***Ode to Aadhaar***

*Grass seemed greener on the Aadhaar side*
*Seduced by its spell, I got taken for a ride*
*Linking my card, not once but twice*
*Lulled by its lore and some lies*

*But soon I found*
*That Aadhaar was unsound*
*Privacy breaches and bunglings galore*
*Data pirates so desperate to score*

*My unique ID is now up in the air*
*Open to all, both foul and fair*
*Yet the "authority" insists that all is well*
*Link some more…and we'll all be swell!*

*To our courts therefore, I now do turn*
*For privacy, justice, and a little less burn*

**IN THE HIGH COURT OF DELHI AT NEW DELHI**

**EXTRAORDINARY CIVIL WRIT JURISDICTION**

**WRIT PETITION (CIVIL) NO. _____ OF 2018**

IN THE MATTER OF:-

**SHAMNAD BASHEER ...PETITIONER**

*versus*

**UNIQUE IDENTIFICATION AUTHORITY OF INDIA & ORS. ...RESPONDENTS**

**WRIT PETITION UNDER ARTICLE 226 OF THE CONSTITUTION OF INDIA SEEKING APPROPRIATE WRIT AND DIRECTION FOR DECLARATION OF BREACH OF THE FUNDAMENTAL RIGHT OF PRIVACY AND CONSEQUENT DAMAGES/DIRECTIONS PREVENTING FURTHER BREACH/DAMAGE AND FOR FORMULATION OF APPROPRIATE REDRESSAL MECHANISM**

**Most Respectfully Showeth:**

1. The Petitioner is filing the present petition under Article 226 of the Constitution of India before this Hon'ble Court for the redressal of the egregious violation of the Petitioner's right of privacy and dignity under Article 21 of the Constitution of India.

**THE PETITIONER**

2. The Petitioner is a citizen of India and a reputed legal scholar with over seventeen years of experience, particularly in the areas of Intellectual Property and technology law. He began his academic career in 2006 at the George Washington University Law School in Washington DC as the Frank H Marks Visiting Associate Professor of IP Law. He then served as the Ministry of Human Resource

Development Chair Professor in Intellectual Property Law at the West Bengal National University of Juridical Sciences, Kolkata from 2008-09 to 2013-14.

3. The Petitioner graduated from the National Law School of India University, Bangalore, and did his post-graduate studies including a doctorate from the University of Oxford as a Wellcome Trust Scholar. For his contributions to legal education and access to justice, he was awarded the Infosys Foundation Prize in 2014 by a jury headed by Nobel Laureate, Prof. Amartya Sen. The award citation commends his pioneering contributions to intellectual property law, legal education and access to law/justice. In late 2017, he won the Pirappancode Memorial Award for outstanding social justice lawyering. Most recently in February 2018, he was listed as one of the top ten '*lawyers who are changing the world for the better*' by Obelisk Support, a global legal service provider.

4. The Petitioner has been involved in public interest causes for a number of years. In 2010, the Petitioner founded IDIA ('**Increasing Diversity by Increasing Access to Legal Education**'), a non-profit pan India movement to train underprivileged students and help transform them into leading lawyers and community advocates. IDIA is premised on the notion that access to premier legal education empowers marginalized communities and helps them help themselves. The project is run on the backbone of highly

passionate student volunteers from various law schools, who travel across the length and breadth of India to identify marginalised students with an aptitude for the study of law. The selected students are rigorously trained to appear for the leading law entrance examination, namely Common Law Admission Test ('**CLAT**') and All India Law Entrance Test ('**AILET**'). IDIA further arranges for scholarships and adequate mentorship schemes to help candidates blossom to their full potential and take their rightful places as leading lawyers and community advocates.

5. In the last seven years, approximately 88 students trained by IDIA have secured admission to various law schools in India, and of this number, around 57 gained admission to the leading National Law Universities ('**NLUs**'). They reflect a truly diverse mix, comprising candidates from various backgrounds (children of farmers, stone quarry workers, truck drivers and clerks etc.) and hailing from various states. Further details on IDIA are available on its website: www.idialaw.com.

6. In 2011, the Petitioner founded P-PIL ('**Promoting Public Interest Lawyering'**), an informal coalition of law students, law teachers and lawyers to synergistically work towards shared public interest goals by filing public interest petitions and the like. A number of public interest petitions have resulted from the collaborative work of P-PIL, which is now housed within IDIA as a distinct vertical. These public-

spirited initiatives are also meant to augment the 'CHAMPS' training programme, which seeks to convert IDIA's underprivileged scholars into leading lawyers who are **C**reative, **H**olistic, **A**ltruistic and **M**averick **P**roblem **S**olvers.

7. The Petitioner has, in the past, proactively intervened and assisted the courts in matters of significant public importance. Notably, given the Petitioner's background and expertise in intellectual property law, the Petitioner assisted the Hon'ble Supreme Court in *Novartis v. Union of India* reported in (2013) 6 SCC 1 as an *intervener-cum-amicus* in the interpretation of Indian patent law. The apex court agreed with the key contentions of the Petitioner while handing down its path-breaking ruling denying patentability to an important anti-cancer drug. The scholarly writings of the Petitioner were also relied on by the Controller General of Patents in its decision dated 09.03.2012 in C.L. No. 1 of 2011 to grant India's first ever compulsory licence over an excessively priced patented anti-cancer drug in the post TRIPS era.

8. In 2015**,** the Madras High Court upheld a constitutionality challenge by the Petitioner against the Intellectual Property Appellate Board ('**IPAB**'), India's specialist IP tribunal, wherein the Petitioner had questioned the competence of IPAB adjudicators and the fact that the selection panels were predominated by members of the Executive. The court made it clear that all appointments to the IPAB

must be on constitutionally firm footing. Upon appeal of this decision by the Union of India, the Supreme Court declined to interfere, lending finality to the order of the Madras High court in favour of the Petitioner.

9. Apart from being personally aggrieved, the Petitioner is filing the present Writ Petition in the interests of general public as well, since many others have also signed up for a new age digital leash called "Aadhaar" and are likely to be similarly aggrieved.

10. There is no civil, criminal or revenue litigation, involving the Petitioner, which has or could have a legal nexus with the issue(s) involved in the instant petition under Article 226 of the Constitution of India.

11. The Petitioner has also not filed any other petition of a similar nature before any court of law in India.

**THE RESPONDENTS**

12. Respondent No.1 was established in January 2009 through an executive order of Respondent No.2, i.e., notification bearing no. A-43011/02/2009-Admin. dated 28.01.2009, as an attached office of the erstwhile Planning Commission. Respondent No.1 was established for the purpose of implementing "Aadhaar", a scheme originally meant to filter out fake identities and ensure the targeted allocation

of subsidies, benefits, and services to authentic beneficiaries. Central to the scheme was the collection of demographic/biometric data of Indian residents, which was then linked to a unique Aadhaar number issued to such residents. It is pertinent to note that at this time there was no statutory apparatus for the introduction or regulation of this project. This was despite the wide ranging implications the project had and continues to have on the fundamental rights of all citizens including invasive powers to be assumed by Respondent No. 1 in collecting and storing the private data of citizens across the country, including biometric data. Respondent No.1 was later conferred with a statutory status by way of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (referred to hereafter as the '**Aadhaar Act**').

**OVERVIEW**

13. Although conceptualized as a voluntary scheme, Aadhaar gradually morphed into a near compulsory mandate, with forced linkages to a slew of essential services, including banking services, filing of tax returns and cell phone subscriptions. Today, the Aadhaar scheme has become an all-pervasive force that has intruded into the lives of many including the Petitioner.

14. This transformation from a voluntary scheme to a compulsory mandate was engineered gradually with the active support of the

Respondents. Apart from banking, filing Income Tax Returns, LPG connections and the like, Aadhaar was made mandatory for other services/benefits such as health care, passports, scholarships, and even for getting marriages registered**.** A news report, which summarises some of the services for which Aadhaar linkage has been made mandatory is annexed herewith and marked **ANNEXURE P/1.** At present, the apex court has stayed some of the most controversial Aadhaar linkages (such as SIM cards and bank accounts), pending the disposal of the challenge to the constitutionality of the Aadhaar Act. Copies of the relevant orders dated 15.12.2017 and 13.03.2018 in WP (C) No. 494 of 2012 pending before the Hon'ble Supreme Court of India, staying the above mentioned linkages, are annexed herewith and marked as **ANNEXURE P/2 (colly).**

15. Given the all pervasive nature of Aadhaar, the privacy concerns of the Petitioner and countless other 'Aadhaaris' (a term of convenience used hereinafter to refer to all Aadhaar card holders) have increased manifold. By means of the instant Petition, the Petitioner does not intend to challenge the constitutional validity of the Aadhar Act, but is only seeking to establish that the Respondents continue to compromise the security of Aadhaar data through their negligent acts/omissions and consequently violate the fundamental privacy rights of the Petitioner and that of the public at large.

**FACTS**

16. The facts giving rise to the present Petition are as under:

i. The Petitioner, a professor of law, is an Indian citizen residing at Bengaluru.

ii. In 2015, the Petitioner, believing the Aadhar project to be safe, secure and consent based and applied for a unique ID (number) at an Aadhaar enrolment centre operating under the control and direction of Respondent No.1. As part of the enrolment process, the Petitioner was required to provide his biometric information in the form of all ten fingerprints, scans of both irises, and his facial image. Moreover, he also submitted most of his demographic information including his name, residential address, date of birth, e-mail address and mobile number. The Petitioner gave up such valuable personal and private information, in the sincere and honest belief that the Respondents possessed the necessary competence and capability to ensure that his data was secure and would not be compromised.

iii. After his Aadhaar enrolment, the Petitioner received numerous communications from various service providers, including his banks as well as the income tax department, informing him that it was now mandatory for citizens to link their Aadhaar numbers with their bank accounts and Permanent Account Numbers. The said correspondences also cautioned that failure to effectuate such

linkages would result in his bank account being rendered inactive or the income tax returns not being processed. Faced with the daunting prospect of an inactive bank account, the Petitioner made the requisite linkages with his PAN card and his bank account. The Petitioner made such linkages in the bona fide belief that the various agencies (public and private) were operating under the strict regulation of the Respondents (particularly Respondent No.1) and had the necessary capabilities for ensuring the security and safety of the Petitioner's private and personal data. In light of the Order dated 13.03.2018 passed by the Hon'ble Supreme Court (referred to above), the Petitioner has not yet linked his Aadhar card to other facilities / services such as his mobile number etc.

