articulated a 'new' right, but also broadly formulated its scope and legitimate constraints.[47]

Writing in 1977, F.S.Nariman commented that the decision in *Govind* would do more than help point the way: it would set the tone.[48] Over the course of the next three decades, the court has established other aspects of the right of privacy. In 1997, the Supreme Court held that telephone tapping by the government under the provisions of the Telegraph Act of 1885, infringes the right to privacy if not resorted to by just, fair and reasonable procedure.[49] The right of privacy would also preclude such questions from being put by employers to female candidates as modesty and self-respect may preclude an answer. [50] In 1994, the Supreme Court decided in the *Auto Shankar* case[51] that every citizen has the right to safeguard his privacy and nothing could be published in areas such as family, marriage, procreation and education, whether truthful or otherwise, without the citizen's consent. Two

45. '*Govind* is anxious to preserve the rich indeterminacy and open texture of the right to privacy, continuing and revitalizing the inspirations of Justice Subha Rao's memorable minority opinion in *Kharak Singh.*' Upendra Baxi, *supra* note 34 at 74-75.

46. Striking a balance between the liberty of the individual and the security of society, the court held in the instant case that domiciliary visits and picketing by the police would be justified *only* in the clearest cases of danger to the community.

47. See Baxi, *supra* note 34.

48. *Supra* note 41 at 83.

49. *People's Union for Civil Liberties (PUCL)* v. *Union of India*, (1997) 1 SCC 301 (para 18). The court laid down guidelines for tapping under the Act, to create adequate privacy safeguards against official abuse.

50. *Meera Mathur* v. *LIC,* AIR 1992 SC 392. In two other cases, Courts have asserted that even 'women of easy virtue' have a right to privacy. See *Re: Ratanmaia* AIR 1962 Mad 31, and *State of Maharashtra* v. *Madhulkar Narain* AIR 1991 SC 207.

51. *R. Rajagopal* v. *State of T.N.,* AIR 1995 SC 264 (para 28).

exceptions to this rule were carved out for material based on public records, and information about public officials' conduct "relevant to the discharge of their duties". Finally, the court has held that while the right to privacy is an essential component of the right to life, it may be restricted for the prevention of crime or disorder, for the protection of health or morals, and to protect the rights and freedom of others.[52]

With a zeal to translate the philosophy of the right to life and personal liberty into a reality, the Supreme Court has recognized privacy as a fundamental right and defined it in cases involving police surveillance, phone tapping, media attention and so on. However, it is clear that the jurisprudence of the court is still evolving. While some facets of privacy have been defined, the Supreme Court has not yet articulated a 'right of informational self-determination' as it exists in Germany. The need for privacy of personal data in public and private databases has not yet been adequately addressed. At the time of legislating on cyber laws for India, Parliament appears to have largely neglected the issue of privacy of personally identifiable information. Section 72 of the Information Technology (IT) Act of 2000,[53] which is the sole provision dealing with the issue, is very narrow in scope. It prescribes a penalty for breach of privacy of any electronic record, but applies only to offences by authorities exercising power under the Act, such as adjudicating officers, certifying authorities, etc. Thus, there exists a huge gap between the privacy needs of individuals and existing legislative protection in India. On the contrary, privacy has been legislatively restricted by provisions in the IT Act of 2000,[54] the Telegraph Act of 1885,[55] the Prevention of

52. *'X'* v. *Hospital 'Z'*, (1998) 8 SCC 296 (para 28). The Court held that the disclosure by doctors of the HIV positive status of their patient to his fiancée did not violate the rule of confidentiality or his right to privacy.

53. For the text of the IT Act, including Section 72, see http://www.mit.gov.in/it-bill.asp

54. S. 69 of the IT Act gives tremendous powers to the Controller of Certifying Authorities to direct the interception of any information transmitted through any computer resource, if he is satisfied that it is necessary or expedient so to do in the interests of the sovereignty or integrity of India, the security of the state, friendly relations with foreign states, public order, or to prevent incitement to the commission of any cognizable offence.

55. Despite numerous phone-tap scandals resulting in the Supreme Court's laying down guidelines for wiretapping, *(supra* note 49) illegal taps by government agencies continue. The mail of many prominent NGOs in Delhi and strife-torn areas continues to be subjected to interception and censorship. See South Asian Human Rights Documentation Center, Alternate Report to the U.N. Human Rights Committee on India's 3rd Periodic Report under art. 40 of the ICCPR, July 1997, available at http://www.hri. ca/partners/sahrdc/alternate/fulltext.shtml.

Terrorism Act of 2002[56] and the proposed Communications Convergence Bill.[57]

Thus far, the whole data protection discourse and the effort to increase privacy standards in India has taken place only in the context of retaining India's huge potential for business process outsourcing. There has not yet been any wider discussion surrounding the privacy implications of the government's collection, retention and use of personal data. For historic and cultural reasons, the motives of the government in handling personal data are not suspect. However, it will be argued in the succeeding parts that in light of the ever-widening powers of the government to gather and use personal data generally, and specifically with reference to the proposed National ID project, a comprehensive privacy law is urgently needed, not only to safeguard India's economic interests, but equally, if not more importantly, to protect the privacy of its citizens against the increasingly Orwellian powers of the government.

## II National ID Systems and their Consequences for the Right to Privacy and other Personal Liberties

The attacks of September 11, 2001, and subsequent events have globally brought fresh urgency to the challenge of providing information security. One proposal that has received attention in many countries as a solution for problems ranging from counter-terrorism and detecting benefit-fraud, to enabling electoral reforms and preventing illegal immigration, is a nationwide identity system.[58] Recent events in India have also pushed the government to consider the introduction of a National ID card. In fact, a pilot project for the issue of National ID cards in certain Indian states has already begun.

---

56. For the text of the Prevention of Terrorism Act of 2002 see http://mha.nic.in/poto-02.htm. The Act (repealed by an Ordinance in Sept 2004) gave law enforcement sweeping powers to intercept communications. While chapter V also created an audit mechanism including a provision for judicial review and parliamentary oversight, the practical effectiveness of such mechanisms remains to be assessed.

57. For the text of the draft bill see http://www.tiaonline.org/policy/regional/asia/conbill.pdf. The bill aims to create a "super regulator," the Communications Commission for India, to oversee voice and data communications. Chapter XIV of the bill has been criticized for allowing law enforcement to intercept any communication under a very low standard.

58. It is suggested that the term 'National ID card' is a bit of a misnomer, in that a card would likely be but one component of a complex nationwide identity system, the core of which would be a database of personal information on the entire population.

### (a) The Indian National ID card proposal and a short background of smart card applications in India

Although India's population has passed the one billion mark, it does not have a national identification document scheme till date.[59] The Indian citizen has a paper-based document known as the ration card, which serves as identification and for claiming certain government benefits, like subsidized provisions at government fair price shops. Voter registration cards that were introduced a few years ago have not yet been made mandatory.[60] Due to the lack of proper ID, India faces the problem of tracking illegal immigrants, counterfeit identification, bogus voting and inaccurate voting rosters during each election.[61] Hence, the government has argued, the introduction of smart card-based National ID documents is natural in such an environment. It is worth noting that 'smart' card-based technologies have already been used in certain projects in India in the last few years.

