Flesh into Data; A South Asian Perspective on the Right to Privacy in the Biometric Context

HMMC Herath[1#], MSHV Eshan[2]

[1]*Sri Lanka Law College, Sri Lanka*
[2]*PricewaterhouseCoopers, Singapore*
[#]For correspondence; <mayomiherath@gmail.com>

Abstract— *Biometric technology has become an emerging trend in the modern electronic era. However, identification of people by the use of biometric technology leads to human rights issues, out of which intrusions to privacy plays a major role. This study seeks to answer the problem as to what extent the Constitutions in Sri Lanka and India shield the right to privacy in the biometric identification and what measures could be introduced in order to enhance the constitutional privacy protection in Sri Lanka. The primary objective of this paper is to recognize the current constitutional provisions pertaining to right to privacy in Sri Lanka and India in light of biometric identification. The secondary objective is to analyse the constitutionality of the Sri Lankan and Indian biometric identification systems. The subject matter of this discipline has been limited to biometric identification opting out other concerns on the said technology. This study revolves around the human rights concern of the right to privacy although biometric technology itself carries numerous other legal concerns. As per the research methodology, black letter approach was used in order to undertake an in-depth analysis on the Sri Lankan and Indian legal framework on the privacy rights in biometric identification. In addition, empirical research methodology was also used to gather information on the practical implication of the said discipline. Towards the end, this paper supports the argument that the right to privacy ought to be safeguarded as a constitutional right in Sri Lanka in the light of biometric identification while emphasizing the threats posed to privacy by the same.*

Keywords— **Right to Privacy, Biometrics, Human Rights, Biometric Identification**

I.INTRODUCTION

Biometric verification or identification, a process of detecting the physical or behavioural characteristics, is used to affirm ones identity (Syryamkim, et al., 2018). Alongside the information technology advancements it has gained an immense popularity around the globe (German & Baber, 2018).

In 2009, India has introduced an electronic identification system called Aadhaar, where citizens and residents are given a distinctive identification number based on their

biometric and demographic information (Perrigo, 2018). Sri Lanka on the other hand in year 2017 launched a smart identity card process which includes biometric data (Pradeep, 2017; Feranando, 2017; Lee, 2017).

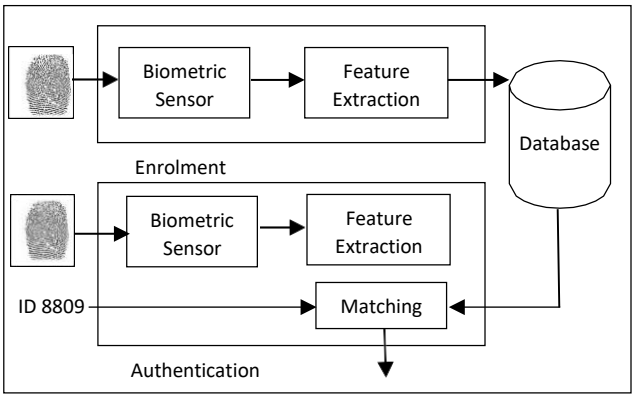

Figure 1. General Biometric System
Source: International Journal of Computer Applications
(Tripathi, 2011)

Majority of the people in the present world, without having to understand the outcomes, are compelled to undertake the biometric identification technology. Both information technology and legal professionals are yet to permit the utilization of biometrics on a large context, especially relating to privacy (Ashbourn, 2013). Understanding the legal perspective on this respect thus has become a necessity in today's world.

The novel technological concept of biometric identification has pushed us to ponder what is necessary to safeguard the fundamental human right of privacy and to guarantee the most favourable upshots for the citizens (Abeyaratne, 2019). Bearing in mind there are a number of possible biometric identification types, for instance hand geometry (measurements of fingers and palm), fingerprint (finger lines, pore structure), facial geometry (distance of specific facial features: eyes, nose, mouth), DNA (DNA code as the carrier of human hereditary features) et al, it is true that whether the utility of biometric identification leads to further risks or better privacy depends upon that specific type of biometric identification (Hert, 2005).Nevertheless it is also true that privacy concerns will be less likely to be

addressed when implementing the biometric identification in the absence of stern legal regulations (Abeyaratne, 2019).