A copy of the order dated 13.03.2018 passed by the Hon'ble Supreme Court of India in WP (C) No. 494 of 2012 is also annexed herewith and marked as **ANNEXURE P/2(Colly).**

iv. Sometime around the beginning of 2018, the Petitioner was devastated to learn by way of a series of investigative press reports that the confidentiality of Aadhaar data and consequently his very privacy, personhood, and dignity had been breached, not once but several times over. He was particularly distressed to note that most of these breaches pertained to personal identity data maintained with the Central Identities Data Repository (referred to hereafter as the '**CIDR**'), a centralized database containing all information collected from Aadhaar applicants by Respondent No.1 and its

various affiliates/partners, including sensitive personal information such as biometric data.

v. The Petitioner fears that his valuable data (as also that of countless other Aadhaaris) is in the illegal possession of unauthorized third parties, who can, at any time, misuse it for their own personal gain. This fear is not just a theoretical one, but one which has played out in the past. A list of illustrative examples demonstrating such breach of Aadhaar data is annexed herewith and marked as **ANNEXURE P/3** which may be read as part and parcel of the present Petition.

vi. From the various accounts of breaches/lapses in the mainstream media, as also the responses and reactions of the Respondents to the same, it is evident that many of these critical breaches were on account of the negligence/willful recklessness on the part of Respondent No.1 to adopt reasonable security measures to secure the private personal information stored with it. The conduct of the Respondent No.1 is in blatant violation of the Aadhaar Act and associated regulations, as well as the Information Technology Act, 2000 (referred to hereafter as the '**IT Act'**) and associated rules. Quite apart from the above, the conduct of the Respondent No.1 and its various partners/affiliates and other third parties (whether authorized or unauthorized) is in violation of the Petitioner's

fundamental right to privacy; and actionable and compensable as a common law tort.

vii. In order to make for an easier perusal of this Petition, the pleadings are arranged under the following main headings:

(A) Security Breaches and Statutory Provisions Violated;

(B) Data Protection Duties under the law;

(C) Appointment of Investigative / Audit Committee;

(D) Constitutional / Common Law Rights and Damages;

(E) The Right to Know; and

(F) The Right to Legal Redressal.

## (A) SECURITY BREACHES AND STATUTORY PROVISIONS VIOLATED

viii. While innumerable breaches of Aadhaar data have taken place till date, only the most prominent ones (as ascertainable from credible reports, journal articles, government statements etc.) are recounted below for the sake of brevity. The same is only an indicative list of such breaches, being those that implicate the Respondents (and their various partners / affiliates) and their lapses / negligence in one way or the other, as available in the public domain. Apart from highlighting the breach itself, the Petitioner has also shown:

(a) How such breaches are likely to have resulted from the negligence of the Respondents and their affiliates / partners; and

(b) The provisions of law (the Aadhaar Act, the IT Act etc.) that are implicated.

**(A.1) <u>Breach-1: The Tribune Tragedy</u>**

ix. In January 2018, the Petitioner was shocked to learn that the Aadhaar data had been subject to one of the worst breaches, where unauthorised third parties could access the personal identity information of various Aadhaaris, including biometric information, for a paltry sum of Rs. 500/-. This shocking news came to light thanks to a rigorous undercover investigation and report by Rachna Khaira, a journalist from the 'Tribune' newspaper. The news report noted that the said journalist had obtained 'unrestricted' access to the data of more than 1 billion Aadhaaris in exchange for a mere Rs.500. In short, the reporter Rachna Khaira was able to access the identity information of any Aadhaari including their name, photo, phone number, and demographic details. To quote from her story:

> *"It took just Rs 500, paid through Paytm, and 10 minutes in which an "agent" of the group running the racket created a "gateway" for this correspondent and gave a login ID and password. Lo and behold, you could enter any Aadhaar number in the portal, and instantly get all particulars that an individual may have submitted to the UIDAI (Unique Identification Authority of India), including name, address, postal code (PIN), photo, phone number and email.*
>
> *What is more, The Tribune team paid another Rs 300, for which the agent provided "software" that could facilitate the printing of the Aadhaar card after entering the Aadhaar number of any individual.*

The Tribune report dated 03.01.2018 reporting the above breach is annexed herewith and marked as **ANNEXURE P/4**.

x. The Respondent No.1 acknowledged the said data breach in its press note dated 04.01.2018, noting that the: "*reported case appears to be an instance of misuse of the grievance redressal search facility. As UIDAI maintains complete log and traceability of the facility, the legal action including lodging of FIR against the persons involved in the instant case is being done.*" The press noted dated 04.01.2018 is annexed herewith as **ANNEXURE P/5**.

xi. Subsequent to the said press release, Respondent No.1 filed a First Information Report ('**FIR**') against, *inter alia,* the Tribune reporter, Rachna Khaira, and certain unknown persons, under Section 36 and 37 of the Aadhaar Act, Sections 419, 420, 468 and 471 of the Indian Penal Code and Section 66 of IT Act. The filing of FIR against the Tribune reporter and others was acknowledged by the Respondent No.1 itself in a press note dated 07.01.2018 and the same is annexed herewith and marked as **ANNEXURE P/6**.

xii. Based on all of the above, it would appear that:

- Access control to the CIDR was given to a certain set of people to *inter alia* enable them to function as authorized personnel who could update/correct entries in the Aadhar

database. This was purportedly done as a "*grievance redressal search facility*", and access control of the same were given to designated personnel and state government officials. These authorized personnel could then enter any Aadhaar number and access the private personal details of the Aadhaaris and effectuate the necessary changes.

- These access control details were "leaked". What made it worse was that the said access controls also permitted some authorized personnel to create multiple other accounts, using which each such subsequent account holder could access Aadhaar data on their own. Needless to say, it was only a matter of time before such a weak and vulnerable security architecture was exploited by those looking to make a quick buck.

- Till date, there appears to be no indication from Respondent No.1 on who exactly was responsible for this lamentable leakage of access controls; and the extent of privacy breach and damage caused to Aadhaaris whose data was compromised as a result.

xiii. It is evident that the systems and processes put in place by the Respondent No.1 did not even provide for the bare minimal level of security. As such, the Respondent No.1 ought to be held

accountable for its negligence/recklessness in failing to adopt reasonable security practices and procedures, in violation of its legal duties under the law.

**(A.1.1) Statutory Provisions Violated**

xiv. A number of statutory duties under both Aadhaar Act and IT Act, as well as their cognate rules and regulations, have been violated in the above instance, as detailed below:

**(A.1.1.1) *Application of Aadhaar Act and Associated Regulations***

xv. Section 28 of the Aadhaar Act places a specific duty on the Respondent No.1 to ensure the security and confidentiality of all identity information held by it, either directly or through its various partners/affiliates. In particular, Respondent No.1 is obligated to "*take all necessary measures*" to ensure that the information in its possession or control is secured and protected against any unauthorized access, use or disclosure. Respondent No. 1's obligation extends to even ensuring that there is no "*accidental or intentional destruction, loss or damage*" of data.

xvi. With a view to achieving the said objects, Respondent No. 1 has to "*adopt and implement appropriate technical and organizational security measures*" not only for itself but also for the various agencies, consultants, advisors or persons appointed or engaged for performing any functions under the Aadhaar Act. In other words,

Section 28 and the scheme of the Aadhaar Act make clear that Respondent No.1 is ultimately responsible for safeguarding the security and confidentiality of Aadhaar data.

xvii. It is evident that this duty under Section 28 of the Aadhaar Act has been breached by the reckless and grossly negligent actions/omissions of Respondent Nos. 1 and 2 and their officers in unleashing a very vulnerable privacy architecture that gave direct access to the CIDR database to so called "grievance redressal" personnel to effectuate changes as they pleased, and permitted such access controls to be multiplied manifold and disseminated widely.

xviii. Considering the sensitivity of the data as well as the complex ecosystem of the Aadhaar enrolment and authentication, which involves numerous third parties in the form of, *inter alia*, enrolment agencies, Authentication User Agencies (referred to hereafter as '**AUAs**'), and Authentication Service Agencies (referred to hereafter as '**ASAs**'), the legislature has also imposed the same set of security standards on all such parties who are acting on behalf of Respondent No.1 as per the requirements of Section 28(4) of the Act.

xix. The duty imposed on Respondent No.1 to ensure that third parties act in accordance with the security protocols is also discernible

from Section 23 of the Act. Under Section 23, Respondent No. 1 is obligated to "*develop the policy, procedure and systems for issuing Aadhaar numbers to individuals and perform authentication thereof*". Towards this end, the Respondent No.1 has the ability to call for information and records and conduct inquiries, audit and inspection of all concerned agencies connected with the implementation of the Aadhaar Act as also to frame regulations specifying various processes relating to data management, security protocols and other technology safeguards under the Act.

xx. Thus, Respondent No.1 is obligated to ensure that all third party partners/affiliates etc. are also subject to equally strong security procedures and practices for maintaining confidentiality of data under this Act. The powers of audit, inquiry and inspection are meant to enable the Respondent No.1 to effectively discharge its onus of satisfying itself that there are no breaches or potential breaches of such sensitive data. The Respondent No. 1 must be called upon to disclose how many such audits, inspections and inquiries it has conducted and to what effect.

xxi. Furthermore, Regulation 3 of the Aadhaar (Data Security) Regulations, 2016 (referred to hereafter as the '**Data Security Regulations**') requires the Respondent No.1 to provide an information security policy for itself and its personnel as well as its partners/affiliates. In particular, such security policy should *inter*

*alia* include and provide for (a) allowing only controlled access to confidential information; (b) a robust monitoring process to identify unusual events and patterns that could impact security and performance of information systems and a proper reporting and mitigation process; (c) encryption of data packets containing biometrics, and enabling decryption only in secured locations; (d) deploying necessary technical controls for protecting CIDR network; (e) measures for fraud prevention and effective remedies in case of fraud;

xxii. Although the said provision uses the word "may", it does indicate a set of appropriate standards to be complied with by an agency such as the Respondent No.1 who is a data controller/custodian of sorts. In fact, Respondent No. 1 calls itself a "data custodian", as is clear from the statement given in the following link: https://uidai.gov.in/component/fsf/?view=faq&catid=26.