*Current smart card applications in India*

A 'smart' card is a plastic card with an embedded electronic integrated circuit chip. This chip is 'intelligent' – it can not only store, but also process information – and, therefore, the card is 'smart'. Biometric data may be registered on the chip using a biometric reader.[62]

Smart cards were introduced in India way back in 1990, by companies that offered telephone cards, employee cards and ATM cards. Real growth came in 1995, with the use of smart cards as SIM cards in mobile phones. [63] Smart cards were also successfully used in Mumbai's BEST buses,[64] and are now proposed to be launched by the Uttar Pradesh

59. Passports and photo driver's licences, while they exist, are not universal.

60. Despite the introduction of the Elector's Photo Identity Card, an official document which establishes one's identity as an eligible voter, the Election Commission of India still recognizes up to 16 different documents as valid forms of identification for voting purposes. See Voter ID compulsory for polls, *The Hindu*, 28.4. 2001 available at http://www.hinduonnet.com/thehindu/2001/04/28/stories/0228000o.htm

61. Ration cards, intended to act as an identity document and as proof of citizenship, have recently been the subject of many scams. In many cases, cards are either bogus, or being misused, because they are stollen or 'lent' to someone else. See Banerjee, Do we still need ration cards? *Times of India*, 16.11. 2002.

62. See *infra*.

63. Gaurav Dua, Analyst, Frost & Sullivan, as quoted in *Convergence Plus*, 15.9. 2003.

64. A consortium led by Alittleworld.com has now proposed to launch a multipurpose smart card, with commuter fare collection being the most lucrative application.

government in an experiment in fair price outlets in five districts.[65]

Apart from mobile phones and ration shops, smart cards will soon be used for transport applications as well. In 2002, the Indian government published smart card specifications developed by the National Informatics Center for driver's licences. These specifications – called SCOSTA (Smart Card Operating System for Transport Applications) – are to be adhered to by all states in implementing their card-based driving licence and vehicle registration systems, so as to ensure interoperability between smart cards of various vendors. Gemplus, a leading provider of smart card solutions, has achieved certification for meeting SCOSTA standards and will implement contracts for SCOSTA-compliant cards this year. Although it is primarily intended to be used as a driving licence and vehicle registration card, GemSCOSTA has the capacity for multiple ID applications, such as for National ID purposes.[66]

**National IDs: on the cards**

About the year 2000, the Union Home Affairs Ministry asked Tata Consultancy Services (TCS) whether it would be feasible to check infiltration by constructing an identity system in the border states.[67] TCS claimed it would be possible to achieve a pervasive biometric ID card, not just for the border states, but also for the whole of India. To ensure reliability and comprehensiveness, TCS proposed the creation of a new database independent of existing, poorly-kept transactional records. It further suggested making it an upgraded operation instead of a bureaucratic process with Parliament enacting legislation for the compulsory registration of citizens and foreign residents. [68] After 13.12.2001, the internal security of India became a matter of even greater concern. The attack, coupled with other terrorist activities in different

65. Manjari Mishra, Ration cards to carry advertisements, *Times of India*, 1. 1. 2004. A similar system was installed in Jammu and Kashmir as part of a surveillance and monitoring exercise.

66. GemSCOSTA can carry biometric fingerprints. The memory capacity required for a fingerprint is only 256 bytes per fingerprint, and, therefore, according to Gemplus India's Managing Director, at least two fingerprints may be stored on the card, apart from the other information required for the driver's licence.

67. Rajendra Prabhu, 3rd Smart Card Tech India 2003: From National ID to global citizenry, available at http://www.convergenceplus.com/3rd%20scti%202003.html

68. The TCS report recommended that the whole exercise be made market-friendly, and that the state actually make money by selling information that it gathers about citizens to corporate bodies. See Shuddhabrata Sengupta, "Everyday Surveillance: ID cards, cameras and a database of ditties", in *Sarai Reader 2002: The Cities of Everyday Life*, 297-301 at 298.

parts of India prompted the BJP-led government to issue multipurpose National Identity Cards to about 3.1 million people in select areas of 13 border states. The IT/management lobby has also been pushing the launch of multipurpose biometric cards, ostensibly with the objective of creating a comprehensive, nationwide IT infrastructure to support e-governance initiatives embracing immigration, driver's licences, healthcare, etc.

The first phase of the national ID pilot is to capture biometric fingerprints and personal data for 3.1 million people and set up an electronic registry of citizens. The contract has been awarded to Bharat Electronics Ltd. The next phase will consider the use of smart cards for this national ID pilot. Some work on enhancing the security of SCOSTA to meet with national ID requirements is in progress. Eventually, it is anticipated that the national ID card would be used for multiple government applications.

A project to introduce biometric National ID cards for all Indians has enormous legal, technological and socio-political ramifications. A serious analysis of the substantial and complex range of issues presented by nationwide identity systems is needed before any such system is put into effect. Understanding the goals of such a system is a primary consideration. The first question that will be asked is, do people in India want to move towards an identification regime? Would they be comfortable with the notion of having an identification document on their person at all times? Should this document have biometric identifiers? The crucial point to note is that a positive answer to the first question does not automatically imply an affirmative response to the second. And there is a vast range of choices between having an ID or not having one at all, in terms of what features such an ID could have and what purposes it could serve. But it is critical to understand the implications of the choices before a potentially irreversible move is made.

**(b) Existing national ID systems and their problems**

*Which countries use ID cards?*

Although many countries use some form of identity card, the type of card, its functions and integrity vary enormously. While several countries like Belgium, Greece, Luxembourg, Germany, France, Portugal and Spain have official, compulsory national ID cards, many do not. Amongst the latter are the Nordic countries and Sweden, and common law countries like the US, Canada, New Zealand, Australia and Ireland, which have historically rejected attempts to create National ID Cards. Many countries that do not have a national universal card, have a sectoral/ specific-purpose card for health or social security (in Australia, the Medicare Card, in the US, the Social Security Number).

*What are the main types of ID systems in use?*

Broadly expressed, there are two different forms:

*(1) Registration systems:* The majority of ID systems have a support register containing parallel information to that on the card. In most countries, this register is maintained by a regional or municipal authority rather than as a national system. Germany and France are examples of such a system, where there is no national ID card register.

*(2) Integrated systems:* On the other hand, most card systems established in the last decade are integrated systems, designed to form the basis of general government administration. The card number is, in effect, a national registration number used as a common identifier by many government agencies. In such systems – for e.g. in Spain, Thailand and Singapore – the ID card becomes merely one visible component of a much larger system, fusing a service technology and a means of identification.

*What are the objections against identification systems?*

In several countries, recent proposals for identification systems, particularly multipurpose identification systems, have faced stiff public resistance[69], and been successfully challenged on constitutional privacy grounds.[70] Opposition to the cards combined with the high economic cost and implementation problems have, in some cases, led to their withdrawal. In Australia and New Zealand, proposals to implement a universal identifier as part of a crackdown on tax evasion and welfare fraud led to massive protests in 1987, resulting in the near-collapse of the government. In the US, concern for civil liberties and the historic association of ID cards with repressive regimes has discouraged movement toward a governmentally sanctioned nationwide identity system. Recent proposals to convert the state driver's licence into a national ID system have been stalled because of stiff resistance from both conservative and liberal leaders in Congress. Six specific problems associated with National ID schemes are discussed below:

---

69. National ID systems have been strongly protested against in Japan, Taiwan and South Korea. See EPIC Survey Raises Questions about National ID Cards, Press Release dated 8.10.2003 available at http://www.epic.org/privacy/id-cards/pressrelease10-03.html

70. Recent examples include the Philippines, Hungary and Portugal. See PI Survey, *supra* note 26.

1. *National ID systems have failed to meet stated objectives*

The presumption that a national ID card can improve law enforcement techniques, reduce illegal immigration, diminish fraud, assist national security or improve administrative efficiency is entirely instinctive. There is little, if any, quantifiable evidence in research literature to establish that an ID card system can achieve such goals.[71] ID cards have not stopped car bombing campaigns in Spain, France and Italy, and would have done nothing to stop the September 11 attacks either.[72] On an occasion when the ID card concept was seriously floated in the UK (crime was the issue of the moment), even the Association of Chief Police Officers argued that a card would have little impact on crime[73] and could damage relations between the police and public, especially ethnic minority groups.