The research revolves around the problem as to which extent the Constitutions in Sri Lanka and in India, fortify the right to privacy in biometric identification and what measures could be brought upon in order to enhance the constitutional privacy protection in Sri Lanka. Along with the research problem, this discipline addresses two primary questions; firstly, do Sri Lanka's and India's biometric identification systems violate the constitutional privacy protection? and secondly, what are the challenges posed to privacy due to the biometric identification?

This paper consists of two major objectives; first is to identify the existing constitutional provisions in Sri Lanka and India relating to right to privacy in biometric identification and second is to analyse the constitutionality of the Sri Lankan and Indian biometric identification systems.

As per the limitations, the subject matter of this discipline has limited to biometric identification opting out other concerns on the said technology such as biometric authentication, testing, surveillance and the like. Human rights concern of the right to privacy has only been considered in this paper although biometric technology itself carries numerous other legal issues. There exist different types of laws in different forms such as Acts, Ordinances, Bills relating to privacy and protection both in Sri Lanka and in India. Given that, this study only considers the constitutional provisions on that respect.

II. METHODOLOGY AND EXPERIMENTAL DESIGN

Black letter approach was utilized to entertain a thorough and objective analysis on the current Sri Lankan and Indian legal framework pertaining to right to privacy in a biometric identification perspective. Black letter approach was carried out based on relevant legislations as primary sources and books, journal articles, newspaper articles, commentaries, electronic resources pertaining to biometrics as secondary sources. Additionally, empirical research methodology was used to gather information on the pragmatic usage of the biometric identification. Empirical approach was furnished through conducting semi-structured interviews with stakeholders in the Information Technology Law regime such as lawyers, Information Technology Law lecturers.

III. BIOMETRIC IDENTIFICATION AND PRIVACY CONCERNS

Biometric identification, which has been obtained an immense popularity around the world in various forms, has originated from the Greek wordings bio ("life") and metric ("measurement") (Government Office for Science, 2018). Identification of biometrics has traditionally been based upon human procedures i.e. an individual comparing a

person's traits to those traits of a person that have been alternatively obtained (Luis-García, et al., 2003). Technological development has not only amplified the means of biometrical data which are readily available to collect, but it has also expanded the utilization methods of the same. Biometric identifiers are two fold; physical biometrics [fingerprint identification, hand geometry, face identification, Iris and retinal scan] and behavioural biometrics [speaker/voice recognition: analysing vocal behavior, signature/handwriting: analysing signature dynamics, keystroke/patterning: measuring the time spacing of typed words] (Government Office for Science, 2018). The utilization of biometrical data can be broadly categorized into four purposes: (i) permitting access to restricted areas (ii) confirmation of a service entitlement (iii) recording certain facts and materials and (iv) amalgamation of an activity with a person (Prabhakar, et al., 2003; Government Office for Science, 2018).

Biometric data, unlike passwords and other regular data protection methods, is highly unlikely to be forgotten or to be lost. Additionally the unique nature of such information which differs the same from one person to another, has resulted in a far-reaching belief that biometric recognition is ideal for identification purposes. However, the traits which make it an ideal platform for identification are the same traits which raise privacy concerns towards it. These concerns involve wrongful disclosure (replay attacks, spoofing), misuse of the data and theft (substitution attacks, masquerade attacks). There exists a high tendency that certain parts of the biometric identification systems getting replaced by a Trojan horse programme which ought to be a virus. Additionally, the primary detachment between the biometrics and applications, for instance overriding of the binary system output-Yes/No, paves the way to potential attacks. (Evans, et al., 2015)

Since identification could allow for the non-transparent surveillance of considerable number of people, generally, identification causes greater privacy issues than verification (Pagnin & Mitrokotsa , 2015).

IV. RIGHT TO PRIVACY IN SRI LANKA AND INDIA

At one end, chapter III of the Constitution of Sri Lanka is silent on right to privacy and at the other end, right to privacy failed to obtain a clear manifestation in the Constitution of India. Thus, purportedly, both Sri Lanka and India have not given much of a constitutional attention to this right. This is where judicial decisions come into play. At the outset, Indian Supreme Court in *M.P. Sharma* case decided that "when makers of the Indian Constitution as similar to American Fourth Amendment, has thought it is improper to attribute the discerning of the right to privacy as a fundamental right, there lies no rationale in singling it out as an entirely distinct fundamental right, by way of an exhaustive establishment" (M.P. Sharma and Others v

Satish Chandra, District Magistrate, Delhi and Others, 1954).