A copy of the above webpage is annexed herewith and marked as **ANNEXURE P/7**.

xxiii. Moreover, given the mandate under Article 28 of the Aadhaar Act to adopt appropriate technical and organisational measures to ensure security of data, the above provision is evidently a mandatory obligation. Particularly so, since the right to privacy is a fundamental right under the Constitution of India.

xxiv. Furthermore, Rules 4 and 8 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (referred to hereafter as '**RSP Rules**'**)** enacted under Section 43A of the IT Act prescribe a similar requirement in mandatory terms. In pertinent part, they mandate that all body corporates are to deploy "*reasonable security practices and procedures*" to protect sensitive data within their systems. This will be dealt with more extensively in the section pertaining to the IT Act.

xxv. Respondent No.1 claims on its website and elsewhere that *"The UIDAI has a comprehensive security policy to ensure the safety and integrity of its data. It will publish more details on this, including the Information Security Plan and Policies for the CIDR and mechanisms for auditing the compliance of the UIDAI and its contracting agencies."* However till date, there is no independent confirmation that such policy exists and the Respondent No.1 has taken no steps to publish this policy or even make it available in court proceedings. A copy of webpage from the website of Respondent No. 1 as regards publication of information security plan and policies is annexed herewith as **ANNEXURE P/8**.

xxvi. As per the Rule 4 of the RSP Rules, Respondent No. 1 has to mandatorily publish the said security policy and it has failed in this

duty. The lack of such publication also leads one to infer that there is no such policy put in place by Respondent No.1.

xxvii. It is submitted that obligations in respect of securing Aadhaar data have been cast on various affiliates/partners of Respondent No. 1 as well, including the various service providers appointed to take care of the enrolment/updation process (including the so-called "*grievance redressal personnel*"). Illustratively, Schedule V of the Aadhaar (Enrolment and Update) Regulations, 2016 (hereafter referred to as the '**Enrolment Regulations**'), which lays down the statutory framework for Aadhaar enrolment and update, provides for a binding 'Code of Conduct for Service Providers'. Among the various obligations imposed on service producers, many including those stipulated by Clauses 17 (requiring service providers to ensure the security of data) and 23 (requiring service providers to abide by the security, confidentiality and security protocols put in place by Respondent No. 1) have been breached in the Tribune case.

xxviii. Moreover, the Data Security Regulations (and specifically Regulation 5) require all third party affiliates/partners to ensure that the Aadhaar data is not exposed to breaches. There is a clear and binding duty on all agencies who have access control to Aadhaar data to protect its confidentiality, privacy and security. More importantly, a concomitant duty is cast upon the Respondent

No.1 to ensure that such affiliates/partners adhere to their privacy and security commitments. Should there be any lapse on the part of such agencies, Respondent No.1 is duty bound to take action against them, including but not limited to, suspension of their activities and withdrawal of access controls. To the best of Petitioner's knowledge, till date, no penalty has been imposed on those personnel/affiliates of Respondent No.1 who were responsible for the Tribune Tragedy. It is further submitted that Respondent No.1 is also in violation of other requirements of Regulation 3 of the Data Security Regulations, in so far as it has failed to conduct an audit in the aftermath of the Tribune Tragedy.

xxix. From all of the above, it is clear that under the overall scheme of the Aadhaar Act, the ultimate duty/responsibility of securing Aadhaar data lies with Respondent No.1. Unfortunately, it has failed miserably in this task, as evidenced from the Tribune Tragedy and various other breaches outlined in this petition and in **ANNEXURE P/3**.

**(A.1.1.2)** ***Application of IT Act and Associated Rules***

xxx. Apart from liability under the Aadhaar Act, Respondent No.1 is also liable under the terms of the IT Act. Being a "body corporate" handling "sensitive personal data" under Section 43A of the IT Act, it is liable for losses flowing from its negligent handling of data.

xxxi. First, Sections 46 and 56 of the Aadhaar Act make clear that it does not exclude other remedies available under other laws. Secondly, the Aadhaar Act draws extensively from the IT Act, and many of the security standards applicable under the IT Act are in turn made applicable to the data collected under the Aadhaar Act. Illustratively, Section 30 of the Aadhaar Act stipulates that the provisions of the IT Act and associated rules shall apply to the "biometric information" collected under the Aadhaar Act and such information shall be deemed to be an "electronic record" and "sensitive personal data or information".

xxxii. Furthermore, Section 70 (4) of the IT Act imposes an obligation on Respondent No. 1 to prescribe adequate security practices and procedures for the protection of Aadhaar data. As per the said provision, any computer resource, which has been declared by way of an official gazette notification to be a "protected system", shall have security practices and procedures in place. By way of an official gazette notification dated 11.12.2015, Respondent No. 2 declared "*the UIDAI's Central Identities Data Repository (CIDR) facilities, Information Assets, Logistics Infrastructure and Dependencies Installed at UIDAI (Unique Identification Authority of India) locations to be Protected System for the Purpose of Information Technology Act 2000".*

A copy of the Notification dated 11.12.2015 is annexed herewith and marked as **ANNEXURE P/9**.

xxxiii. Therefore, Respondents Nos.1 and 2 are under a clear obligation to institute robust security practices and protocols to prevent breaches of Aadhaar data. Unfortunately, far from doing so, the Respondent Nos.1 and 2 have unleashed a perilously insecure system with loosely dispersed access controls and a very vulnerable privacy architecture.

**(A.1.2) Claim for Damages under IT Act**

xxxiv. Given that the Aadhaar Act does not preclude the applicability of the IT Act, Respondent Nos.1 and 2 are liable to compensate aggrieved Aadhaaris for security breaches under Section 43A of the IT Act for its negligence in implementing and maintaining reasonable security practices and procedures in relation to sensitive personal information and data, thereby causing wrongful loss or wrongful gain to individuals. It is explained below how each element of Section 43A has been fulfilled in the instant case.

**(A.1.2.1) *Sensitive Personal Information***

xxxv. The Respondent No. 1 is in possession and control of "*sensitive personal data or information*" of Aadhaaris, which as defined under Rule 3 of the RSP Rules, includes biometric information and

passwords. Section 30 of the Aadhaar Act also stipulates that biometric information is deemed to be "*sensitive personal data or information*" as defined by the IT Act and rules made thereunder, which provisions shall apply in addition to and not in derogation of the provisions of the Aadhaar Act.

xxxvi. Biometric information is in turn defined under Section 2(g) of the Aadhaar Act as a *"photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by regulations;" [emphasis supplied]*

xxxvii. It appears that the Aadhaar data that was accessed and made available to unauthorized third parties as per the Tribune reports included the photographs of Aadhaaris.

xxxviii. It is submitted that the Aadhaar number also qualifies as a "*password*", under Rule 2(h) of the RSP Rules, as it is in the nature of a "*secret key*" that one uses to "*gain admittance or access to information"* including demographic and other details of an individual including his/her photograph. This was evidenced in the Tribune Tragedy, where those with the relevant access controls (user name and password) could simply enter an Aadhaar number and gain access to demographic details and photographs of Aadhaaris hosted on the CIDR database.

xxxix. The harvesting of data by the illegal distribution of access controls (user name and password) in the Tribune Tragedy also highlights how the very architecture of Aadhaar permits the mere entry of an Aadhaar number as a "password" to access confidential demographic data of an Aadhaari.

**(A.1.2.2)** ***Negligence in implementing reasonable security standards and practices***

xl. To satisfy the second limb of Section 43A, it must be shown that the body corporate was negligent in implementing "*reasonable security practices and procedures*" in relation to such sensitive personal data. For a policy/system to constitute a reasonable security practice under Section 43A of the IT Act, it must be one that is *"designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force."* As such, the security standards outlined in the RSP Rules constitute reasonable security standards as under the above definition and are mandatorily applicable to the Respondent No.1 and any breach thereof is actionable under the terms of Section 43A of the IT Act. It is submitted that the Respondent No.1 and/or its various affiliates operating under its overall supervision have time and again, violated these important security standards. More specifically, the Respondents have breached the RSP Rules in three broad ways:

(a) They have failed to lay down an information security policy for itself and its core operations;

(b) They have failed to publish a privacy policy; and

(c) They have failed to abide by ISO Standards.

***Failure to Lay Down an Information Security Policy for itself and Core Operations***

xli. As per Rule 4 of the RSP Rules, Respondent No.1, as a body corporate, is required to publish a privacy policy which, lays down: a) clear and easily accessible statements of its practices and policies, b) the type of personal or sensitive personal data or information collected by it, c) the purpose of collection and usage of such information, d) the manner in which information including sensitive personal data or information is to be disclosed and e) its reasonable security practices and procedures.

xlii. It is submitted that Rule 4 is a mandatory obligation and Respondent No.1 has failed to comply with this mandate by not publishing on its website a comprehensive privacy policy and an an information security policy. It bears noting in this regard that as per Rule 8 of the RSP Rules, the published privacy policy shall provide for reasonable security practices and procedures.

xliii. As per Rule 8 (1) of the RSP Rules, a body corporate such as Respondent No.1 shall be considered to have complied with reasonable security practices and standards only if it has (a) implemented such security practices and standards and (b) has a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected.

xliv. Rule 8 of the RSP Rules further provides that in the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

xlv. Thus, on a conjoint reading of Rules 4 and 8 of the RSP Rules, it is clear that there is a binding obligation on Respondent No.1 to frame a comprehensive information security policy for safeguarding the data of Aadhaaris.

xlvi. To the best of the Petitioner's knowledge, Respondent No.1 has not disclosed the existence of any such comprehensive "information security policy", which applies to itself and its core operations. The only policy that is publicly available pertains to security

protocols/pre-requisites to be followed by the Respondent No.1's affiliates/partners, as below:

a) 'UIDAI Information Security Policy-UIDAI External Ecosystem-Authentication User Agency/KYC User Agency' (hereafter referred to as "**Affiliate Security Policy (AUA)**"); and

b) 'UIDAI Information Security Policy-UIDAI External Ecosystem-Authentication Service Agencies' (hereafter referred to as "**Affiliate Security Policy (ASA)")**

xlvii. As evident, these two policies (collectively referred to hereafter as '**Affiliate Security Policies'**) are applicable only to select affiliates i.e. registered AUAs, KUAs, ASAs and KSAs. It is relevant to note that they do not apply to the Respondent No. 1 itself or to its core operations and the secure maintenance of the CIDR database.