2. *National ID systems create more problems*

Millions of people will be severely inconvenienced each year through lost, stolen or damaged cards or - more devastatingly - through failure of the card's computer systems or reading machinery. While the idea of a national ID card might be superficially attractive, many countries have discovered that the technology creates more problems than it solves. Their introduction in recent times has created a range of unforeseen administrative and social complexities. Thailand, which introduced its first ID card in 1989, is still ironing out fundamental problems after all these years. Critics also contend that such cards create a misplaced reliance on a single document, and attract substantially larger investment in corruption and counterfeit activity. Hence there is a fundamental flaw in the notion of an infallible identity card.

---

71. See PI's Submission to the Canadian Parliament on National Identity Cards, 4.10.2003, at http://www.privacyinternational.org/issues/idcard/pi-can-submission-10-03.htm

72. In its report '*Mistaken Identity*', PI has looked at terrorist incidents since 1986 and found that of the 25 countries most affected, 80% already had national identity cards, one-third of which incorporate biometrics. Additionally, it found that in the most high-profile al-Qaida attacks, terrorists either moved across borders using tourist visas (in the case of 9/11), or were already domiciled in the country and equipped with legitimate ID cards (the Madrid train bombings). Based on the actual evidence, the report concluded that the likelihood of an ID card preventing a terrorist attack is virtually zero.

73. There is no evidence suggesting that the use of identity cards by many European countries has led to any appreciable reduction in crime. See 'No Id Cards' available at www.no2id.com

3. *National ID systems conceal hidden agendas*

While the stated justifications for identity schemes vary, there is often an instinctive notion that a card system can be a conduit for 'nation-building' in which cohesion and national identity can be strengthened. In this sense, the card may be an initiative grounded in nationalism. Countries such as Malaysia, China, Singapore and Indonesia have openly promoted National ID Cards as a means of establishing 'national membership'. Race, ethnicity and religion, often the driving-force behind nationwide ID systems,[74] have long been a facilitating factor in allowing certain regimes to readily identify and persecute their victims. To cite an example from recent times, ID cards with ethnic classification instituted in Rwanda by the Belgian colonial government and retained after independence were central in shaping and perpetuating ethnic identity. During the genocide, Rwandan ID cards helped distinguish the *Tutsis* from the *Hutus*, and target persons based on group affiliation. No other factor was more significant in facilitating the speed and magnitude of the 100 days of mass killing in Rwanda.[75]

*4. National ID systems lead to function creep and discrimination*

The inevitable outcome of introducing a high security ID card is that it will become an internal passport, demanded in limitless situations. This is a classic example of "function creep"— the continuous expansion in the use of a system first intended for a limited purpose. Aggravating this situation, in many countries that have adopted a national ID system, people who fail to produce their cards on demand are regarded with suspicion.[76] Identity systems often force 'undesirables'[77] to register with the government or make them subject to routine interrogation, harassment and prejudice by officials.[78] Ethnic minorities, recent

74. *E.g.*, ID cards ('passes') carried by South Africans during the *Apartheid* era mentioned 'race' and were used to restrict free travel and enforce social and political control. See Richard Sobel, "The Degradation of Political Identity Under a National Identification System", 8 *B.U. J. Sci. & Tech. L.* 37, 48 (2002).

75. For a study of how National ID cards with group classifications have contributed to mass eliminationist policies in modern history, see Jim Fussell, "Genocide and Group Classification on National ID Cards", in Watner and McElroy (ed.), *National Identification Systems: Essays in Opposition*, 55-69 (2004).

76. For *e.g.*, in Greece and Argentina, being caught cardless could land a person at the local precinct.

77. This would include the 'floating population' in most cities, consisting of migrant labour like *rickshaw wallas, dhaba wallas, dhobis, maalis*, maids, street vendors, hawkers, etc.

78. The UK High Court addressed this point in 1954 when it outlawed the wartime ID card. See C.H. Rolph, "The English Identity Cards", in *National Identification Systems: Essays in Opposition*, *supra* note 75.

immigrants and socially excluded groups such as the homeless find themselves unfairly singled-out and disadvantaged.

5. *Privacy risks surrounding national ID systems*

Every identity system is made up of a support register containing personal information parallel to that on the ID card. When this information is maintained on a central database, the ID number acts as a common identifier for multiple government agencies. The risks that this poses for individual privacy are monumental. Centralized information is centralized power. A national identifier contained in an ID card enables disparate information about a person scattered in different databanks to be easily linked and analyzed through data mining techniques. This would allow the entries in one set of data to influence other, unrelated parameters. Moreover, multiple-agency access to sensitive data (or multiple-use of the ID card) greatly increases the potential for misuse of personal information (by 'snooping', social sorting and profiling), either through corrupt disclosure, or lapses in security.

6. *National ID systems shift the balance of power from the individual to the state*

Years ago, when an ID card was sought to be introduced in Australia, Michael Kirby J., President of the New South Wales Court of Appeal, warned that the issue would mark a fundamental shift in the balance of power between citizens and the state.[79] At their heart, ID systems invariably pave the way for the convergence of government services and the development of a comprehensive linkage between public and private sector information systems. Such initiatives turn nations into more authoritarian societies.[80] This profound impact is inevitable because the modern ID card is a component of a complex web of technology that fuses the most intimate characteristics of the individual with the machinery of state.[81] In order to give the card the necessary legal gravity,

79. Quoted from Justice Kirby's evidence to the joint select committee on an Australia Card, 1986.

80. See Sobel, *supra* note 74, "The development towards a National ID system fundamentally contradicts what it means to live in an open democratic society, where the government derives its powers from the consent of the governed, and activities such as work, travel and medical care are readily available and treated in ways respectful of privacy. In contrast, authoritarian governments bestow or deny identities and opportunities through identification numbers or documents, intruding into individuals' lives."

81. Davies, Reckless ID card plan will destroy the nation's freedom, *The Telegraph*, 29.9. 2001. See also Clarke, Human Identification in Information Systems, 7 *Information Tech. & People* 6 (1994): Many people are unwilling to submit to the

its introduction is accompanied by a substantial increase in police power. Authorities will, after all, want to demand the card in a wide range of circumstances, and people must be compelled to comply. Government rarely promotes this sobering outcome. Instead, such initiatives are benignly dressed up as "citizen cards" guaranteeing entitlement to benefits and services, and streamlining a person's dealings with the government.

From the above discussion, it is clear that national ID systems have a significant impact on privacy and other personal liberties, making a contemporary ethical and policy analysis of the Indian project obligatory. Given the wide range of technological and logistical challenges, the likely direct and indirect costs and the gravity of the policy issues raised, any proposed nationwide identity system would require strict scrutiny and significant deliberation well in advance of design and deployment.

## III The implications of Multi-purpose Biometric National ID Cards: Why not to Have Them

### (a) How biometric national ID cards are a threat to privacy

There are basically two levels of objection to the deployment of biometric technology in a nationwide identity system. The first layer of critique is that the use of this technology amounts to a wholesale violation of the right to privacy that is not, and cannot, be justified even on grounds of compelling state interest. The second dimension is that even if one buys into the need to sacrifice individual privacy for an overarching 'national interest', the claims made by the industry and government that biometric technology is an effective means of achieving stated goals is clearly unsustainable, unsubstantiated and at best questionable.