Deviating from the strict approach over constitutional privacy protection in *M.P. Sharma* case, *Kharak Singh* contended that "the right to personal liberty involves the freedom from restrictions on one's movements as well as the freedom from intruding into one's private life. Although Indian Constitution does not clearly set forth right to privacy as a fundamental right, it is necessarily a predominant component of individual liberty" (Kharak Singh v The State of Uttar Pradesh and Others, 1962). It is noteworthy that the courts in India were reluctant to unequivocally discern a fundamental right to privacy in here as well.

Indian Supreme Court in *Rajagopal* case, took the stance that the right to privacy is not propounded as a fundamental right in the Indian Constitution though it is more likely to be implied from Article 21 and held that a resident possesses a right to secure his individual privacy and also that of his family. Whether truthful or falsify and whether complementary or critical, no person is eligible to publish anything without the respected person's consent. The Court pinpointing an exemption to this situation stated that "when a case evolve into a public concern, privacy rights no longer prevails and press and media become legitimately eligible to comment. Nevertheless, in a dignity perspective (Article 19(2), Constitution of India) an exemption should be granted to this rule, i.e., a victim of a sexual assault, kidnap, abduction or a similar offence must no longer be abased in publishing the occurrence in press or media" (R. Rajagopal alias R.R. Gopal and Another v State of Tamil Nadu and Others, 1994). Hence, it is clear at this point that the Indian courts has surmised an implicit right to privacy behind the curtains of "individual liberty" under Article 21 of the Constitution.

Both *M.P. Sharma* and *Kharak Singh*, which were landmark cases deciding that the constitutional defence of privacy is not granted in India were overruled by the 2017 Supreme Court decision in *Puttaswamy*, which directly holds forth whether the Constitution of India entitles the right to privacy to be that of a fundamental right. *Puttaswamy* decision identified the significance of granting a constitutional protection to privacy rights via judicial interpretation by considering the characteristics and the scope of the liberties each person is entitled under the Indian Constitution. In order to interpret and initiate this right, Justice Chandrachud probed into Article 21 and declared that "the right to privacy is intrinsic to the right to life and liberty warranted to individuals through Article 21 and citizens possess a right to secure that privacy" (Justice K.S.Puttaswamy(Retd) and Another v Union Of India and Others, 2017). Justice Bobde further explained that "privacy and liberty are inherently linked in a manner that

privacy is the fundamental status required for exercising the right of personal liberty" (Justice K.S.Puttaswamy(Retd) and Another v Union Of India and Others, 2017).

On the other hand, it is unfortunate that the Sri Lankan Constitution, in its Fundamental Rights chapter does not furnish an explicit identification of citizens' right to privacy and also does not carry an equivalent provision to that of Article 21 of the Constitution of India.

In 1910, *Chinnappa* case identified a right to household privacy in upholding a Jaffna custom, where a landowner was allowed to cross over into the neighbour's land to screen his fence with leaves (Chinnappa et al v Kanakar et al, 1910). When perusing *Abraham* it is evident that Sri Lankan judiciary was intrepid to determine that not even an estate owner is eligible to enter the labourer's land intruding his privacy (Abraham v Hume, 1951). Sri Lankan Supreme Court, in *A.M.K Azeez* case, has reduced the appellant's sentence after observing that certain disrespectful statements were made to them by the police when the latter entered the former's house during the night suspecting them for stealing certain materials (A.M.K Azeez v W.T Senevirathne (S.I. Polce), 1966).