A copy of the said Affiliate Security Policies as available on the website of Respondent No. 1 is annexed herewith and marked as **ANNEXURE P/10 (Colly)**.

xlviii. It is submitted that this failure by Respondent No. 1 to lay down a comprehensive security policy also constitutes gross negligence and would have facilitated/enabled several breaches over the years, including the ones outlined in this petition.

***Failure to Publish Privacy Policy***

xlix. Apart from the failure to provide for a comprehensive information security policy, Respondent No.1 has also failed to fulfill another one of the mandates in Rule 4 of the RSP Rules: to publish a privacy policy on its website. The privacy policy that is presently available on the website of the Respondent No.1 is only a standard website policy and not the privacy policy, as envisaged under Rule 4 of the RSP Rules, for:

a) It does not provide details of the extent of storage and processing of the data which has been provided during the Aadhaar registrations;

b) There is no list of the types of personal data which is stored or the security practices deployed for their protection;

c) The policy does not provide any information on the procedure for disclosure or transfer of the sensitive personal information stored by the Respondent No.1 in their database; and

d) Most importantly, it does not disclose the existence of a comprehensive documented information security policy as required under Rule 8 of the RSP Rules.

A copy of the privacy policy available on the website of Respondent No. 1 at the link as follows is annexed herewith and marked as **ANNEXURE P/11** <**https://uidai.gov.in/home/privacy-policy.html-**>.

***Failure to Abide by ISO Standards***

l. The Respondent No.1 has also breached the mandate under the RSP Rules to comply with the relevant ISO security standards. More specifically, Rule 8(2) refers to the IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements" (hereafter referred to as the "**ISO Standard**") as one of the standards that would constitute a 'reasonable security practice' and Rule 8(4) makes clear that compliance with this standard would constitute deemed compliance with reasonable security practices and procedures.

li. Some of the key mandates under the relevant ISO security standard (ISO/IEC 27001:2013) are as below:

- establish, implement, operate, monitor, review, maintain and improve a documented Information Security Management System ("**ISMS**");
- establish and make available an information security policy document within the organisation and to interested parties;
- define and apply an information security risk assessment process that, inter alia, identifies the information security risks;
- report information security events through appropriate management channels as quickly as possible;
- conduct internal audits at planned intervals to provide information on whether the information security

management system is effectively implemented and maintained;

- plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting;
- top management to review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness;
- password management systems to be interactive and ensure quality passwords;
- access to program source code to be restricted;
- establish a policy on the use, protection and lifetime of cryptographic keys and it shall be developed and implemented through their whole lifecycle;
- networks shall be managed and controlled to protect information in systems and applications;
- information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification;
- privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable;

- establish a formal and communicated disciplinary process to take action against employees who have committed an information security breach.

liii. It is submitted that the Respondent No.1 and its affiliates/partners have failed to comply with a number of the above ISO standards, as is clear from the breach highlighted by the Tribune Tragedy. Significantly, it does not appear that any of the key employees or management personnel responsible for the Tribune Tragedy were identified and/or held accountable through a disciplinary process.

liii. Respondent No.1 is also under an obligation to ensure that an information security risk assessment process that, *inter alia*, identifies the information security risks, is implemented. The innumerable instances in which Aadhaar data has been compromised at the affiliate's/partner's end leads one to infer that the Respondent No.1 has failed to adhere to this standard.

liv. Lastly, it bears noting that the ISO Standard mandates periodic security audits. In particular, Clause 9.2, reads as below:

> *"The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:*
> *a) conforms to*
> *1) the organization's own requirements for its information security management system; and 2) the requirements of this International Standard;*
> *b) is effectively implemented and maintained.*
> *The organization shall:*
> *c) plan, establish, implement and maintain an audit programme(s),*

*including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;*
*d) define the audit criteria and scope for each audit;*
*e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;*
*f) ensure that the results of the audits are reported to relevant management; and*
*g) retain documented information as evidence of the audit programme(s) and the audit results."*

lv. Apart from the above, Rule 8(4) of the RSP Rules also mandates an annual audit of the "reasonable security practices and procedures" deployed by the Respondents. It bears noting that Respondent No.1 was established as a body corporate in the year 2009 and has been under an obligation to carry out regular audits since the said year. It is not clear if these audits were carried out regularly. In any case, no specific audits appear to have been conducted in the aftermath of any of the major breaches highlighted in this petition.

lvi. To the extent that there is no publicly available information on the extent of compliance (or breach) with any of the ISO security standards outlined above, the Petitioner prays that a committee be appointed to ascertain the robustness of the security systems and processes instituted by the Respondents.

lvii. Apart from the above violations, the Respondent No.1 is also liable for failing to put in place certain basic/fundamental tenets of a reasonable security policy. One such tenet is the principle of least privilege. The principle of least privilege (also known as the

principle of least authority) mandates that users of Information Technology systems be granted only those privileges (access controls etc.) that are absolutely necessary to complete the assigned tasks/functions. This principle works to limit the scope for unauthorized access and breaches and makes it easier to track/audit in the aftermath of a breach. By permitting a multitude of "grievance redressal personnel" to create multiple accounts, the Respondent No.1 blatantly flouted the above security safeguard. This grotesque failure was implicitly acknowledged by Respondent No.1, as access controls were restricted in the aftermath of the Tribune Tragedy. The news report indicating such access restriction is annexed herewith and marked as **ANNEXURE P/12**.

**(A.1.2.3)** ***Wrongful Loss/ Wrongful Gain***

lviii. The final limb to be established while asserting a claim under Section 43A of the IT Act is to prove a wrongful loss to the Petitioner or a wrongful gain to a third party at the expense of the Petitioner.

lix. In the Tribune Tragedy as well as the other breaches recited herein below, the net result has been that the Petitioner and others have been effectively divested of his private confidential data on account of the gross negligence of Respondent No.1 and its partners/affiliates in complying with the basic minimum security practices and procedures, as required under the law. Such actions

are admittedly theft of data and require to be dealt with severely and in the right earnestness.

lx. Moreover, the Hon'ble Supreme Court has recognized the right to informational self determination as an aspect of the right to privacy under Article 21 of the Constitution in *Justice KS Puttaswamy v. Union of India,* Writ Petition (Civil) No.494 of 2012 reported in (2017) 10 SCC 1 (referred to hereafter as "***Puttaswamy***"). The idea that individuals have property rights over their personal data, entitling them to control such personal data as they see fit, has gained widespread traction in international human rights jurisprudence. The following extract from a scholarly article (Christophe Lazaro, Daniel Le Metayer, *The Control over personal data: True Remedy or Fairy Tale?*, available at https://arxiv.org/ftp/arxiv/papers/1504/1504.03877.pdf) is instructive in this regard:

> *"Beside self-determination and self-management, informational privacy scholars have also conceptualized control and data subject's rights in terms of property. Indeed, an important part of the privacy literature has focused on property-based metaphors and descriptions to sustain the argument that a greater control over personal information could be achieved through market-oriented mechanisms based on individual ownership of personal data. According to this view privacy can be compared to a property right: "[P]rivacy can be cast as a property right.* ***People should own information about themselves and, as owners of property, should be entitled to control what it is done with it****"*

lxi. Apart from the wrongful loss suffered in terms of loss of control over his personal data, the Petitioner has also lost considerable

amount of time, energy and money on account of the various breaches, including having to change his email password etc.

lxii. As such, the Petitioner suffered a wrongful loss and is entitled to legal redressal under the Aadhaar Act and IT Act, including compensation.

**(A.1.3) Conduct of the Respondent No.1 and Lack of Legal Remedy**

lxiii. Far from redressing the various data breaches and putting in place measures to prevent such future lapses, the Respondents have attempted to cover up their gross negligence. Illustratively, when news of the Tribune Tragedy first broke, Respondent No.1, issued a press note dated 04.01.2018, claiming that "*data including biometric information is fully safe and secure*." This flies in the face of the reported breaches in the Tribune Tragedy incident. In the very same press note, the Respondent No.1 acknowledged that the "*reported case appears to be instance of misuse of the grievance redressal search facility"*. And that personal data such as "*name and other details*" have been compromised. These statements are a clear admission of the fact that the said breach involved the demographic data of various Aadhaaris. A copy of this press note dated 04.01.2018 is already annexed herewith and marked as **ANNEXURE P/5**.

lxiv. Further press statements by Respondent No.1 served only to exacerbate the confusion. In its press release dated 07.01.2018, the Respondent No.1, claimed that "*This is a case in which even though there was no breach of Aadhaar biometric database, because UIDAI takes every criminal violation seriously, it is for the act of unauthorized access, criminal proceedings have been initiated"*. It is submitted that this claim is contradictory, blatantly erroneous and reveals a deep ignorance of privacy law and principles. Firstly, the fact that photographs could be accessed with an Aadhaar number means that at least one portion of the biometric data housed within the CIDR database has been breached (by virtue of it being accessible to unauthorized third parties). Secondly, even assuming the said photographs (which count as "biometric" data under the Aadhaar Act) were not accessible, the fact remains that all other personal demographic data of Aadhaaris such as the petitioner were still "breached". The term "breach" in its ordinary usage refers to situations of unauthorized access to a database such as the CIDR. This press note dated 07.01.2018 is already annexed herewith and marked as **ANNEXURE P/6**.

lxv. Rather than taking responsibility for their poor security design, Respondent No.1 went on to initiate criminal prosecution against the Tribune reporter, Rachna Khaira who exposed this security scam. In this regard, it bears noting that Section 47 (1) of the Aadhaar Act precludes Aadhaaris such as the Petitioner from

initiating and filing a complaint in the event of a breach. Rather, such privilege vests solely with Respondent No. 1. Till date, no steps appear to have been taken against any of the Respondents' officials in the breaches described in this Petition.

lxvi. It is submitted that even in the absence of specific remedies in favour of the Petitioner under the Aadhaar Act, various common law doctrines provide scope for relief in instances such as this where privacy rights of the Petitioner and other Aadhaaris are severely compromised owing to the reckless/negligent acts of the Respondents, as outlined later in this petition.