*Welcome to the world of biometrics: understanding the basics*

The most fascinating part of the new ID card is its biometric identifier. It is a two hundred year old concept, but until now has been applied mainly in criminal investigations. The little chip on the card that makes all the difference between a 'smart' card and a piece of plastic (or a credit card) can store up to 64KB of data, including biometric data like fingerprints, iris data, DNA pattern analysis, etc.

---

regimen of carrying ID cards, or are unprepared to produce them, on grounds that this reeks of a totalitarian regime, reflects and perpetuates a power relationship that they despise, or carries with it the seeds of discrimination (as reflected by the card's contents). Many also feel it is an insult to human dignity to require them to use a number or a code instead of a name.

Three conventional forms of identification are in use today. The first is something you have, such as a card, key or passport. The second is something you know, such as a password or PIN. The third is something you are, such as a pattern of ridges on a fingertip; or something you do, such as writing or speaking. This third form of identification is known as 'biometrics'. Biometric systems are applications of biometric technologies, which allow the automatic authentification and/or identification of a person.[82] Each biometric is, to a greater or lesser extent:

- universal (it exists in all persons),
- unique (it is distinctive to each person), and
- permanent (the element remains permanent over time).

There are two main categories of biometric techniques (which may be used in combination) depending on whether stable data or dynamic behavioural data are used:[83]

> *Firstly*, there are *physiological-based techniques*, which measure the physical characteristics of a person and include fingerprint verification,[84] finger image analysis, iris recognition,[85] retina analysis, face recognition,[86] outline of hand patterns,[87] ear shape recognition, body odour detection, voice recognition, DNA pattern analysis, sweat pore analysis, etc.
>
> *Secondly*, there are *behavioural-based techniques* which measure the behavior of a person and include hand-written signature

82. Biometric systems are used in two ways: authentication and identification. Authentification means checking that a person is who he says he is – what the industry calls 'one-to-one' matching. This would be used for border controls, access to physical environments, to websites, *etc.* – for any situation where currently a password or document proof of identity would be the norm. Identification means finding out who a person is by checking her against a large number of stored identities – or 'one-to-many' matching. This is used to identify suspicious people in public spaces like airports, shopping malls, etc. See Rana Dasgupta, "The Face of the Future: Biometric Surveillance and Progress", in *Sarai Reader 2002: The Cities of Everyday Life,* 290-96 at 296.

83. Quoted from the art. 29 – Data Protection Working Party's Working document on biometrics, adopted on 1.8. 2003, available at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf.

84. Fingerprint scans use the minutiae of the fingertips.

85. Iris scans are based on the pattern of specks in the colourful part of the eye.

86. Face recognition systems analyze the shape of the face.

87. Hand geometry recognition is based on the bone structure of the hand. Vascular analysis examines the pattern of veins on the back of the hand.

verification,[88] voice analysis,[89] keystroke analysis,[90] gait analysis, *etc*.

The collection of biometric data (*e.g.*, image of the fingerprint, picture of the iris or retina, recording of the voice) is carried out during the 'enrollment' phase by using a sensor specific to each type of biometric. The biometric system extracts from the data subject-specific features to build a biometric 'template'. It is the template presented in a digitized form that is stored, and not the biometric element itself.

*How biometric technology erodes the right to privacy*

If multipurpose biometric national ID cards are introduced in India, they will have a profound impact on privacy and considerably change the fabric of contemporary Indian society. The many grave privacy risks surrounding the use of biometric systems have been highlighted even by the EU's article 29 – Data Protection Working Party, in its 2003 study.

*Thumb Down! Biometrics and the corrosion of privacy of person, data and behaviour*

Biometric technologies require the collection of information intrinsic to each person. To some, the capture of fingerprints is demeaning because of its distinctly criminal overtones. To others, DNA analysis-based technology that requires samples of body fluids or body tissue would be highly intrusive. Some biometric data can also be very sensitive, for *e.g.*, in face recognition systems, data revealing racial or ethnic origin may be processed. Also troubling, in systems based on fingerprints or DNA information, samples may be collected from traces unknowingly left behind, without the data subject's knowledge, much less consent. While the first stage of data capture for the Indian National ID pilot apparently involves the collection of fingerprints only, it is not unlikely that the program might 'expand' to encompass additional or multiple identifiers, in the interests of 'enhanced security'. Naturally, the biometric ID project also involves the gathering of vast amounts of co-relating personal data. Individual habits and behaviour, therefore become increasingly transparent as people's actions are monitored through the

88. Signature scans examine the shape of a signature (static) or its progression (dynamic).

89. Voice analysis examines the frequency patterns in a human voice.

90. Keyboard dynamics use the way a keyboard is pressed to authenticate a person.

use of biometrics.[91] This is not only worrisome in itself, but also due to the potential for sharing personal data with other organizations, such as 'business partners', corporations and governments with which a 'strategic relationship' is enjoyed.

*Biometrics and the privacy risks of multipurpose identification*

Biometric schemes are expensive. Therefore, the transcendent rationale for applying biometric projects for multiple purposes becomes apparent – cost sharing. These multiple uses would, however, extend well beyond a single organization to multiple organizations in both the public and private sectors.[92] Such a mixing of government and commercial applications on one ID card amounts to leaving an electronic trail of virtually every individual activity. Even the EU's working party has warned that the standardization necessary for interoperability will lead to greater interlinking between databases, and a greater risk of use of data for incompatible purposes. The existence of a common identifier could, for *e.g.*, alert an employer to information about an employee's doctor visits and potential health problems. Compounding privacy risks, contactless cards can be read remotely without needing to be swiped at a terminal.

The government, on the other hand, argues that without interoperability, it is difficult to develop a 'business case' for biometrics. This then is the driving force behind biometric schemes: the enormous political backing and industrial power of the global purveyors of biometric technology. In order to give a rationale to the new direction of technology, biometric companies have had to spawn new social visions. By stoking public fears about terrorism and emphasizing at the same time the presumed gains from biometrics, the industry has done a prodigious job of giving the ID project its legitimacy, and completely obfuscating the pervasive erosion of privacy that the biometric cards will herald. How else did the fortunes of these hitherto relatively unknown enterprises rise exponentially in the aftermath of September 11?[93]

---

91. The outcome of any authentication procedure may be stored in a system, ostensibly for later audits of system performance, but in effect giving rise to a massive surveillance apparatus.

92. Both government and businesses in India want to see a national ID card (perhaps even GemSCOSTA) cover multi-sector applications like healthcare, banking, voting and so on.

93. See Dasgupta, *supra* note 82 at 291-92. Market researchers have predicted that the value of the world market for biometric systems will grow from $66 million in 2001 to almost $0.9 billion by 2006. See Armin Grûneich, *Deutsche Bank* Research, *Biometrics – Hype and Reality*, No. 28, 22.5. 2002 at 11. They forecast that the smart card market will grow from 3.7 million units in 2001 to 21.7 million units by 2005, a growth rate of 72.7 per cent, *supra* note 63.

In his excellent piece on biometrics and progress, Dasgupta has posed a vital question: Are we to accept technological advancement for its own sake, even though it is driven by motives of sheer profit, and divorced from any commitment to an ethical vision? Sellers of biometrics may claim that the aim of their project is to promote simple, moral, accountable, responsive and transparent (SMART) governments. But giving the state control over unprecedented amounts of personal data is a dire misadventure. As history has shown, the collection of information has a negative effect on the human ability to make free choices about personal and political self-governance. It is difficult to imagine that the security needs invoked to justify the adoption of biometrics and ID cards would also carry the argument for its multiple uses.

