LAW MANTRA THINK BEYOND OTHERS
(I.S.S.N 2321- 6417 (Online)
Ph: +918255090897 Website: journal.lawmantra.co.in
E-mail: info@lawmantra.co.in contact@lawmantra.co.in

COMPROMISING CITIZENS' PRIVACY FOR NATIONAL INTEREST: A FAIR TRADE OFF?*

INTRODUCTION

The identification of individual has always been challenging and society has always tried its best with the available technology. The current struggle of adoption of new technology for identification and further strengthening the system is nothing new.

Proponents of the government argue that security and national interest is more important than privacy. It can be difficult to discuss privacy in a global context because the word *privacy* has no universal definition.[1] **John Stuart Mill** in his essay, '**On Liberty**' (1859) gave expression to the need to preserve a zone within which the liberty of the citizen would be free from the authority of the state. According to Mill:

"The only part of the conduct of any one, for which he is amenable to society, is that which concerns others. In the part which merely concerns himself, his independence is, of right, absolute. Over himself, over his own body and mind, the individual is sovereign."[2]

The U.S. Supreme Court interprets the US Constitution as protecting as a privacy matter both information privacy and a broader range of interests often described as *personal autonomy*, but much uncertainty remains about the scope of the constitutional privacy interest.[3]

Hon'ble Supreme Court of India in its recent judgment of *Justice K S Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*[4], has held right to privacy to be a fundamental right within the meaning of Article 21 of our Constitution.

In the judgment, Justice D Y Chandrachud [for CJI Khehar, Justice R K Agrawal, and Justice Abdul Nazeer] has opined privacy to include:

"Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left

---

· **Mr. Ashutosh Kashyap and Ms. Vishakha Srivastava, 4th Year B.A.LL.B, Chanakya National Law University.**

[1]Robert Gellman, Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries, CGD Policy Paper 028, Page 3 (August 2013).

[2]John Stuart Mill, *On Liberty*, Batoche Books (1859), at page 13.

[3]Whalen v. Roe, 429 U.S. 589 (1977),
Accessible at http://www.law.cornell.edu/supct/html/historics/USSC_CR_0429_0589_ZS.html.

[4]WRIT PETITION (CIVIL) NO 494 OF 2012.

alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being;"[5]

In the same judgment, Justice Chelameswar out forth his observations as:

"The decision making process regarding the freedom of association, freedoms of travel and residence are purely private and fall within the realm of the right of privacy. It is one of the most intimate decisions. All liberal democracies believe that the State should not have unqualified authority to intrude into certain aspects of human life and that the authority should be limited by parameters constitutionally fixed."[6]

Therefore, it can be safely concluded that the Supreme Court has tried to give clarity to the meaning of privacy. But still both the terms, Privacy and National Interest are largely vague and have no definite meaning whatsoever.

Basic Flaw

Biometrics relies on unique physical attributes. Fingerprints are the most classic biometric, with face, iris, voice, hand geometry, and other systems in use and more in development.

"A biometric identifier may work today only under ideal conditions with bright lights, close proximity, and a cooperative data subject. In the future, however, a later generation of the same technology is likely to allow the capture of the same biometric identifier in low light, without the data subject's consent, and while that data subject is walking down a public street at some distance from the sensor. When evaluating the privacy consequences of identification technology, it does not seem appropriate to assume that privacy protections afforded by current technological limits will continue to protect privacy in the future. Technology will change, but the need to address privacy will not."[7]

Identity Theft and the Advanced Persistent Threat

Identity theft is the misuse of another individual's personal information to commit fraud.[8] Identity theft (sometimes called *identity fraud*) occurs in many ways, but the basic elements are the same. Criminals gather personal information by stealing mail, workplace records, or other information, or they use high-tech methods such as hacking of websites, fraudulent email (phishing), social

[5] Ibid., para F, at page 263.
[6] Ibid., at page 306.
[7]Robert Gellman, Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries, CGD Policy Paper 028, Page 2 (August 2013).
[8] The President's Identity Theft Task Force (US), *Combating Identity Theft: A Strategic Plan,* page 10 (2007), http://www.identitytheft.gov/reports/StrategicPlan.pdf.

media sites, or purchasing information from companies selling background information about individuals. The criminals use the information to open credit accounts, take over existing accounts, obtain government benefits or services, or in other ways. Identity theft has grown in volume and cost in recent years. Losses in the United States are uncertain but total billions of dollars annually.[9]

While the crime of identity theft is not limited to the United States, much of the world's identity theft activity affects Americans. There are many reasons, including the widespread availability of personally identifiable information about US citizens, the reliance on Social Security Numbers for credit and identification purposes, lack of effective privacy laws, and the wealth of the country. Identity theft is an industry complete with the wholesale buying and selling of personal data by criminals. The Internet makes it possible for criminals to engage in identity theft from any place in the world. Today, poorer countries may not be prime targets for identity thieves, especially those operating via the Internet. However, this could change as cell phones, bank accounts, and Internet-based transactions spread. Any personal identification system must consider the possibility that identity thieves will look for ways to capture and exploit identifying information.