**(A.2) Breach-2: Srivastava Spoof**

lxvii. Apart from the Tribune Tragedy outlined above, it appears that several other breaches of Aadhaar data have taken place. In one such instance, an unauthorized third-party application titled 'eKYC Verification' created by an entrepreneurial engineer, Abhinav Srivastava, carried out eKYC authentication transactions on the CIDR database (hereafter referred to as the "**Srivastava Spoof**").

lxviii. The eKYC Verification application (hereafter referred to as "**Srivastava App**") carried out these unauthorized transactions by spoofing an insecure application (referred to hereafter as the "**e-Hospital App**") built by the National Informatics Centre (referred

to hereafter as "**NIC/Respondent No.3"**) as part of its e-hospital management system. As evident from the term, "spoofing", in the context of network security refers to the practice of "*providing false information about one's identity in order to gain unauthorized access to systems*" or when "*communication is sent from an unknown source disguised as a source known to the receiver"*.

lxix. One of the features provided by Respondent No.3's e-hospital management system, through the e-Hospital App, was the Online Registration System (referred to hereafter as the "**ORS**"), which utilised the eKYC authentication services provided by Respondent No.1 to provide online appointments to members of the public at some of the leading government hospitals. Abhinav Srivasatava was able to successfully spoof the said e-Hospital App, as the same was made available for public download by Respondent No.3 on the popular platform 'Google Play Store'.

lxx. It bears noting that Respondent No.3 is a 'KYC User Agency' (hereafter referred to as '**KUA**') authorized to carry out eKYC authentication transactions using the CIDR database. It appears that Abhinav Srivastava exploited the security loopholes in NIC's e-Hospital App, particularly its vulnerable Application Programming Interface (hereafter referred to as "**API**") and key/token to gain unauthorized access to the CIDR database.

lxxi. From the various accounts of this breach in the public domain, it would appear that the modus operandi of Abhinav Srivastava was as follows:

(a) He downloaded the e-Hospital App and observed its working, both at the application front end and the server back end;

(b) Thereafter, he decompiled the relevant NIC software on the server backend and extracted its API and key / token;

(c) He then built his own application to facilitate Aadhaar authentications. This consisted of both a front-end mobile application (hosted in Google Playstore) and a back end server (hosted on Google's app engine- a cloud computing platform that allows hosting web applications). Abhinav Srivastava's back end server spoofed the e-Hospital App, such that the e-Hospital App's backend server could not differentiate a request between the Srivastava App and NIC's e-Hospital App.

lxxii. As mentioned above, Respondent No.3 is a KUA as well as a KSA (both being integral entities within the Aadhaar authentication ecosystem) working under the overall supervision of the Respondent No.1. More specifically, it operates as a licensee / affiliate of Respondent No.1.

lxxiii. It is submitted that the Srivastava Spoof was made possible owing to Respondent No.3's gross negligence in publicly disclosing the e-Hospital App and its API/key for reverse engineering/decompilation by a third party with basic software skills. Using this API, Abhinav Srivastava was able to construct his own application and spoof the e-Hospital App while it communicated with the Respondent No.1's server, pretending to be a licensed KUA such as Respondent No.3.

lxxiv. Apart from the above, Respondent No. 3, also breached other standard security protocols, including an abject failure to ensure that all communications via the e-Hospital App was secure. Specifically:

(a) The communication between the e-Hospital App and its backend server was through an insecure HTTP connection, rather than a secure HTTPS connection;

(b) Data packets were not encrypted and signed with keys as required under relevant Aadhaar regulations.

lxxv. In short, the Srivastava App mimicked or spoofed the working of the e-Hospital App and interfaced with the CIDR and carried out authentication transactions pretending to be Respondent No.3. An article explaining the methodology used to access the Aadhaar data by the Srivastava App is annexed herewith as **ANNEXURE P/13**.

lxxvi. Although Abhinav Srivastava was arrested on the basis of an FIR filed by the Respondent No.1, till date, it appears that no action has been taken against any of the personnel of the Respondent No.1 or Respondent No.3, which is a registered affiliate of the Respondent No.1, being a KUA and a KSA. This illustrates the utter callousness with which the Respondent Nos.1 and 2 has treated data security breaches. More so, since Respondent No.3's e-Hospital App and the relevant API and key/token were publicly accessible for at least 6 months between January and July, 2017, as understood from news reports. Also, the unauthorized access to the CIDR database by Abhinav Srivastava was prevalent for a good 6 months, before the breach was discovered in the first place.

**(A.2.1) Provisions Violated**

lxxvii. Apart from the various statutory provisions cited in the Tribune Tragedy above, the Srivastava Spoof also points to the following failures on the part of Respondent Nos.1 and 3:

(a) Failing to secure communications through HTTPS and signing the relevant data packets;

(b) Failing to secure the API as well as its token/key;

(c) Failing to systematically audit and track breaches; and

(d) Failing to deploy a fraud analytics system.

**(A.2.1.1)** ***Failure to secure communications through HTTPS and sign the relevant data packets***

lxxviii. From the Srivastava Spoof, it is clear that Respondent No.1's affiliate, NIC (which is a registered KUA and KSA) failed to secure its communications, making it accountable for one of the most egregious breaches of Aadhaar data.

lxxix. In this regard, it bears noting that the Aadhaar (Authentication) Regulations, 2016 (hereafter referred to as the "**Authentication Regulations**") lay down the precise process to be followed by requesting entities while transmitting an authentication request to the CIDR. Clause 9 of these regulations clearly mentions that all such transmissions must first be packaged into 'PID' blocks, and then have to be encrypted, signed and transmitted using a secure protocol (as may be specified by Respondent No. 1 for this purpose), which was clearly not followed by the Respondent No. 3.

lxxx. As per Clause 9 of Authentication Regulations, the CIDR is then required to *"validate the input parameters against the data stored therein and return a digitally signed Yes or No authentication response, or a digitally signed e-KYC authentication response with encrypted e-KYC data, as the case may be, along with other technical details related to the authentication transaction".*

lxxxi. A reasonably secure communication protocol and process as per the above would at the very least have entailed the client application (e-Hospital App in this case) sending the request to its

back end server through a 'secure protocol'. As per the specifications laid down by the Respondent No.1 in March 2018 *vis a vis* Aadhaar authentication applications, the secure protocol to be used by authentication applications is HTTPS.

lxxxii. Far from doing this, NIC hosted its e-Hospital App on an insecure 'HTTP' connection rather than an 'HTTPS' connection, effectively rendering all communications insecure. It also failed to encrypt the data packets using keys as required under the above Authentication Regulations.

lxxxiii. Further, paragraph 2.11 of the Affiliate Security Policy (AUA) mandates that the network between the AUA / KUA and ASA / KSA should be secure private lines, or in the case of a public network, should be via a secure channel such as SSL or VPN and that the AUA / KUA server should block any requests other than the ones coming from AUA / KUA PoT terminals.

lxxxiv. By not adhering to the above policy, Respondent No. 3 has not only explicitly violated the minimum security standards, but also committed gross negligence in rendering the data of Aadhaaris vulnerable to breach.

**(A.2.1.2)** ***Failure to secure the API as well as its token/key***

lxxxv. Respondent No.3 contributed significantly to the Srivastava Spoof by making its API and relevant key/token publicly susceptible to reverse engineering and accessible on Google 'Play Store'.

lxxxvi. Specifically, Respondent No.3 violated Regulation 17 (1) (f) of the Authentication Regulations which obligates all requesting entities to ensure that "*the private key used for digitally signing the authentication request and the license keys are kept secure and access controlled".*

lxxxvii. Amongst other things, the actions of Respondent No.3 also violate paragraph 2.8 of the Affiliate Security Policy (AUA), which requires the requesting entities to protect the keys throughout their lifecycle including the aspects of "*key generation, key distribution, and secure key storage".*

lxxxviii. Thus, by making the vulnerable API along with its key publicly accessible, Respondent No.3 was in gross violation of its statutory duties listed above. Moreover, it is also in breach of Regulation 14 (m) of the Authentication Regulation, under which a requesting entity is responsible for all its authentication operations and results and ensuring compliance with the standards and specifications laid down by Respondent No.1.

lxxxix. Regulation 25 of the Authentication Regulations imposes liability upon requesting entities in cases of default, i.e., where the requesting entity:

> *"(a) fails to comply with any of the processes, procedures, standards, specifications or directions issued by the Authority, from time to time;*
> *(b) is in breach of its obligations under the Act and these regulations;*
> *(c) uses the Aadhaar authentication facilities for any purpose other than those specified in the application for appointment as requesting entity or ASA;*
> *(d) fails to furnish any information required by the Authority for the purpose of these regulations; or*
> *(e) fails to cooperate in any inspection or investigation or enquiry or audit conducted by the Authority."*

xc. In such scenarios, Respondent No. 1 is empowered under to, *inter alia*, suspend the activities of a requesting entity or agency, terminate its appointment and impose other disincentives upon them. Such action can also be taken against *"any entity or agency with which an AUA has shared its license key for Yes/ No authentication and any entity with which a KUA has shared e-KYC data".*

xci. Such power to initiate action against requesting entities is also provided by way of a circular dated 28.02.2017 issued by the Respondent No.1, which stipulates that the "*AUA/KUA shall be fully responsible for the misuse and illegal sharing of the license key in production or pre-production environment of UIDAI. AUA/KUA shall not allow any other agency to perform authentication by sharing their license key*." The Circular then goes on to state that "*In case, Authority notices misuse or illegal sharing of license key by the AUA/KUA/sub-AUA, Authority shall terminate the license of AUA/KUA and other actions including criminal prosecution shall be*

*taken against AUA/KUA as well as the sub-AUA and other entities as per the Aadhaar Act and its Regulations."*

A copy of Circular dated 28.02.2017 is annexed herewith and marked as **ANNEXURE P/14**.

xcii. By allowing the Srivastava App to gain unauthorised access to its server / API / Key and misuse its authentication privileges, Respondent No. 3 has fallen foul of the above direction, which is binding on NIC by virtue of Regulation 14 (n) of the Authentication Regulations.

xciii. The actions of Respondent No.3 are also violative of the relevant requirement on access controls under paragraph 2.6 of the Affiliate Security Policy (AUA), which only permits access to information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) to authorized individuals.

xciv. Furthermore, Respondent No.3 is also in breach of Regulations 3 and 5 of the Data Security Regulations as well as the Affiliate Security Policy, which require requesting entities to ensure that appropriate controls are implemented to prevent and detect any loss, damage, theft or compromise of the software assets.