Nevertheless, it is noteworthy that when media and public has pressurized for more lucidity, the courts of Sri Lanka have successfully able compromise a stability between the right to privacy and freedom of expression (Article 14(1)(a), Constitution of Sri Lanka). In doing so, Sri Lankan courts have in certain circumstances expanded the freedom of expression to affect the right to information and the right to know. Given that, Justice Hector Yapa in *Sinha Ratnatunge* where the President was defamed, proclaimed that "the duty of the press should be to make the citizens more knowledgeable than in general. They must not manipulate their constitutionally protected right to freedom of speech and expression to intrude the citizen's privacy, based on the fact that the right to privacy does not falls under the umbrella of fundamental rights" (Sinha Ratnatunga v The State, 2001). His Lordship further went on to state that "the defamation law in both civil and criminal context upholds the right to human dignity subjecting to certain authority on the freedom of speech and expression. The press must not under the purview of its freedom of speech and expression make gratuitous invasions into the right to privacy, either of a lay man or even a public figure. Thus, the President as a public figure is capacitated to a justifiable amount of privacy to which the press is not permitted to interrupt" (Sinha Ratnatunga v The State, 2001).

From the above pronouncement of Justice Yapa, it is evinced that the current law in Sri Lanka only provide for a civil remedy against a privacy breach, found in the Roman Dutch Law known as actio injuriarum (Sooriyabandara,

2016). However, application of the said remedy is restrictive as numerous fulfilments are required for such a claim to be a success. Therefore, dissimilar to India, Sri Lankan right to privacy is not constitutionally supported.

V. CONSTITUTIONAL CHALLENGE ANALYSIS

Along with the implementation of Aadaar system in India, far-reaching concerns arose as to the enforcement and safeguarding of the right to privacy of the citizens in terms of collecting and storing such private information. Indian Supreme Court in 2017 whilst striving to address this issue held that one's right to privacy is intergral to the right to life and personal liberty and hence insinuated in Article 21 of the Constitution (Justice K.S.Puttaswamy(Retd) and Another v Union Of India and Others, 2017) i.e., the right to privacy was declared as a fundamental right (Bansal, 2017; Panday, 2017).

The concept of a regular identification database becomes constitutionally questionable, with the Indian Supreme Court holding privacy to be that of a fundamental right. Since there lies no extensive legal structure for the safeguarding of privacy rights and no clear-cut constitutional right to privacy in India, there arises a question whether the Indian government is violating the privacy rights of the individuals via Aadhaar (Panday, 2017). However, in 2018 the Indian Supreme Court divulged the Aadhaar system as constitutional (Mittal, 2018; Locker, 2018).

Informational privacy is one aspect of privacy. Indian government strikes to create an enthralling state interest which overrides the privacy protection, while weighing the sensitive balance between personal interests and a state's legitimate objectives. Intercept abandoning social welfare interests, safeguarding national security, crime inquiring and averting, motivating innovation and knowledge expansion involve the legitimate objectives of a state among others (Justice K.S.Puttaswamy(Retd) and Another v Union Of India and Others, 2017). Although these objectives of the state bear significance, a constitutionally protected privacy right should supersede such state aims.

It has been contended by the Indian Supreme Court that the Aadhaar Act, a money bill passed by the Parliament of India to provide legal backing to the Aadhaar project which provides for the interloping of Aadhaar numbers with bank accounts and other private services as constitutional. Although it imminently infringes Article 14-non-discriminative protection (The Wire Staff, 2017; Chaturvedi, 2018), Article 19(1)(d)-freedom of movement (The Wire Analysis, 2017), Article 19(1)(g)-career engagement (Bhatia, 2017) and Article 21-right to life and personal freedom (Koner, 2017) of the Indian Constitution. As per Article 141 of the Indian Constitution "Supreme Court's laws oblige every court within the national frontiers of India" (Bhatia, 2018), which means that the Supreme Court may grant an

order as is necessitated for acquiring justice and any order given shall implement across India.

Notwithstanding the fact that a decision of the Indian Supreme Court possesses a binding nature, its Article 13(2) may pronounce the Aadhaar Act unconstitutional by stating that "the State should not form any law which removes or curtails the fundamental rights secured via Part III of the Constitution and any law made breaching this clause, to the degree of that breach shall be invalid." By looking at this Article, it could be urged that a law that permits personal data collection without proper safety measures is in breach of the right to privacy in Article 21 and ought to be articulated invalid under Article 13(2). Thus, the Act should have been declared unconstitutional by the Puttaswamy court, which reflects the idea that, in contrary to the Indian Supreme Court's decision, Aadhaar system is unconstitutional and contravenes the right to privacy.