*Down the road to 1984: consequences of the loss of privacy*

The loss of the private sphere has serious implications for both the individual and society as a whole. Futuristic sci-fi movies have rung warning bells for years about the dangers of severing technology from values. If we give up our privacy for the sake of security, there is the very real possibility that we will end up with neither.

*Consequences for the individual: the social cost of 'safety'*

Biometrics create new capabilities for the association of identity with transactions that have never been recorded before, such as passing through a door within a building or across an intersection. By requiring individuals to be entered into a databank to exist in a legal sense or to have a bureaucratic identity, biometrics reduce individuals to codes. To add to this de-humanizing effect, the possibility of being known at any point, of an individual's identity being continually checked – in banks, malls, airports, etc. – against everything else that is known about her, will be a massive escalation in the observation matrix from the occasional 'checking-in' we currently do with each passport check or ATM withdrawal. By allowing one's very face to be converted into a digital code that can be checked at any moment without the need for any consenting action, biometrics will have a significant effect on interiority.[94] Surveillance is usually blind to what is prescribed as 'normal' behavior. The effect on behaviour is thus to whittle away at the edges of self and impose an anxious homogeneity. It will lead to a more paranoid self in which the public realm will be a hostile and tiring place where one wonders

94. Dasgupta, *supra* note 82 at 295-96.

constantly if one is looking innocent.[95]

*Consequences for freedom and democracy: our worst Orwellian fears realized*

Biometric technologies create an environment in which the government has enormous power over individuals, imperiling the sense of individuality.[96] Submitting to this technological imperative will make the repression 'troublemakers' and dissenters much easier. The lack of consistent identification of individuals is the sole factor that has held back what has been referred to as 'the dossier society' and 'the surveillance state'.[97] Never before has the state or the private sector had such a capacity to dissect an individual's life – her ethnic origin, religious and political convictions, union membership, health information – with just one swipe of an ID card. Nothing is more antithetical to the spirit of a free society. To quote from Dasgupta : "Perhaps a good test of the effectiveness of a democracy might be whether or not it permitted the populace to say 'No' to any more progress: to declare that a particular technology had been taken far enough, and should not be taken further; that new kinds of change were likely to make society worse rather than better, and should cease."[98]

**(b) How really effective is biometric technology?**

So, are biometric IDs the inevitable and welcome by-products of our corporate-controlled technology evolution and its quest for convenience and safety? Governments have become interested in biometric identification since 9/11 arguably because, unlike other forms of ID, it is more difficult to alter or tamper with one's own physical or

95. *Id.* at 296. See also Schachter, *supra* note 29 at 27-28, "Surveillance and ensuing disclosure – or even trepidation that disclosure might ensue – might jeopardize spontaneity, which otherwise would be reflected in the frivolous, impetuous, sacrilegious and defiant discourse that liberates daily life."

96. "Privacy is important to the development of an individual's thoughts and opinions, which shape and ultimately define who an individual is. If there is no guarantee of privacy in which to wrestle through important issues, and to develop and adopt what is most meaningful to an individual, the development of personality will not be complete, and neither, by extension, will the personality of a nation," Jane E. Kirtley as quoted in Schachter, *supra* note 29 at 28.

97. Privacy protection involves resistance to the establishment or consolidation of monolithic information systems. Informational chaos and functional separation amongst agencies has ensured the individual has not become a servant to the state. See Simon Davies, "Touching Big Brother: How biometric technology will fuse flesh and machine", *Information Tech. & People,* Vol. 7, No. 4 (1994).

98. Dasgupta, *supra* note 82 at 290.

behavioral characteristics.[99] It is claimed that biometric technologies promise higher security or greater convenience at a lower price and at reduced processing times in comparison with traditional technologies like passwords. There is no compelling evidence, however, that these benefits – security or convenience and costs – have ever been substantiated simultaneously in an actual implementation.[100] In its 2002 study, *Deutsche Bank* has concluded that despite all the hype, the important question as to whether biometric procedures can help fight terrorism is very likely to be answered in the negative, at least for the time being. As the studies quoted from below show, biometric identification relies on technology that is far from proven. Important questions remain about the effectiveness of automated biometric matching techniques, particularly for large-scale applications.

*Performance indicators for biometrics*

The biometric features of a human being are not rigid and exhibit some natural variation. This means that *a biometric system cannot authenticate a person with 100 per cent certainty*. Instead, it can only assess whether a presented template and the stored master template are "similar enough" to warrant acceptance. Since all biometric systems rely on such similarity decisions, there is some degree of arbitrariness – or proneness to error – in any biometric authentication process. The degree of similarity that is required for a positive match depends on the system parameter, *i.e.*, the decision threshold. If the threshold is set to 'low security', then the system allows for large variations and a legitimate user is unlikely to be refused access due to a natural variation. As a consequence, however, it is more likely that the system will recognize an illegitimate user with somewhat similar biometric features. On the other hand, if the threshold is set to 'high security', the system might not recognize natural variations, and may reject a legitimate user. It is therefore important to realize that contrary to claims made by the government and biometric industry, biometric authentication schemes require a trade-off between security and convenience.[101]

99. In the EU, there are discussions concerning the incorporation of biometrics on passports and visas. The US now requires biometric identifiers for foreigners when entering and leaving the country.

100. *Deutsche Bank* ('DB') Research, *supra* note 93 at 1-11.

101. *Ibid.* The study concludes that biometric systems are best employed as an additional layer of security to augment rather than replace traditional technologies in sensitive settings, such as nuclear power plants and military facilities, where system costs and user convenience are less critical.

*Deutsche Bank* has also noted the following in its study:

- Not everyone can necessarily be enrolled in a given biometric system. *E.g.*, manual laborers sometimes have abraded fingerprints that cannot be detected by a sensor.
- Not every legitimate user is necessarily recognized by a biometric system. *E.g.*, a gardener may have cracks in the skin of his fingers that are mistaken for minutiae.
- Not every illegitimate user is necessarily barred by the biometric system. *E.g.*, a face recognition system might not be able to discern identical twins.

*The study concludes that at present, biometric technologies are not reliable enough to replace traditional technologies in mass-market applications.*

*Performance of biometric systems: the big hoax*

Unfortunately, fairly little independently collected quantitative data on the real-life performance of biometric systems is available to the public. The *National Physical Laboratory* (NPL) of the UK conducted a still-authoritative study on the performance of eight different biometric systems (including fingerprints, iris scans, hand geometry, voice and face recognition) using both live and off-line tests, with the following results:[102]

- The study revealed *large variations* in system performance, indicating that the technology is not mature.
- The variety of different technologies that were tested by the NPL reflects the *uncertainty in the biometric market*. There is no clearly leading biometric technology, if one also considers the cost-performance ratio and prospective user acceptance.[103]
- The system that performed best in the test – *iris scan* – is also by far the most expensive, and one that many people consider *highly intrusive or potentially damaging*.[104]

---

102. Biometric Product Testing Final Report, Issue 1.0, 19.3.2001, Center for Mathematics and Scientific Computing, National Physical Laboratory, Teddington, UK quoted in *DB Research*, *supra* note 93, at 8-9.

103. While the False Rejection (FR) rate of iris scan technology was the lowest at 0.25 percent, the FR rates for fingerprints and face recognition technologies were very high at 11percent and 17 percent respectively.