**(A.2.1.3)** ***Failure to systematically audit and track breaches***

xcv. As per Regulation 6 of the Data Security Regulations, all agencies, consultants, advisors and other service providers engaged by the Authority, and ecosystem partners such as registrars, requesting entities, Authentication User Agencies and Authentication Service Agencies are required to get their operations audited by an information systems auditor certified by a recognised body under the Information Technology Act, 2000 and furnish certified audit reports to the Authority, upon request or at time periods specified by the Authority. As per this provision, Respondent No. 1 is also empowered to conduct or direct such audits.

xcvi. Similar obligations, including monitoring of audit logs, have been laid on requesting entities by way of Clause 13 of the Affiliate Security Policy (AUA) which policy is binding upon Respondent No. 3, which is a KUA / KSA.

xcvii. Regulation 21 of the Authentication Regulations also confers wide powers on the Respondent No.1 to conduct audits of *"the operations, infrastructure, systems and procedures, of requesting entities, including the agencies or entities with whom they have shared a license key or the entities on whose behalf they have performed authentication, and Authentication Service Agencies"* to ensure that such entities are acting in compliance with the regulatory apparatus governing their actions.

xcviii. On detection of any deficiencies, Respondent No. 1 is also empowered to direct the concerned entity to furnish information as to its activities and may also require such entity either to rectify the deficiencies or take action as specified in these regulations.

xcix. Despite the above, it is not clear if the audit provisions outlined above were ever complied with by Respondent No.3 and the extent to which Respondent No. 1 monitored compliance with this important mandate. It bears noting though that Respondent No.1 had issued a circular dated 28.02.2017, whereby all AUAs and KUAs were instructed to, *inter alia*, audit their authentication applications and submit an audit report to the Respondent No.1 by March 31, 2017. It is relevant to note that the Srivastava Spoof took place during the time period between January-July 2017 and the breach was not detected till as late as July. Thus, it is reasonable to infer that either no audit was undertaken or that the said breach was intentionally covered up. This sequence of events points to an alarming lack of due diligence and oversight on the part of the Respondent No.1 as well as its affiliates/partners, Respondent No.3 in the case. The circular dated 28.02.2017 is already annexed herewith and marked as **ANNEXURE P/14**.

**(A.2.1.4)** ***Failure to deploy a fraud analytics system***

c. The Srivastava Spoof also points to the failure of Respondent No.3 to deploy a Fraud Analytics System / Module, as recommended under the Affiliate Security Policy (AUA) as well as the Authentication Regulations. Regulation 3 of the Data Security Regulations stipulates that Respondent No. 1 may prescribe an information security policy setting out inter alia the technical and organisational measures (including monitoring processes) to be adopted by Respondent No. 1 and its personnel, and by agencies, advisors, consultants and other service providers engaged by Respondent No. 1, registrar, enrolling agency, requesting entities, and Authentication Service Agencies. Needless to state, such a policy ought to include monitoring processes that are capable of identifying unusual events and patterns that could impact the security of the information systems.

ci. In fact, under paragraph 2.13 of the Affiliate Security Poli**cy** (AUA), AUAs / KUAs are advised to deploy a Fraud Analytics Module, capable of analyzing authentication related frauds. Furthermore, Regulation 14 (1) (l) of Authentication Regulations also refers to the Fraud Analytics System and mandates the requesting entity to inform the Respondent No.1 of any fraud pattern that is detected. Respondent No.3's calamitous failure to detect the breach for almost 6 months points to a severe lapse, and a strong inference of the absence of a formidable Fraud Analytics Module / system.

cii. The fact that Srivastava App was able to send unlimited number of eKYC authentication requests without being detected indicates that neither Respondent No. 3 nor Respondent No.1 had a robust monitoring process that could identify unusual events and patterns as required under the above Data Security Regulations.

**(A.2.2) Other Violations**

ciii. The actions of Respondent No.3 are also in violation of the ISO Standard, applicable under the terms of the IT Act and discussed earlier in the context of the Tribune Tragedy. Specifically, apart from the audit related provisions, Respondent No. 3, NIC, is also in violation of the security standards in relation to password management, access to program source code etc.

civ. Moreover, as was the case with the Tribune tragedy, the concerned personnel involved in facilitating the breach or whose negligence led to the breach have not been identified and subjected to penalties or at the very least, a disciplinary process. Amongst other things, this violates the ISO Standard requirement that disciplinary proceedings be initiated against employees who have committed an information security breach.

cv. Lastly, the Srivastava Spoof also amply illustrates the inherent flaws in the security and privacy architecture engendered by

Respondent Nos. 1 and 2. One of the fundamental principles of a sound data protection regime is that of "data minimization", as per which no more personal data than is necessary ought to be transmitted to third party agencies (requesting entities in the Aadhaar ecosystem). As evident from the Srivastava Spoof, while carrying out eKYC authentications, the demographic information of the Aadhaaris is transmitted to the requesting entity, thus exposing their personal details to third parties and making them vulnerable.

**(A.2.3) Action against NIC**

cvi. Despite the shocking lapses on the part of Respondent No.3, Respondent No.1 has failed to initiate any action against it. This despite the fact that the Respondent No.1 has ample powers to initiate action against Respondent No.3, including terminating its license. These powers flow from Regulation 25 of the Authentication Regulations as well as the Circular dated February 28, 2017.

cvii. By enabling an unauthorized third party to access identity information of several Aadhaaris through a vulnerable API application, Respondent No.3 breached a number of important security safeguards and statutory obligations. Similarly, by failing to supervise and monitor Respondent No. 3 for potential breaches,

and then failing to take action once the breach was discovered, Respondent No.1 is also in violation of its statutory duties.

cviii. As such, a direction may be issued to the Respondent No.1 to initiate appropriate action against Respondent No.3, including the filing of a criminal complaint before the appropriate authority, for its failure to adhere to the security practices and provisions under the Aadhaar Act and the IT Act. An immediate audit must also be ordered such that all those affected are able to ascertain the extent and scope of the breach and the potential for damage to their personal identity, dignity and privacy as a result of this breach.

cix. Apart from culpability on the part of Respondent No.3, it is submitted that Respondent No.1 is strictly liable for the above breach, as it is bound by a strict standard under Section 28 of the Aadhaar Act, which casts liability for even accidental losses.

**(A.3) <u>Breach-3: Publication of Aadhaar Data</u>**

cx. A report published in May 2017 by the Centre for Internet and Society, a reputed think tank (hereafter referred to as '**CIS**'), showed that a number of websites of central and state governments publicly disclosed the private information (including Aadhaar numbers and bank accounts) of more than 130 million Aadhaaris.

The CIS report dated 16.05.2017 containing details of the said illegal public disclosure is annexed herewith as **ANNEXURE P/16.**

cxi. Further, in another instance, it was reported that 210 different websites, a majority of them belonging to the central and state government agencies/departments, publicly displayed the personal data of the Aadhaar beneficiaries including their names, addresses, and Aadhaar numbers. This was admitted in a reply to unstarred question no.1364 in the Rajya Sabha by the Minister of State for Electronics and Information Technology, on December 29, 2017. The reply given by the Minister dated 29.12.2017 is annexed herewith as **ANNEXURE P/17**.

**(A.3.1) Provisions Violated**

cxii. The actions of the various affiliates/partners of the Respondents in publishing the confidential identity information of Aadhaaris is in gross violation of the Act and associated regulations, which prohibit unauthorized disclosure of personal identity information, including Section 28 of the Aadhaar Act. The term "*identity information*" is defined in Section 2 (n) of the Aadhaar Act to include an individual's Aadhaar number, biometric and demographic information. Thus, there is an obligation to secure not only the biometric information, but also other *identity information* such as the Aadhaar number and related demographic information.

cxiii. Moreover, as per Section 29 (3) (b) and Section 29 (4) of the Aadhaar Act, identity information cannot be further disclosed other than with the prior consent of the individual; nor can it be published, displayed or posted publicly, or used for any purpose other than for purposes specified by the regulations.

cxiv. It is further submitted that Regulation 6 of Aadhaar (Sharing of Information) Regulations, 2016 (referred to hereafter as "**Sharing of Information Regulations**") precludes the publishing, displaying or publicly posting the Aadhaar number of an individual. Similarly, Regulation 4(2)(b) and Regulation 5 (3) of the Sharing of Information Regulations prohibit a requesting entity and any entity other than requesting entity from sharing Aadhaar data without the consent of the Aadhaaris.

cxv. Such illegal disclosure also contravenes Rules 6 and 7 of RSP Rules which prohibit all data custodians such as Respondent No.1 from disclosing or transferring sensitive personal information to third parties without the express consent of data subjects and only after ensuring that such third parties maintain the same level of security practices specified in the Rules. Lastly, Respondent Nos. 1 and 2 (as well as their affiliates/partners) are also in violation of the ISO Standard, which requires that the privacy of the personally identifiable information be secured.

cxvi. From all the above, it is clear that overall, Respondent No.1 has failed miserably in securing the sensitive personal information as mandated under Section 28 of the Aadhaar Act. The Respondent Nos.1 is also liable under Section 43A of the IT Act and have to compensate all affected Aadhaaris whose sensitive personal information was breached. As explained in detail in the section on the Tribune Tragedy, sensitive personal information includes even Aadhaar numbers (which qualify as "passwords").

**(A.3.2) Cover Up and Conduct of Respondent Nos.1 and 2**

cxvii. Here again, rather than notifying data subjects of the breach and taking steps to redress it, Respondent Nos.1 and 2 have been more keen on covering up their own lapses/negligence. As per Respondent No. 1's press release dated 20.11.2017, the placing of personal data by 210 websites in the public domain was "*a measure of proactive disclosure under the RTI Act by the government and institutional websites…*". Nevertheless, in the very next paragraph, it is mentioned that "*UIDAI and Ministry of Electronics & IT had directed the concerned Government departments/ministries to immediately remove it from their websites and ensure that such violation do not occur in future.*" Thus, Respondent No.1 while acknowledging that such public disclosure is a "*violation",* simultaneously attempted to defend it on flimsy grounds. The same displays a woeful lack of accountability on the part of

Respondent Nos. 1 and 2 and an attempt to cover up its gross negligence / willfulness in compromising the security of Aadhaar data. In any case, the attempt to justify the illegal disclosure as a "*proactive disclosure under the RTI Act*" is completely unfounded, as the websites disclosing the data included entities that are not subject to RTI norms.