Across the Palk Strait, Sri Lanka had launched a programme to issue an electronic identity (e-ID) card including biometric data in 2017, in the absence of constitutional privacy or data protection (Pradeep, 2017; Feranando, 2017; Lee, 2017). Right to privacy stands behind the closed doors in the Sri Lankan Constitution. While scrutinizing Article 17 of the Constitution along with Article 126(1) it can be understood that an application relating the infringement of a fundamental right by executive or administrative action can be filed in the Supreme Court (Abeyaratne, 2019). A communal merit of privacy may extend to its utility to hinder the government and administrative bodies from exercising their discretionary powers (Solove & Schwartz, 2018). If the executive or an administrative body breaches a citizen's privacy rights through their actions, during an era of them being electronically active, such activity could be challenged in the Supreme Court, wholly if the right to privacy stands as a fundamental right (Abeyaratne, 2019).

There exist numerous situations in Sri Lanka where citizen's privacy rights have been deprived and offenders have excluded from their liability by putting forward the shield of national security or public order. This situation would have been different if the right to privacy was a fundamental right in Sri Lanka. If that is the case, the Supreme Court would have granted the relief prayed for by the complainant, except where such a suit falls within the sphere of Article 15(7) of Constitution which lays down the restricted circumstances that the fundamental rights could be overlooked (Abeyaratne, 2019).

Privacy could be categorised into information, communication, bodily privacy and territorial privacy (Electronic Privacy Information Center & Privacy International, 2001). Bearing that on mind, if privacy is looked upon from the point of view of expression as

secured by Article 14(1)(a) of the Constitution of Sri Lanka, it can be claimed that freedom of speech and expression sleeves up the right to privacy (Abeyaratne, 2019). On the flip side, if privacy is looked upon in terms of information which is warranted by Article 14A of the 19th Amendment to the Sri Lankan Constitution, it can be urged that right to information covers the right to privacy (Abeyaratne, 2019). Nevertheless, if public interest offsets the right to privacy, that right in turn offsets the latter. It is also notable at this point that this right which carries a huge weightage is attached to right to information and lacking teeth. This clearly does not explicitly indicate a provision where the right to privacy is a distinct and a well-established fundamental right in Sri Lanka. Furthermore, it is highly unlikely this right to be executed against private organisations, without a distinct statute being implemented.

Hence, in the absence of a fundamental right to privacy warranted by the Constitution, constitutionality of the Sri Lankan biometric identification system still remains sceptical and is at a stake if the constitutionality of the currently operated biometric identity card system is questioned as it did in India (Abeyaratne, 2019).

VI. RECOMMENDATIONS

Sri Lanka has to meet certain requirements to clinch citizens' privacy whilst implementing the electronic National Identity Card (e-NIC) system. Such requirements involve identification of the right to privacy as a fundamental right in the Constitution, formation of data protection laws and privacy intensifying policies and utilization of novel technologies augmenting privacy.

A. Novel Legislative Proposals

In the absence of a constitutional privacy protection, Sri Lanka should at a minimum level provide safeguards to the currently launched biometric Identification system as India has done through implementing the Aadhaar Act backing their Aadhaar identification system. In order for the e-NIC system to be a success, Sri Lanka should pass an exhaustive privacy legislation which caters judicial ameliorations and other implementation procedures to curb privacy breaches. Accordingly, the following must be incorporated in the new legislation,

1) explanations as to the criteria of collecting and storing the information of the individuals
2) proper judicial review of cases where data was gained or utilized in an inappropriate manner
3) clarifications as to the manner of utilizing personal information
4) lucidity of novel advancements, laws and polices

B. Privacy Enhancing Policies

Amongst certain policies followed by numerous states to abridge privacy challenges, data minimization plays an

important role. It demands the governmental entities to restrict the quantum of information ought to be gathered, enabling a data infringement notification which obliges such entities to notify the individual if personally recognizable data is dealt with.

In order to safeguard individual privacy, peculiarly from government abuse, Germany possesses a numerous policies. Certain policies constrain the technology by proscribing centralized database of biometric data or permitting the utility of incognitos for electronic contracts. Furthermore, biometric information in Germany is wholly used for identification purposes and is not permitted the use of the same to verify any other kind of information (Whitley & Hosein, 2016).