104. Mark Ward, Questions over eye scan plan, *BBC News*, 7.5. 2003. See also National Institute for Science and Technology's report stating it had insufficient data to determine whether iris recognition is an accurate identifier, available at http://itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf

- Lastly, *the facial recognition system performed rather poorly*, despite the fact that the subjects faced the camera frontally.[105]

As the studies quoted above show, there are serious concerns about the efficacy of biometric technology. Even without considering the huge privacy risks associated with the deployment of biometrics, performance indicators show that many of the claims made for the technology to be used in the National ID Card are simply false. Even the US Defence Department has found wide discrepancies between manufacturers' claims of successful biometric identification rates and those seen in the field.[106] Nor does any guarantee of security or a valid security certification scheme currently exist.[107] Finally, it is still unknown at this point how a biometric system with millions of records would perform.[108] The identifier proposed for the Indian project, *i.e.*, the fingerprint, is known to have a high false rejection rate of 11 per cent. It is important to appreciate the significance of false matches made by a biometric system. Each of these false matches will cost time and effort that could have been spent protecting security in other ways, by investing resources in measures that are more likely to work. The justification advanced for the biometric national ID appears to be based more on emotion and rhetoric than credible research. Given that there are in fact grave privacy risks surrounding the use of biometrics as discussed in section A, it would appear to be a huge mistake for the government to launch an identity scheme of the scale and magnitude envisioned.

## IV Critical Evaluation of the Biometric National ID Card Project Proposed in India

There are several fundamental concerns relating to the national ID card project already launched in parts of India. These concerns are at two levels: the procedural and the substantive.

105. Even studies sponsored by the US Defence Department have shown that face recognition technology is unreliable: the system is right only 54 per cent of the time and can be significantly compromised by changes in lighting, weight, hair, sunglasses, subject cooperation and other factors. See McCullagh and Zarate, "Scanning Technology a Blurry Picture", *Wired News*, 16.2.2002.

106. Mark Ward, *supra* note 104.

107. The DB study states that biometric enrollment and authentication processes are not impervious to being attacked at different stages. Further, security standards for biometric schemes have not yet been developed.

108. See Nov. 2002 Report on Border Security by the US General Accounting Office available at http://gao.gov/news.items/d03546t.pdf

**Concerns raised by the launch of biometric national ID cards: the process**

The national ID pilot has enormous legal, infrastructural and socio-political ramifications. However, the Government of India launched this hugely significant project with absolutely *no public consultation* involving stakeholders outside the IT and management industry. Many grave concerns immediately spring to mind in considering a scheme of this magnitude: What is the extent of personal data that will be collected for this ID? How will it be protected from unlawful use? Who can query the database? How will this be regulated? Who can demand to see an ID and for what reason? Unfortunately, the Indian government, unlike the countries it purports to emulate by the introduction of such a national ID card, has not deemed it necessary to discuss any of these issues through public hearings with stakeholders outside of industry groups, which only stand to benefit from this multi-crore project. When the UK's Labour government recently mooted the idea of a national ID card, it launched a six-month consultation period to discuss its proposal and invite public comment. In Canada, the government has involved the public and civil society groups in discussions about an ID card proposal. Democracies are meant to guarantee a participatory process.

The Indian government has cited the example of ID cards in other countries to legitimize the launch of a scheme in India.[109] These kinds of *comparisons* are not only unhelpful, they're *dangerously misleading*. Take for instance the national ID system in Germany: the standard German ID card *(Personalausweis)* is used like a US driver's licence and a handy mini-passport, especially when travelling within the EU. Although the *Personalausweis* contains information like the date and place of birth, height, color of eyes, etc. it is important to stress that unlike the card proposed by the Indian government, it does not carry any biometric identifiers. Additionally, the government's proposal involves the creation of a central database of citizen data. On the contrary, information corresponding to that on the German *Personalausweis* is locally, not centrally maintained.[110] Therefore, comparisons with certain other countries where IDs might have existed even for many decades,

109. Interestingly enough, the UK does not have a mandatory national ID system to date. The two main identity documents issued by the British government are the passport and the photo-driving licence. Not all UK residents qualify for these documents and there are currently only an estimated 10 million photo-driving licences in circulation. The paper-driving licence, which remains in much wider circulation, does not even contain a photograph or date of birth but only the holder's name and address.

110. Germany has no national ID card register, and in fact, there are constitutional limitations on the establishment of any national number.

do not paint an accurate picture.

The logistical challenges of creating a secure and reliable national ID system in India present no small feat. In fact, one of the main reasons the British government decided in 2003 that it would not press ahead with its highly criticized national ID scheme[111] is because, given its size and complexity, there were still too many problems that needed resolving. Interestingly enough, while the government of a country of about 60 million people finds it an immense logistical challenge to introduce a secure and accurate national ID system, the Indian tech industry and government have not balked at the 1.05 billion population figure.

It is a mammoth leap to go from not having any identity card at all to introducing a national ID card with biometric identifiers and multiple applications, thereby negating the right of privacy. The fact that there are some western countries with national ID systems is not reason enough to adopt the scheme in India. While the introduction of national ID cards might arguably have some benefits, we need to be aware of the trade-offs and consequences, and legitimate the choices made. The government's unwillingness to engage in any wider conversation about this important project compounded by its misinformation efforts go against every canon of democratic legitimacy.

**Concerns raised by the launch of biometric national IDs cards: the product**

It is a great irony that in 1906, Mahatma Gandhi led a campaign of resistance against the South African government's introduction of identification documents for all Indians. The measure required every Indian over the age of eight to be fingerprinted and registered. There as well, the IDs were ostensibly introduced to control illegal immigration. In an emblematic moment demonstrating their protest, two thousand Indians threw their IDs into a cauldron of burning paraffin. Today, almost a century later, the Indian Government wants to introduce the same tool for ostensibly the same objective.

Modernizing elites in the so-called 'Third World' are often better placed than the industrialized west to put in place technologies of mass surveillance on a nationwide basis, due to the lack of constitutional

111. Widespread opposition from groups across the political spectrum to the national ID scheme resulted in the government's watering down its measure to merely making available *voluntary plain identity cards* for those who wished to take it up. Any move towards compulsion would require clear public acceptance, full debate and a vote in both Houses of Parliament, and would not be made until the end of the decade.

safeguards to privacy, or the lack of awareness at the public level of privacy issues.[112] While a national ID card system might seem innocuous, its implications can be devastating. The introduction of the cards will legitimize a huge invasion of privacy. Not only will the state have control over vast amounts of personal data, those who do not get the cards (perhaps because they are immigrants or refugees – the Bangladeshi *rickshaw* puller or the Nepali *gorkha*) will now have to face considerable police harassment at day-to-day levels because they will not be able to produce their cards when they are stopped on the streets. More worryingly, national ID cards with group classifications (religion, race, ethnicity) are known to lead to societal and institutional polarization, even demonization. In India, pogroms like the anti-Sikh riots of 1984, and the more recent anti-Muslim massacres in Gujarat in 2002 have been administered with the help of electoral registers, and a biometric ID card system would make such exercises that much simpler and more efficient.