A copy of press release dated 20.11.2017 issued by Respondent No. 1 is annexed herewith and marked as **ANNEXURE P/18**.

cxviii. In fact, Respondent No. 1, in its press note dated 04.01.2018 (**ANNEXURE P/5**) stated categorically that "*Aadhaar number is not a secret number*." A sentiment that appears to have been echoed by a Minister as well, who spoke of the need to make Aadhaar numbers and data more "public"; arguing that the public display of "private" confidential data was *inter alia*, for the "*information of general public*" , a sentiment that resonated with Respondent No.1's claim in its press release dated 20.11.2017 that this disclosure was a noble "*measure of proactive disclosure under RTI Act".*

cxix. These statements demonstrate an utter lack of legal awareness of privacy rights, which are not mere legal rights in India, but fundamental rights guaranteed under the Constitution.

**(A.4) <u>Breach-4: The Biometric Frauds</u>**

cxx. Notwithstanding the repeated assertions by the Respondent No.1 that Aadhaar biometric data is safe, it is clear that the truth is otherwise. Apart from the Tribune Tragedy and the CIS Report mentioned earlier, Aadhaar affiliates/e-KYC user agencies such as Axis Bank Limited along with its banking correspondent Suvidhaa Infoserve Private Limited, and eMudhra Limited, were found to have illegally stored and replayed Aadhaar biometric data.

cxxi. The said breach was not a one-off instance, but continued for more than 6 months from July 14, 2016 up until February 19, 2017. Interestingly, the breach was admitted by Respondent No.1, which issued show-cause notices to each of these errant entities under Regulation 25 of the Authentication Regulations on February 20, 2017 ("**Notice**"). The Notice specifically alleged that these ecosystem partners violated the Aadhaar Act and associated regulations by illegally storing biometric data and carrying out multiple concurrent transactions using the same Aadhaar number. It then went on to explicitly note that the actions of the affiliates posed a "*grave threat…. to the privacy of biometrics of people*". Moreover, Regulation 7(2) of the Authentication Regulations (which imposes an obligation on requesting entities to encrypt and secure the biometric data at the time of capture) was cited as one of the breached provisions.

cxxii. The Respondent No.1's callousness in securing the data of Aadhaaris and complying with its statutory and other legal obligations is more than amply evidenced through its delay in issuing the show cause notice, i.e., on February 20, 2017, roughly a month after the first illegal authentication transaction had taken place. News reports dated 24.02.2017 and 02.03.2017 highlighting the breach are annexed herewith as **ANNEXURE P/19 (Colly).** Respondent No.1's clarification of the incident by way of a press note dated March 5, 2017 is annexed herewith as **ANNEXURE P/20.**

cxxiii. Although Respondent No.1 appears to have made it mandatory for all the Aadhaar ecosystem partners to transition to "registered" biometric devices by June 2017 so as to prevent future breaches of this sort, multiple extensions were given thereafter for compliance with the said requirement. As on date, it is not clear if the requirement of deploying registered biometric devices has been fully complied with and is being enforced. In fact, as per the latest affidavit submitted by the Respondent No.1 to the apex court in the constitutionality challenge, entities like "*banks, PDS etc.*" are still at "*various stages of implementing RD in their systems.*"

The latest Circular dated 02.02.2018 mandating transition to registered devices, and reflecting the various extensions already granted, is annexed herewith and marked as **ANNEXURE P/21**.

cxxiv. In any case, the decision to transition to registered biometric devices has been taken belatedly, after many of the privacy breaches/abuses have taken place. In this connection, cyber security expert Dr. Rakesh Goyal has also opined that the biometric devices used in the Aadhaar ecosystem are extremely vulnerable to hacking, data theft, and in some cases even appeared to store the biometric data, in contravention of the statutory framework.

cxxv. Other instances involving misuse of Aadhar biometrics have been described in detail in **ANNEXURE P/3.** All of these incidents demonstrate the extremely weak and vulnerable nature of the Aadhaar privacy architecture and the immense scope for breaches; lending weight to the Petitioner's claims that his data (as well as that of countless other Aadhaaris) is now up for grabs and subject to the serious risk of identity theft and other kinds of abuse at the hands of third parties.

**(A.4.1) Provisions Violated**

cxxvi. In the above instance of 'replay attacks', the AUAs were in violation of Regulation 7(2), 9(5) and 17(1) of the Authentication Regulations, which, *inter alia*, prohibit storing and retaining of any copies of the biometric information by Requesting Entities. Moreover, as per Regulation 4(1) of the Sharing of Information Regulations, core biometric information captured by a requesting

entity from the Aadhaar number holder cannot be stored. Here again, it is submitted that the liability of the intermediaries ought to be read along with the obligation on the Respondent No.1 to secure all Aadhar identity information under Section 28 of the Aadhaar Act as well as the ISO Standards.

**(A.5) Other Breaches and Security Concerns**

cxxvii. The threat to private Aadhaar data is further exacerbated by the existence of 'State Resident Data Hubs' and similar data repositories, which interlink numerous scattered databases using an individual's Aadhaar number. Through this, the personal data of each Aadhaari is consolidated under a single hub, effectively permitting unscrupulous elements to profile an individual and subject them to continuous surveillance, amongst other things. Thus, using an Aadhaar number, previously discrete silos of data are being integrated and brought under one single head. It is apposite to note that the use of Aadhaar data for such resident data hubs was conceptualized by the Respondent No.1 itself through arrangements with various state governments as well as private players. Such scattered resident data hubs worsen the already weak security architecture of the Aadhaar ecosystem. A news report summarizing the functioning of State Resident Data Hubs and their potential for misuse is annexed herewith as **ANNEXURE P/22.**

cxxviii. Apart from the security concerns highlighted through the various breaches above, a French security researcher has on numerous occasions exposed the multiple security flaws within the Aadhaar ecosystem, pointing to the possibility of identity theft and other abuses of personal data. An interview in this regard is annexed herewith and marked as **ANNEXURE P/23**.

cxxix. A number of other instances of breach of informational privacy such as the sale of forged Aadhaar cards, misuse of data without prior permission, unauthorised publication of names and numbers of Aadhaar card holders etc. appear to have occurred and have been widely reported since the inception of the Aadhar scheme. A comprehensive list of most such breaches, as available in the public domain has already been annexed herewith and marked as **ANNEXURE P/3.**

**(B) DATA PROTECTION DUTIES UNDER THE LAW**

cxxx. The inability of Respondent No.1 to secure the identity information of Aadhaaris, including that of the Petitioner, has resulted in a serious and egregious violation of the fundamental right to privacy and dignity, as affirmed in the recent apex court decision in ***Puttaswamy (supra)*.** Furthermore, by failing to adopt reasonable security measures to secure Aadhaar data, the Respondents have violated various statutory duties laid down under, *inter alia*, the IT

Act and Aadhaar Act. To recapitulate, the main duties are discussed below.

cxxxi. Section 28 of the Aadhaar Act casts an over-arching duty on Respondent No.1 to ensure the security and confidentiality of the Aadhaar data by *inter-alia* adopting and implementing appropriate technical and organizational security measures within the Aadhaar ecosystem. It bears repetition that this statutory standard of care imposed on the Respondent No.1 is a strict one, in as much as the said provision obligates the Respondent No.1 to prevent even an accidental loss of data.

cxxxii. In order to better appreciate this standard of care, one may look to the Data Protection Act, 1998 (hereafter referred to as '**DPA**') of the United Kingdom, which stipulates a largely similar standard. As per Section 4 (4) of the DPA read with its Part I of Schedule I, it is the duty of a data controller (anyone who determines the purpose and manner in which data has to be processed) to *inter alia* take "*appropriate technical and organisational measures*" against "*unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*". While interpreting the scope and ambit of this provision, the Information Commissioner's Office has made clear that any such technical/organisational measures must necessarily ensure a level of security proportionate to the magnitude of harm that might

result from an unauthorised/unlawful processing of data. Illustratively, in the case of Staysure.co.uk Limited, where an insurance company's website, containing personal information of various data subjects, was unauthorisedly viewed and modified by a hacker, the Information Commissioner held that the company had failed to take appropriate technical measures. This conclusion was particularly influenced by the failure of the insurance company to apply available software security updates. A copy of Monetary Penalty Notice dated 20.02.2015 issued against Staysure.co.uk Limited is annexed herewith and marked as **ANNEXURE P/24**.

cxxxiii. In the various instances narrated in this Petition too, the breaches have been caused by the failure of Respondent No.1 and its various partners/affiliates to ensure a level of security proportionate to the magnitude of harm that could result from an unauthorised or unlawful processing of data. Consequently, the Petitioner (and countless other Aadhaaris) is entitled to legal redressal including a relief for damages under Section 43A of the IT Act.

cxxxiv. Finally, the failure of Respondent No.1 to effectively carry out its data protection duties is apparent from the recent attempt by it to roll out a Virtual ID ('**VID**'). As per Respondent No.1's circular dated 10.01.2018, Aadhaaris will soon be able to generate a temporary 16-digit random number called VID in lieu of their

Aadhaar numbers for authentication transactions. This will essentially give each Aadhaari the option of not using her Aadhaar number and thereby preventing any potential unauthorized disclosure/use. Apart from the VID, Respondent No.1 has also proposed the introduction of a 'Limited KYC' system, to be facilitated through 'UID Tokens'. This too is meant to improve the anonymity and privacy of Aadhaaris. Under this new system, a few AUAs called 'Global AUAs' will continue to have full e-KYC access, while some other AUAs called 'Local AUAs' will only have limited KYC access and will not be allowed to store Aadhaar numbers. Such 'Local AUAs' will instead have to procure agency specific UID Tokens, which are to be used in lieu of Aadhaar numbers to identify their customers. While these proposed changes are welcome, they should have been done far earlier. The late introduction of these measures is an implicit acknowledgement of the fact that the earlier system was highly vulnerable from a privacy perspective. In any case, the new system does nothing to ameliorate the concerns of the Petitioner and countless other Aadhaaris whose Aadhar numbers and details have already been compromised. The circular issued by the Respondent No.1 dated 10.01.2018 proposing the introduction of the VID, Limited KYC and UID Token is annexed herewith and marked as **P/25**.