Data sharing by agencies and service providers could cause numerous threats to privacy. Data intermeddling between organizations generally enables tracking and permitting the data collected for a single objective to be utilized for distinct other objectives by leaving an electronic trail of one's activities. For instance, when an employer retrieves an employee's medical records, banking details among others, an interloping of databases could take place. Certain states adopt data controlling policies that particularly interdict linking numerous databases which includes personally recognizable information.

Belgium holds a stringent privacy structure for individual information. The Belgian Privacy Commission retain a stern authority on the utilization of individual data in public as well as private schemes whilst adopting ''ask once" principle for E-governance, that obliterate personal information submission to government agencies in many instances (Mariën & Audenhove, 2010).

In Austria, each individual e-ID card incudes a unique recognition number attached to the person's recognition in the Central Register of Residents. In order to prevent the databases from linking, this number is not utilized for transactions, rather an induction of this number is built which assists to secure personal data (Leitold, 2006; Polzer, 2007).

Policies should be designed in a manner that personal information is restrained or maintained appropriately to its purpose and utilized only to the degree incumbent for that event. Additionally, individuals must be eligible to require and receive their personal information and accommodated with ways and means of challenging such information. Revising or dissolving such data is necessary if the challenge is successful. German, Belgian and Austrian data handling policies could be implicated in Sri Lanka in appropriate levels to cater the privacy requirements in the biometric identification system in the country.

C. Privacy Enhancing Technologies

In order to reduce the privacy threats that may pose by the currently operating biometric identification system in Sri Lanka, following privacy enhancing technologies can be incorporated

Encryption is a method which converts readable information into an encoded form and protects the personal data in e-ID cards, transits, and information accumulated via a third force as a central database, from being non-authoritatively accessed. States may encrypt individual data included on an e-ID system to secure the information from manipulation (Rashmi & Shohreh, 2017). Access Control is a method which obstruct the interlopers and averting them from entering the resources through verifying them as unpermitted individuals based upon biometric authentication. In achieving the objective, this method requires to include a PIN to approve any data transfer through an e-NIC. This can not only control the release of data but also restrict the accessibility of data in an e-NIC (Bioenable, 2019).

Bio metric credential verification is another technique that e-ID systems could secure user privacy rather than supplying readable data. A verification mechanism can be utilized in order to mitigate the gathering and issuing subtle individual data. For instance, more than including a scanned image of a digitized fingerprint, an e-NIC may save several key features of the fingerprint permitting the system, a person's positive recognition (Dirjish, 2019).

VII. CONCLUSION

In 2018, the Indian Supreme Court, through *Puttaswamy* judgment proclaimed the biometric identification system-Aadhaar to be constitutional and decided that it could be an obligatory requisite for government services. Nevertheless, disregarding the binding nature of the said Supreme Court judgement, the compulsory intermeddling of Aadhaar numbers to bank accounts and other private services is deemed to be unconstitutional. If the Indian Supreme Court had declared the Aadhaar Act as an unconstitutional and was in breach of privacy rights, there would arise a probability of the Act being amended and re-executed with more enhanced privacy safeguarding measures. The consequences of such a decision would result in the Aadhaar system becoming the fundamental and compelling identification evidence in India-a single number linking citizens and residents to all agencies of the government. Whilst Aadhaar might initiate more coherent service distribution, it also unveil numerous of Indian citizens to cybercrime and possible privacy breaches.

Across the Palk Strait, Sri Lanka, in 2017, had initiated an e-NIC project which includes biometric data in the absence of constitutionally protected right to privacy. Albeit converting the existing national identity cards into a digital

formation generates probable advantages to the citizens, currently operating Sri Lankan e-NIC system neither reliable nor apt without guaranteeing the public privacy, data protection and well secured IT infrastructure. The fundamental requirement Sri Lanka has to consider when executing the e-NIC procedure is to identify the right to privacy as a fundamental right in the Constitution. Additionally, Sri Lanka should also look upon in creating an e-NIC application scheme with wide input from every stakeholder involving the private sector, formulate an e-NIC structure to assist both current and emerging technologies, warrant the privacy and data protection through the implementation of appropriate laws and policies and ensured accessibility and availability of e-NIC remedies to all the citizens.