The use of biometrics does not guarantee protection against identity theft. The Electronic Frontier Foundation (EFF), an international non-profit digital rights group based in the United States, writes about the problems with compromised biometric systems:

"Arguments in support of biometrics rest on the flawed assumption that these ID schemes prevent identity fraud. Yet identity and authentication systems based on biometrics are weak because once these indicators are compromised, they cannot be reissued like signatures or passwords. You cannot change your fingerprints or your irises if an imposter is using this data. Up to five per cent of national ID cards are lost, stolen or damaged each year. Aggregated personal information invites security breaches, and large biometrics databases are a honeypot of sensitive data vulnerable to exploitation. Identity thieves can also exploit other identifying information linked to stolen biometric data. Those at the mercy of these databases are often unable to verify their security or determine who has access to them."[10]

A national identification database – with or without biometric identifiers – may become the target of criminals who want to exploit identity information. It could also become the target of other governments looking for dissidents, expatriates, or others. Anyone seeking to destabilize a country's activities that rely on an identification system might target that system. The more any single identification system is used, the greater the vulnerability.[11]

Centralization and Surveillance

In 1988, Australian privacy analyst Roger Clarke introduced the term '*dataveillance'* to mean the systematic monitoring of people's actions or communications through the application of information technology.[12]

---

[9] Ibid., at page 11.
[10] Electronic Frontier Foundation, *Mandatory National IDs and Biometric Databases*,
Accessible at https://www.eff.org/issues/national-ids.
[11]Robert Gellman, Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries, CGD Policy Paper 028, Page 18 (August 2013).
[12] Roger Clarke, Information Technology and Dataveillance, 5 Commun. ACM 498-512 (May 1988),

The use of an identification system can create detailed usage or transaction records. Consider an ID card that a user presents to engage in a transaction or activity that is reported to a central database. The central database may keep a record each time it receives a request for identification. Depending on how those records are maintained, the file for each individual could reveal each time the individual obtained benefits from a government agency, patronized a merchant, used a credit card, received health care, withdrew money from an ATM, transferred money to someone, accessed the Internet, or engaged in any other activity that relied on verification of identity. The record would not only show the activity. It would possibly include a variety of details about the transaction, such as amount withdrawn from an ATM, also the time and location when the activity occurred. The resulting centralized file would provide a detailed history of each individual's activities, perhaps over an extended period. What else other than its comprehensive activity records would constitute a surveillance system?

Conclusion

Biometric system of identification has been a recent phenomenon in many developing countries. The adoption of biometrics has not always been accompanied by an adequate discussion of privacy. In some countries, this identification scheme is for a specific service and in some, this identification system has been made mandatory for host of services either subsequently or since beginning only.

In both the cases they lacked adequate discussion of privacy and carried on with the work in the garb of national interest without thinking about repercussions.

It is nothing but compromising citizen's privacy. In a country like India where a vast population casts vote for a candidate without any agenda or mandate, money and muscle power still pervades the electoral system of the country. A vast population lives under below poverty line and struggles for two meals a day. This agenda of shoving down a scheme under their throat in complete absence of element of choice is nothing but tyranny. The government of the day itself is not aware of the risks involved and the threats that this system might pose. Such a drastic step of making a voluntary identification system subsequently into a mandatory one, and not just for some social service scheme but for host of services in the name of national interest can never be a fair trade off.

The greater the applicability, the greater the risk involved. In today's era a country's geographical size doesn't matter nor does the number of troops matter. The great reliance on technology has made us all vulnerable. There are State-sponsored cyber wars and in this war even a small country can disrupt everything in a big and powerful country. Even in the presence of legal infrastructure, compromising citizen's privacy can be a heavy cost. A law is not easy to amend. It is a complex and lengthy process. Compromising citizen's privacy for a vague concept such as 'National Interest' meaning of which can be twisted to meet various selfish motives of people in power or people posing threat to the system, can never ever be a fair trade off.

Accessible at http://www.rogerclarke.com/DV/CACM88.html.