Research Paper Social Science

Aadhaar, Function Creep and The Emerging Symbiotic Relationship between Society and Technology

Dr Valsamma KM Associate Professor, Department .of SAC, KCAET, KAU, Tavanur, Kerala, India.

ABSTRACT

Aadhaar is in the eye of the storm ever since UIAD declared that it is going to use multimodal biometrics for issuing Aadhaar enabled unique identification numbers to a large portion of India's 1.2 billion population. What was initially touted as a voluntary scheme was soon morphing itself into a compulsory scheme and also exhibiting signs of function creep when the scope of bio metric scanning was extended to additional purposes not announced earlier. In no time, the Govt was pushing forward Aadhaar by introducing the AePS [the Aadhaar enabled payment system].The paper presents a critical analysis of current approaches and performance of various biometric system.

KEYWORDS Multimodal biometrics, UID; SSN; Aadhaar.

I. INTRODUCTION

The biometrics is perhaps another holy grail in the making for researchers and easily the object of an extended quest. After slowly taking foot hold in our lives, it has almost single handedly taken the landscape by storm, changing the traditional method of transactions like tokens, usernames and passwords. E-transactions are the way of the future[1]. Financial institutions and banks, along with many other organizations, are being forced to modify the techniques with which they carry out business. To build upon and make the best use of appropriate technologies that will boost the proper utilization, presupposes a receptive and competitive ambience. These technological changes have brought with them e-transaction hackers and identity theft. Cyber crimes have become common and are only expected to increase. However, a more efficient means of protecting identities and transactions is required to be implemented and the best method of providing such secure identification at this time is by employing biometric systems. Biometric systems are systems that exploit the automated methods for recognizing individual's physiological or behavioral features. It is a specialized information system with the objective of differentiating the bona fide user from impostors and has all the components of a real information system, defined as an organized combination of people, Hardware, software, data resources, policies and procedures, that stores, receives, transforms and disseminates information in an organization. Aadhar is now currently used as one of the biometric identifier. The linking of Aadhar to cooking Gas for DBTL , social security pension, scholarships, NREGA wages etc is all before us.

II.Recent Advances

Biometric Identifiers connects identification numbers and other records, within a given population and are unique in that. That is, it is a new form of media that digitally mediates between the body and the identity, between technology and biology. Biometrics when combined with other advances in ICT can leverage far more functional purposes like voting, transfers or enabling financial or health insurance markets etc. that, further incorporation, make easier the access to rights, services and enforce public accountability. That is, it is essentially a pattern recognition system that makes a personal identification, by establishing the authenticity of a specific physiological or behavioral characteristic possessed by the individual. It can be used in two ways: identification to determine who the person is, through one- to- one comparison and verification, to determine whether the person is, who he claims to be by one- to- one comparison. A biometric system can be divided into the enrollment and the identification module in a strict logical sense[2]. In the enrollment phase, the biometric characteristic of an individual is first scanned using a biometric sensor to acquire a digital representation of the characteristic. This digital representation is further processed by a feature extractor to produce a compact, expressive representation: the so called ' template', which depending on the application can be stored in a data base or/and in a magnetic or smart card. As with enrolment stage, in the identification phase too, a biometric image captured by a sensor, is processed by a similar algorithmic procedure to get a ' live template': which is further compared/ matched against a stored template to confirm whether the person is known to the system in the database, in the case of database or the biometric capture is one on the chip card, in the case of magnetic chip/smart card.

The most widely used biometric authentication to date is finger print recognition. Fingerprints are one of multimodal biometrics used in Aadhaar where we rely on the graphical ridge valley patterns from human fingers[3].Biometrics has grown a long way from its origin in bertillonage and dactyloscopy to iris scanning, DNA analysis and beyond. In all these techniques, what is en route is the process of acquisition, storage and analysis of biological information via algorithmic and computational methods, whereby the notion of 'body as information' is obvious. Finger prints and the science behind it remains to be the staple of science fiction films and novels as far back as 1894. In the novel The Tragedy of Puddn'head Wilson, fingerprints are shown as conclusive evidence of identity. Again, in a 1951 film Fingerprints don't lie the theme is centered round fake fingerprints. In Along came Spider a movie made in 2000 the theme is removal of fingerprints. Though retina, iris scan(i.e., recording the iris, the annular region of the eye, bounded by the pupil and sclera on either side which is considered the most accurate biometric parameter), voice, face, DNA as identifiers have come of age only recently, science fiction films like Mission Impossible, Robot , X-Men 2, Star Trek III have been showing face recognition even before. The Mobile Offender Recognition and Information System (MORIS) of recent origin in the US and, the Checkpoint's system developed by Omni Perception which identify faces even in a crowd integrates biometrics into one prototype platform. As a result of all these emerging technologies, the dividing lines between fact and fiction stands considerably blurred. Now it has come to the fore that fingerprint scanners can be fooled by what is known as spoofing. Fake fingerprints known as "gummy fingers" can be created by making moulds of latent fingerprints left by legitimate users. This can be done using play-doh, gelatin and silicon. Liveness detection by pulse oximetry, blood pressure etc is regarded as a safeguard. When a submitted sample is incorrectly matched to a template enrolled by another user it gives rise to false acceptance. Actually Live false reject rate and spoof false accept rate determines the success of biometrics. Researchers at the University of Notre Dame have found that even patterns in

irises change significantly as people age. As the length of time between the photos increases, the rate of false matches also increase.