India's international treaty commitments – for example, under the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the UN Convention on the Rights of the Child (UNCRC) – oblige the government to protect and guarantee the right to privacy. The UDHR contains the modern privacy benchmark at an international level. Article 12 specifically protects territorial and communications privacy. It states: "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honor or reputation. Everyone has the right to the protection of the law against such interferences or attacks." Numerous other international human rights treaties, some of which India is a party to, also specifically recognize privacy as a right.[113]

India's constitutional guarantees would also make the biometric national ID scheme untenable. Unless the government can show that the introduction of biometric national ID cards will not infringe upon individual privacy, it will not only be violating its international commitments, but also the mandate of the Constitution as interpreted by the Supreme Court in a plethora of cases over the last three decades. The importance of the private sphere where the individual has a right to be let alone, in the interests of his self-development, has been judicially recognized as a fundamental right since *Govind* was decided. Since as early as 1975, the court has emphasized the value of privacy in promoting self-development, and in protecting the individual's interest in becoming,

112. Sengupta, *supra* note 68, at 298.

113. Art 17 of the ICCPR, and art 16 of the UNCRC adopt the same language as that in art 12 of the UDHR. For the texts of these instruments, see http://www.unhchr.ch/html/intlinst.htm

being and remaining a person.[114] The Supreme Court's privacy jurisprudence is still evolving, but the importance of protecting the individual from official surveillance is unequivocally established. Any identity scheme that puts in place a mass surveillance apparatus impairing individual autonomy and self-development would manifestly run contrary to the essence of the constitutional protection of the right to privacy. Moving towards a system of national identification numbers, databanks and identity cards contradicts the constitutional and philosophical bases of our democratic government and undermines the moral economy of political and personal identity.

The philosophy underlying the constitutional protection given to the right of 'informational self-determination' in Germany is its vitality in promoting the dignity of the individual and the development of his personality. The individual capacity for self-determination and deliberative democracy are indispensable to the maintenance of a democratic order. This aspect of self-determination is threatened when government or private action interferes with a person's control of her reasoning process. The same values of human dignity and inviolate personality are recognized and sanctified in Indian constitutional jurisprudence. The Indian Supreme Court has held that the right to life means more than animal existence.[115] It includes the right to live with human dignity[116] and all those aspects, which go to make a person's life more meaningful, complete and worth living.[117] The right to life carries with it the necessary conditions for promoting the development of every individual. The penumbra of privacy is said to emanate from the totality of constitutional provisions intended to secure inviolate personality and thus promote the meaningful pursuit of happiness. Even the Preamble of the Indian Constitution, which contains the ideals and aspirations that the Constitution-makers intended to be realized, assures

---

114. See K.K. Mathew, "The Right to be Let Alone", (1979) 4 SCC 1 (*Jour*), for a comment by the former judge of the Supreme Court on the value of privacy and the nature of the interest it protects. "Individual autonomy, perhaps the central concern of any system of limited government, is protected in part under our Constitution by explicit constitutional guarantees. In the application of the Constitution our contemplation cannot only be of what has been but what may be," Mathew, J. in *Govind*, *supra* note 40.

115. *State of Maharashtra* v. *Chandrabhan,* AIR 1983 SC 803 (paras 1, 20).

116. *Francis Coralie* v. *U.T. Delhi, Administrator,* AIR 1981 SC 746 (para 3); *Olga Tellis* v. *Bombay Corpn.,* AIR 1986 SC 180 (paras 33-34); *D.T.C.* v. *Mazdoor Congress Union D.T.C.,* AIR 1991 SC 101 (paras 223, 234, 259); *Consumer Education and Research Center* v. *Union of India,* (1995) 3 SCC 42 (para 22).

117. *Maneka Gandhi* v. *Union of India,* AIR 1978 SC 597; *Bd. of Trustees of the Port of Bombay* v. *Nadkarni Dilip Kumar Raghavendra,* AIR 1983 SC 109 (para 14).

every citizen human dignity. It could, therefore, be argued that even in India, the right to informational self-determination might be recognized and protected as a necessary concomitant of the right to privacy, based on human dignity and inviolate personality. As Upendra Baxi has written, "in *Govind v. State of M.P.*" – which remains the cornerstone of privacy rights in India – "the Court has preserved the rich indeterminacy and open texture of the right to privacy."[118]

However, regardless of whether or not the right to informational self-determination is recognized in India, the proposed biometric ID card project poses a significant risk to the essential values of dignity, autonomy and inviolate personality that the Supreme Court has already recognized and articulated. If a legal challenge were to be brought against the biometric national ID scheme, it is questionable whether the government would be able to build a plausible case that compelling state interests outweigh the substantial concerns in protecting individuality and democracy in this instance. "With the Supreme Court's having given the right to privacy a foothold in the fundamental rights chapter, the Orwellian fear of the 'knock on the door' has been contained. 1984 is just not seven years away. By judicial dictum it has been hopefully pushed back for decades."[119] Once again, we the people are at an important crossroads. The intrusion into the private sphere foreshadowed by the biometric national ID card project is the gravest threat to the elementary conditions of our free democratic community. The risks and consequences of the project merit immediate and urgent reconsideration, if the Constitution's guarantee of the right to life and personal liberties and the Preamble's assurance of human dignity are not to be rendered devoid of meaning.

## V Where to Go: Policy Choices and the Need for a Well-Defined Privacy Law in India

### (a) Policy options relating to the proposed biometric national ID project

While on the one hand, biometric national IDs may arguably be of value in reducing the danger of terrorism and illegal immigration, on the other hand, there are serious concerns about their introduction, which incidentally cut across similar discussions relating to data mining, profiling or electronic surveillance:

1. A distrust of what other uses the government will make of information acquired for national ID purposes and of the

118. Baxi, *supra* note 34.

119. Nariman, *supra* note 41 at 83.

mistakes it may make in handling that information in an effort to reduce terrorism or illegal immigration.

2. The political consequences for any democracy of a widespread fear of governmental misuse of very large quantities of information about its citizens, whether the fear is realistic or not.

3. The social and personal consequences of a lost sense of the ability to sharply limit access to information about one's activities and communications.

The choice, therefore, is whether to rely on legal safeguards and construct a biometric ID system in a data protection-friendly manner, or, not trusting such checks and balances, to reject the biometric identity project. There are a range of four concrete options in terms of responding to the question about whether to have a multi-use biometrically-enabled national ID card or not.

(a) Accepting the idea *in toto*, *i.e.*, to have a national ID with biometrics for multiple applications; or

(b) Accepting the idea of a biometric-enabled national ID, but restricting its uses; or

(c) Accepting the idea of a national ID, but without any biometric identifier(s); or

(d) Rejecting the entire proposal for a nationwide identity system *in toto.*

In 2002, the US National Research Council prepared a study on Nationwide Identity Systems, outlining questions that needed to be asked before the US moved (if ever) towards such a system.[120] These policy questions are equally relevant to guide the Indian discussion:

- What is the *purpose of the system*? Possibilities range from expediting and/or tracking travel, to prospectively monitoring individuals' activities in order to look for suspicious activity, to retrospectively identifying perpetrators of crimes.
- What is the *scope of the population* that would be issued an ID card? How would the identities of these individuals be authenticated?
- What is the *scope of the data* that would be gathered about individuals participating in the system? Would only identity

120. National Research Council, IDs – Not That Easy: Questions about Nationwide Identity Systems (2002) available at http://books.nap.edu/html/id_questions/ch1.html

data be collected? Or would other data be collected, stored, and/or analyzed as well? With what confidence would the accuracy and quality of this data be established and subsequently determined?

- *Who would be the user(s)* of the system? If the assumption is that the public sector/government will be the primary user, what parts of the government, in what contexts, and with what constraints? In what setting(s) in the public sphere would such a system be used? Would state and local governments and the private sector have access to the system? What entities within the government or private sector would be allowed to use the system? Who could contribute, view, and/or edit data?
- What *types of use* would be allowed? Who would be able to ask for an ID, and under what circumstances? Beyond simple queries, would analysis and data mining of the information collected be permitted? By whom and for what purpose(s)?
- Would participation in and identification by the system be *voluntary or mandatory*? In addition, would participants have to be aware of, or consent to, having their IDs checked (as opposed to, for example, allowing surreptitious facial recognition)?
- What *legal structures* protect the system's integrity as well as the data subject's privacy and personal liberty, and determine the government and relying parties' liability for system misuse or failure?