ACKNOWLEDGEMENT

Authors convey their humble gratitude to Mr. Sunil D.B. Abeyaratne, Attorney-at-Law for his mentorship throughout the study.

REFERENCES

A.M.K Azeez v W.T Senevirathne (S.I. Polce) (1966) Justice T.S Fernando.

Abeyaratne, S. D., 2019. *Attorney-at-Law, LL.M, Commercial Arbitrator, Visiting Lecturer on ICT Law, Researcher of China-South Asia Law Research Center* [Interview] (06 April 2019).

Abraham v Hume (1951).

Ashbourn, J., 2013. *Practical Biometrics: from Aspiration to Implementation.* 2 ed. London: Springer London.

Bansal, S., 2017. *Privacy upheld as fundamental right: What term means for you, what's govt view.* [Online] Available at: https://www.hindustantimes.com/india-news/9-things-to-know-about-privacy-whatsapp-data-to-i-ve-nothing-to- hide-logic/story-804NFOPRPKAE2q7Z9vdtoI.html [Accessed 31 March 2019].

Bhatia, G., 2017. *The Constitutional Challenge to Aadhaar/PAN – III: The Petitioners' Rejoinder and the Issues before the Court.* [Online] Available at: https://indconlawphil.wordpress.com/tag/article-191g/ [Accessed 3 April 2019].

Bhatia, G., 2018. *The Aadhaar Judgment: A Round-Up.* [Online] Available at: https://indconlawphil.wordpress.com/tag/aadhaar/ [Accessed 03 April 2019].

Bioenable, 2019. *Biometric Access Control.* [Online] Available at: https://www.bioenabletech.com/biometric-access-control.html [Accessed 04 04 2019].

Chaturvedi, A., 2018. *The Key Arguments In Supreme Court Against Aadhaar.* [Online] Available at: https://www.bloombergquint.com/aadhaar/the-

key-arguments-in-supreme-court-against-aadhaar
[Accessed 3 April 2019].

Chinnappa et al v Kanakar et al (1910) Justice Grenier.

Dirjish, M., 2019. *Biometric Verification Solution Use Identity Proofing.* [Online] Available at: https://www.sensorsmag.com/components/biometric-verification-solution-use-identity-proofing
[Accessed 05 04 2019].

Electronic Privacy Information Center & Privacy International, 2001. *Privacy & Human Rights: An International Survey of Privacy Laws and Developments,* Wasington DC: Electronic Privacy Information Center.

Evans, N., Marcel, S., Ross, A. & Teoh, A. B. J., 2015. Biometrics security and privacy. *IEEE Signal Processing Magazine,* 32(5), pp. 17-18.

Feranando, V., 2017. *Smart IDs from today.* [Online] Available at: http://www.sundayobserver.lk/2017/10/29/news/nic-goes-digital
[Accessed 31 March 2019].

German, R. L. & Baber, K. S., 2018. *Current Biometric Adoption and Trends,* Texas: University of Texas at Austin.

Government Office for Science, 2018. *Biometrics: a guide.* 1 ed. London: Government Office for Science.

Hert, P. D., 2005. *Biometris: legal issues and implications,* Seville: IPTS.

Justice K.S.Puttaswamy(Retd) and Another v Union Of India and Others (2017) A Sikri.

Kharak Singh v The State of Uttar Pradesh and Others (1962) N R Ayyangar.

Koner, S., 2017. Constitutional Validity of Aadhaar: is it a violation of Right to Privacy?. *Journal on Contemporary Issues of Law ,* 3(7), pp. 1-11.

Lee, J., 2017. *Sri Lanka implements new biometric enrollment process for eID cards.* [Online] Available at: https://www.biometricupdate.com/201704/sri-lanka-implements-new-biometric-enrollment-process-for-eid-cards
[Accessed 31 March 2019].

Leitold, H., 2006. *Austrian Citizen Card.* London, E-Government Innovationszetrum.