Mark Twain, the wit had once said that classic is a book which everybody wants to have read but nobody wants to read. UID can be rightly accorded the status of Mark Twain notion of classics: that is, it is the unique number which the Government wants everybody to own but no body to possess without coercion. The time is now to take stock of what multimodal biometrics, the technology behind Aadhaar means to most of us. The impact of Aadhaar cannot be dismissed as inconsequential at a time when life itself is incrementally becoming digital. This prompts us to ask ourselves how biometric identification is going to affect our privacy. Biometrics is a milestone in the emerging symbiotic relationship between society and technology. But the tradeoff between security on the one hand and the privacy on the other cannot be overlooked. By and large privacy appears to be an evolving concept, burdened with several definitions. Biometrics when Used in certain ways, provides vast security because the biometric identifier is much harder to steal or counterfeit. On the other hand, where biometrics are authenticated remotely, a hacker might be able to steal, copy, or reverse-engineer the biometric. This misappropriation could also come about through insider misuse. Concerns about actual harm that could be caused by biometric technologies are primarily perceptual. Although the technology is in fact harmless, the perception of harm may call users to obstruct the implementation of a program .

III AADHAR FUNCTION CREEP

Function creep, the process by which the original purpose for obtaining the information is extended to include purposes other than the one originally stated and can occur with or without the knowledge/ agreement of the person supplying the data[4-5]. In a speech delivered at Melbourne on "India's Transformation: The role of Information Technology" the UIAD chairman has gone on record that "by Oct 2013 UIAD has issued 450 million Aadhhaar numbers" at a cost of 35 billion (3500 crores). What is visible here is also an example of function creep. The use of SSNs is a prime example of function creep—an individual's SSN is used for an array of purposes in the public and private sectors . The National Human rights commission (NHRC) is holding the opinion that the decision of government to provide its citizens with Aadhaar to facilitate access to benefits and services, in its present form could ultimately lead to discrimination. History tells us that in the US in 1936 Social security Numbers had a similar beginning. Then the sole purpose of SSN was made out to be to sub serve the interest of Government in record keeping for determining the amount of social security taxes that had to be credited to each contributor's account. Further, the intention of SSN was borne out by the legend ,"Not for identification" printed on the card. By 1961 the Internal Revenue Service (IRS) began using the SSN for tax identification purpose. By 1997 "everything from credit to employment to insurance to many states' drivers licenses requires Social Security Number" . "Not for identification" was easily forgotten by Government and in no time SSN became the de facto national identification number.

In the US in the wake of the 4th amendment courts are intervening when there is an invasion of a "reasonable expectation of privacy" which is why justice Brandeis of the US supreme court had warned in his famous Olmstead dissenting judgment: "the greatest danger to liberty lurk in the insidious encroachment by men of zeal, well meaning but without understanding". But in a litigation between DOW Chemicals and EPA on the legitimacy of EPA authorized over flight on the 2000 acre factory site, when it came to a question of deciding what constitutes a reasonable expectation of privacy the court had decided in favor of the Govt and EPA. The argument that the photographs captured by EPA was highly confidential information that DOW had taken reasonable and objective steps to preserve as private was not admitted. The core issue is not one of controlling biometrics but rather the challenge of how law and policy should control contemporary information systems. Tracking issues are also a major concern today in part because the public has been made aware of informational commerce.

IV CONCLUSION

In the security-conscious world in which we live, it is more likely that Aadhar enabled unique identification numbers are here to stay and it is a milestone in the emerging coexistent relationship between society and technology. What was offered was a voluntary scheme was soon changed its shape to a compulsory scheme, exhibiting signs of function creep when the scope was extended to additional purposes not announced earlier. It is expected that "everything from credit to employment to insurance to many states' drivers licenses requires Aadhar, "Not for identification" was easily forgotten and in no time It became the de facto national identification number.

REFERENCES

[1] Prabhakar, S., S. Pankanti, and A.K. Jain, 2003. Biometrics Recognition: Security and Privacy Concerns. IEEE Security & Privacy,. 1(2); 33-42. | [2] J.D.M. Ashbourn, 2000.'Biometrics : Advanced Identify Verification: The Complete | Guide', Springer-Verlag;1-352. | [3]R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press. | [4] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, 1982. "Electron spectroscopy studies on | magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, | 740-741. | [5] M. Young, 1989. The Technical Writer's Handbook. Mill Valley, CA: University Science, | 648-655. |