Each of the questions above evokes a larger set of issues that must be resolved. In addition, many of these issues are interdependent, and choices made for each will bear on the options available for resolving other issues. These decisions will also determine the technological underpinnings of the system. A scheme with potentially such a significant impact on the physical environment needs to be subject to a comprehensive assessment process that requires:

– Broad agreement on what problems a nationwide identity system would address. Once there is such an agreement, alternatives to identity systems can also be considered as potential solutions;
– full public disclosure of the technology and the applications envisaged;
– appropriately funded social impact analysis;
– clear identification of and deliberation upon the goals of such a

system, with input sought from all stakeholders. Public review of these goals prior to selecting a proposed system is essential;

– active public participation in scheme design; and

– controls built into the scheme.

This kind of impact assessment will be vital to informing the policy choices. In the meantime, one needs to seriously consider the imposition of a moratorium on the applications of biometrics, given their extraordinarily serious implications, and the absence of any effective protections. Such a ban would need to remain in force until after the assessment exercise, and, if the scheme is approved as result, until a comprehensive set of design requirements and protections has been devised, implemented, and is actually in force. Only in this manner can biometric technology providers and scheme sponsors be forced to balance the interests of all parties, rather than serving only narrow, vested interests.

**(c) Legal safeguards**

In the event it is decided in favour of a nationwide identification system, certain legal safeguards to protect individual rights need be implemented. In a world that demands that corporations maximize profit, market share and shareholder value, the possibility that the purveyors of biometric technologies might self-regulate is highly unlikely. As such, two other more viable options are: specific regulation and a generic privacy law.

*Specific regulation*

Once there is sufficient understanding of the nature and implications of biometric technologies, the implementation of the biometric ID scheme needs to be specifically regulated. Some important principles that can be underscored are:[121]

Design standards for biometric measuring devices which ensure that the biometric will not be permitted to be accessed or captured; audit of compliance of biometric measuring devices with the design standards; prohibition of the manufacture, import, installation or use of biometric measuring devices that do not comply with the design standards; two-way device authentication, i.e., chips on individuals' devices must test the authenticity of devices that seek to transact with them, and must not merely respond to challenges by devices; and no central storage, instead, storage only on a device under the person's control, and subject to

121. Clarke, Biometrics and Privacy, 15.4.2001, available at www.anu.edu.au/people/Roger.Clarke /DV/ Biometrics.html

security features that make capture of the data by any other party unlikely.

**Generic privacy legislation: a potential model for India**

The biometric national ID pilot has already been implemented in parts of India. Biometric driver's licences will also become operational in many states soon. At this point, whether or not the proposed multipurpose biometric national ID project finally goes through, a generic privacy law will be indispensable for the protection of individuals against governmental and corporate privacy invasive practices. India urgently needs to summon the necessary political will for a comprehensive privacy law ensuring stringent privacy standards to be passed in Parliament. So far, the only push for such a law has been born of the desire to retain India's revenues from outsourcing operations for American and European companies, whose laws prevent the flow of data to countries without adequate privacy safeguards. However, a strong privacy law is needed first and foremost to protect the rights of Indians against abuse by both, the private sector and government, which are collecting vast quantities of personal information, even independently of the national ID project, without any checks or controls. Recent years have seen a rapid expansion in the automation of governmental functions. To take the example of just one state in India – Andhra Pradesh – it has amassed an enormous amount of personal data from its various 'citizen-friendly' e-governance projects like e-Seva, Saukaryam, MPHS and so on. [122] Considering the serious privacy risks all of this data is exposed to, the immediate need for a comprehensive privacy law cannot be over-emphasized.

As a point of reference and potential model, [123] it is worth looking at the scheme of privacy protection under the EU Directive on Data Protection.[124] The directive lists eight broad principles to be adhered to in protecting the privacy of personal information at every step, from collection to storage and dissemination. These principles are quoted at length below:

---

122. See the official website of the Department of IT & Communications, Government of Andhra Pradesh, available at www.ap-it.com

123. The US Privacy Act of 1974 affords limited protection due to its many exceptions. For an examination of the Act's failure to protect Americans against a flurry of privacy erosive measures, see Marcella and Stuki, *supra* note 1 at 173-77. In addition, considering that the US has a more self-regulatory and market-oriented approach, it is felt that the comprehensive framework of European data protection would be more desirable in the Indian scenario.

124. Directive 95/46/EC of the European Parliament and of the Council dated 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://europa.eu.int/comm/internal_market/privacy/law_en.htm. The directive outlines the basic principles for privacy legislation for EU member countries.

i. Collection limitation principle
There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

ii. Data quality principle
Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

iii. Purpose specification principle
The purposes for which personal data are collected should be specified not later than at the time of data collection, and the subsequent use limited to the fulfilment of those purposes, or such others as are not incompatible with those purposes, and as are specified on each occasion of change of purpose.

iv. Use limitation principle
Personal data should not be disclosed, made available or otherwise used except:

- with the consent of the data subject; or
- by the authority of law.

v. Security safeguards principle
Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure of data.

vi. Openness principle
There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

vii. Individual participation principle
An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him; within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have

the data erased, rectified, completed or amended.

viii. Accountability principle
A data controller should be accountable for complying with measures that give effect to the principles stated above.

## VI Conclusion

The legal and policy issues associated with nationwide identity systems warrant much more detailed and comprehensive examination and assessment than has been presented by the Indian government so far. It is hoped that questions and issues raised here will help to both further and inform the policy debate.

The government's national ID initiative comes at a time when the surveillance apparatus in India has grown exponentially to embrace countless activities in everyday life from banks, to apartments, offices, industrial areas and traffic intersections.[125] ID cards will only be one more element in the apparatus of surveillance, adding to the battery of legal instruments ranging from the IT Act to the Communications Convergence Bill which authorize official intrusion by state agencies in the interests of 'national security'. Right now, the choice is ours. But it won't be for much longer, because corporations and the government are moving to implement such schemes, and once they have been implemented, the scope for opposition will be drastically reduced.

While biometrics providers flourish by selling their technology, the result will be the arming of the government and private corporations with enormous power over individuals, and have devastating effects for our personal liberties and democratic tradition. It is critical that we appreciate the seriousness of the threats, and impose substantial constraints on biometric technologies and their use. This demands public commitment instead of passivity on the issue – the public must resist misinformation campaigns and the appealing imagery of smooth access to public benefits through 'the service card'. It also demands courage by elected representatives, who must withstand pressure from large corporations, and from the national security and law enforcement apparatus that invokes such bogeymen as terrorism, illegal immigration and domestic law and order as justifications for the implementation of

125. The hi-tech surveillance industry sees India as one of the most lucrative potential markets with a growth potential of 25 per cent in an industry that already has a turnover of close to US$20 million per annum. See Bhatnagar, "Industry Sector Analysis Report of Safety & Security Equipment in India", as quoted in Sengupta, *supra* note 68 at 300.

privacy invasive technologies. Only then can one hope to achieve some balance among the needs of individuals and society as a whole.

"As nightfall does not come all at once, neither does oppression. In both instances, there is a twilight where everything remains seemingly unchanged. And it is in such twilight that we must all be most aware of change in the air – however slight – lest we become unwitting victims of the darkness."[126]

126. William O. Douglas, former Justice of the US Supreme Court (1939-'75), in a letter to the Washington State Bar Association, 1976, as quoted in Diana Rachel Hyman, *Defenses of Solitude: Justice Douglas, the Right to Privacy, and the Preservation of the American Wilderness*, thesis presented to the Program in the History of American Civilization, Harvard University (Jan 2003).