Locker, M., 2018. *India Supreme Court says the world's largest biometric ID system doesn't violate privacy.* [Online] Available at: https://www.fastcompany.com/90242475/india-supreme-court-says-the-worlds-largest-biometric-id-system-doesnt-violate-privacy
[Accessed 03 April 2019].

Luis-García, R. d., Alberola-López, C., Aghzout, O. & Ruiz-Alzola, J., 2003. Biometric identification systems. *Signal Processing,* 83(12), pp. 2539-2557.

M.P. Sharma and Others v Satish Chandra, District Magistrate, Delhi and Others (1954) B Jagannadhadas.

Mariën, I. & Audenhove, L. V., 2010. The Belgian e-ID and its complex path to implementation and innovational change. *Identity in the information society,* 3(1), pp. 27-41.

Mittal, P., 2018. *SC upholds constitutional validity of Aadhaar, strikes down certain provisions.* [Online] Available at: https://www.livemint.com/Politics/eUH1dl06ly9otiDHqGNCfM/ Aadhaar-verdict-Supreme-Court-upholds-constitutional-validi.html
[Accessed 3 April 2019].

Pagnin, E. & Mitrokotsa , A., 2015. *Privacy-Preserving Biometric Authentication: Challenges and Directions.* New York, Springer-Verlag New York, pp. 169-182 .

Panday, J., 2017. *India's Supreme Court Upholds Right to Privacy as a Fundamental Right—and It's About Time.* [Online] Available at: https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its- about-time
[Accessed 31 March 2019].

Panday, J., 2017. *India's Supreme Court Upholds Right to Privacy as a Fundamental Right—and It's About Time.* [Online] Available at: https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its- about-time
[Accessed 31 March 2019].

Perrigo, B., 2018. *India Has Been Collecting Eye Scans and Fingerprint Records From Every Citizen. Here's What to Know.* [Online]
Available at: http://time.com/5409604/india-aadhaar-supreme- court/
[Accessed 31 March 2019].

Polzer, S., 2007. *The Austrian e-card as a Citizen Card (buergerkarte).* [Online]
Available at: https://joinup.ec.europa.eu/document/austrian-e- card-citizen-card-buergerkarte
[Accessed 05 04 2019].

Prabhakar, S., Pankanti, S. & Jain, A. K., 2003. Biometric Recognition: Security and Privacy Concerns. *IEEE Security and Privacy ,* 1(2), p. 33.

Pradeep, C., 2017. *NIC goes digital.* [Online] Available at: http://www.sundayobserver.lk/2017/10/29/news/nic-goes- digital
[Accessed 31 March 2019].

R. Rajagopal alias R.R. Gopal and Another v State of Tamil Nadu and Others (1994) Kumar Sumit.

Rashmi, J. C. & Shohreh, K., 2017. Biometric Encryption. *International Advanced Research Journal in Science, Engineering and Technology,* 4(8), pp. 16-19.

Sinha Ratnatunga v The State (2001) Justice Hector Yapa.

Solove , D. J. & Schwartz, P. M., 2018. *Information Privacy Law.* 6 ed. New York: Wolters Kluwer.

Sooriyabandara, V., 2016. Balancing the Conflict between Right to Privacy under Sri Lankan Fundamental Rights Perspective. *Sabaragamuwa University Journal,* December, 1391-3166(1), pp. 1-17.

Syryamkim, V. I., Kuznetsov, D. N. & Kuznetsova, A. S., 2018. Biometric identification. *IOP Conference Series: Materials Science and Engineering,* 363(1), p. 012005.

The Wire Analysis, 2017. *FAQ: What the Right to Privacy Judgment Means for Aadhaar and Mass Surveillance.* [Online] Available at: https://thewire.in/law/right-to-privacy-aadhaar- supreme-court
[Accessed 3 April 2019].

The Wire Staff, 2017. *The Aadhaar Debate: 'The State Has No Right of Eminent Domain on the Human Body'.* [Online] Available at: https://thewire.in/law/aadhaar-income-tax- supreme-court
[Accessed 3 April 2019].

Tripathi, K. P., 2011. A Comparative Study of Biometric Technologies with. *International Journal of Computer Applications,* 14(5), p. 12.

Whitley, E. & Hosein, G., 2016. *Global Challenges for Identity Policies.* 5 ed. London: Palgrave Macmillan UK.