**(C) APPOINTMENT OF INVESTIGATIVE/AUDIT COMMITTEE**

cxxxv. It is submitted that the precise extent of damage arising out of the present set of Aadhaar breach cases is difficult to quantify, owing to the sheer lack of transparency and the deliberate obfuscation engaged in by the Respondents. Given that a vast majority of Aadhaaris are likely to have been affected in the same manner as the Petitioner, it is necessary to undertake a detailed investigation/audit of the various breaches and the robustness of security systems and protocols implemented by the Respondents and their various partners/affiliates.

cxxxvi. It is therefore prayed that the court appoint an independent investigative/audit committee comprising multiple stakeholders/experts to investigate and audit *inter alia* (a) all security and privacy breaches of the Aadhaar database, including the breaches outlined in this Petition and **ANNEXURE P/3**, (b) the robustness of the security systems and processes instituted by the Respondent No.1 and its affiliates/partners, as well as their security policies and practices, operations, infrastructure, and procedures, and their compliance with the same, (c) the extent of monitoring of affiliate/partner activities and security systems by Respondent No.1 including audits etc., (d) the extent of non-compliance by Respondent No.1 and its various affiliates/partners with the various statutory duties in relation to the security of the Aadhaar ecosystem, (e) the efficacy or otherwise of steps taken by Respondent No.1 in remedying and rectifying their security

practices pursuant to the breaches, and any lapses in this regard and (f) the loss/destruction/unauthorized disclosure of/access to the Petitioner's own Aadhaar data by acts/omissions of the Respondents.

cxxxvii. Such a comprehensive audit/investigative report by an independent court appointed committee would enable the Petitioner and various other Aadhaaris to gain a better understanding of the various data breaches and security lapses in order to appropriately protect themselves against future harm and agitate more appropriate legal redressal measures, including additional damages, where applicable.

**(D) CONSTITUTIONAL/COMMON LAW RIGHTS AND DAMAGES**

cxxxviii. The Petitioner submits that his right to life and dignity has been compromised owing to the reckless manner in which the Respondents have handled issues of data security and confidentiality. The fact that his data is now available to any third party for identity theft and other abuses has resulted in severe mental anxiety and emotional distress; and an inability to participate fully in society without a fear of potential harms at the hands of third parties who might misuse his data. The Petitioner has also noticed an increase in the number of spam related offerings to both his email inbox and his cell phone after his

registration with Aadhaar. With his personal data now available to all and sundry, the Petitioner fears that he will be subjected to an increasing array of intrusions into his private sphere of seclusion.

cxxxix. Such unsolicited emails and messages are also a significant source of nuisance and inconvenience.

cxl. Further, it is submitted that the right of non-discrimination is intrinsically linked to the right to informational privacy, given the particular vulnerability of persons of minority communities to dignity harms and violations of autonomy at the hands of a hostile majority. The Supreme Court in its judgement in ***Puttaswamy* (*supra*)** has recognized the vulnerability of minorities to profiling and its concomitant dignity harms and equality violations. Being a Muslim and a member of a minority community, the threat of potential harms to the Petitioner are even more accentuated. For one, given that in today's post truth world, almost all Muslims are seen as terrorists and interrogated as such at various international airports and the like, the risk of harms from a data breach and consequent identity theft or the tampering with personal data is significantly more magnified. Secondly, given the present political climate in the country for minorities and the growing patriotic fervor of those committed to purging the country of its plural ethos, the Petitioner fears that unrestrained access to his data could have potentially fatal implications.

cxli. It is submitted that although the Aadhaar Act and the IT Act do not provide for adequate legal redressal for data breaches, various common law precedents provide ample scope for the Petitioner to pursue a slew of remedies for data breaches, including punitive damages.

cxlii. Common law courts have recognized the right to claim damages for privacy violations. Recently, a UK court awarded damages to individuals whose private and confidential data had been negligently published by the State on its website. In this case, *TLT & Ors. v. The Secretary of State for the Home Department*, [2016] EWHC 2217 (QB), the Queen's bench specifically held that such damages were recoverable under "common law", implying that parties need not rest their case solely upon statutory provisions.

**(D.1) <u>Legal Redressal under the Aadhaar Act</u>**

cxliii. The Aadhaar Act does not provide any right of direct legal redress for data subjects directly aggrieved by breaches. Rather it relies on the data custodian, namely Respondent No. 1, to initiate actions for data breaches. This is an utterly arbitrary redressal mechanism, given that most breaches will likely owe themselves to the fault/neglect of the custodian itself, and the authority cannot be expected to initiate action against itself. The constitutionality of this

arbitrary redressal mechanism (as per Section 47 (1) of the Aadhaar Act, a court can take cognizance of an offence punishable under the Act only upon a complaint filed by the Respondent No.1) is currently under challenge before the Hon'ble Apex Court and therefore, the Petitioner is not raising such challenge by way of the present petition.

## (**D.2**) **Damages under the IT Act**

cxliv. It is submitted that although the Petitioner is entitled to claim damages for various data breaches under Section 43A of the IT Act, the redressal mechanism is woefully inadequate and unconstitutional, in as much as the adjudicating authority set up under Section 46 of the Act is constitutionally incompetent to adjudicate the dispute.

cxlv. As per the norms laid down by the Hon'ble Supreme Court, where there is a lis, i.e. a dispute requiring a decision of the rights and obligations of the parties with respect to an affirmation by one and a denial by another, only a court or a constitutionally qualified tribunal may adjudicate upon and decide the matter.

cxlvi. The court's observations in *T.N.Generation and Distribution Corporation Limited v. PPN Power Generation Company Private Limited,* 2014 (4) SCR 667, (while deciding on the power of Tamil

Nadu State Electricity Regulatory Commission to adjudicate disputes) are instructive to the present context:

> *"In view of the aforesaid categorical statement of law, we would accept the submission of Mr. Nariman that the tribunal such as the State Commission in deciding a lis, between the appellant and the respondent discharges judicial functions and exercises judicial power to the State. It exercises judicial functions of far reaching effect.* ***Therefore, in our opinion, Mr. Nariman is correct in his submission that it must have essential trapping of the court. This can only be achieved by the presence of one or more judicial members in the State Commission which is called upon to decide complicated contractual or civil issues which would normally have been decided by a Civil Court.*** *Not only the decisions of the State Commission have far reaching consequences, they are final and binding between the parties, subject, of course, to judicial review."*

cxlvii. Similar safeguards were mandated in *R Gandhi v. Union of India,* Civil Appeal No.3067 of 2004, as well, wherein the Apex Court laid down detailed safeguards to ensure that judicial functions are exercised by constitutionally competent personnel who are independent of the Executive:

> "*We have already held that the Legislature has the competence to transfer any particular jurisdiction from courts to Tribunals provided it is understood that the Tribunals exercise judicial power and the persons who are appointed as President/Chairperson/Members are of a standard which is reasonably approximate to the standards of main stream Judicial functioning. On the other hand, if a Tribunal is packed with members who are drawn from the civil services and who continue to be employees of different Ministries or Government Departments by maintaining lien over their respective posts, it would amount to transferring judicial functions to the executive which would go against the doctrine of separation of power and independence of judiciary*."

cxlviii. As outlined earlier, Respondents' recklessness in safeguarding the security of the Petitioner's personal data renders it liable under the terms of section 43A of the IT Act, which mandates compensatory

damages for security breaches that cause wrongful loss or gain. The Respondents will no doubt contest the claims of the Petitioner in this regard. As such, there is a "lis" between the parties, which require to be adjudicated upon only by a constitutionally competent authority. The present scheme which vests adjudicatory powers with a single government official violates constitutional norms pertaining to the separation of powers and the independence of the judiciary.

cxlix. It bears noting in this regard that the "adjudicating officer" under Section 46 of the IT Act is deemed to be a Civil Court as is clear from Section 46 (5) of the IT Act. Section 46 (5) of the IT Act reads as follows:

> *"Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and-*
> *(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code (45 of 1860);*
> *(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974);*
> *[(c) shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908 (5 of 1908)."*

cl. Despite being deemed to be a court, the adjudicating officer appointed under Section 46 does not have the "*the independence, security and capacity associated with courts*". This is apparent from the eligibility criteria laid down for the appointment of adjudicating officers. As per these criteria, anyone who is an officer not below the rank of a Director to the Government of India or an equivalent

officer of a state government is eligible to be appointed to the position of the Adjudicating Officer. Further, the government is vested with the sole responsibility to appoint the said "adjudicating officer" and there is no judicial involvement in this selection, further violating the terms of *R Gandhi*.

cli. As such, the Adjudicating Officer envisaged under the IT Act is constitutionally incompetent to adjudicate upon such matters. Till such time as this redressal mechanism is constitutionalized, the Petitioner is unable to invoke it.

## (**D.3**) **Common Law Remedies**

clii. As submitted earlier, despite the lack of a direct statutory remedy, the Petitioner is entitled to claim damages under common law, as summarized below:

### (D.3.1) Breach of Statutory Duty

cliii. To reiterate, the Respondents have breached the various statutory duties cast upon them by the Aadhaar Act and the IT Act. Although the Aadhaar Act does not explicitly provide for any direct legal redressal for an aggrieved person such as the Petitioner, it is trite law that damages are recoverable under common law for the breach of an important statutory duty.

cliv. Numerous cases from various common law countries have recognized such a right, predicated on the below preconditions:

(a) The breach of a statutory obligation, which on a proper construction of the statute, was intended to confer a protection/benefit to a class of persons, of whom the petitioner is one; and

(b) The injury or damage was of a kind for which the statute was designed to offer protection.

clv. In India, the above tortious liability principle was applied in *Sm. Mukul Dutta Gupta And Ors. vs Indian Airlines Corporation (*AIR 1962 Cal 311), a case where the Plaintiffs sued the Defendant Corporation for damages resulting from a breach of statutory duty. The Court held as follows:

> [….] "*The learned Standing Counsel, therefore, contended that these Rules were framed for the general benefit of the public and they create no duty in favour of any particular class of citizens. I am not concerned in this case with any rule other than Rule 115 in Part XII.* ***The mandatory provision directing the pilot to occupy a particular place in the plane to secure safe flying is considered so essential that the breach of this rule is visited with punishment of imprisonment or fine or both. But I am unable to hold that it is the only remedy intended by the Rules. I discern in this Rule a further duty to the travelling public, in particular, which gives the travelling public a corresponding right. The travelling public, in my judgment, has, therefore the ordinary civil remedy for enforcement of its breach, namely, an action in damages. I am unable to hold that the punishment provided in the Rules was intended to be the only remedy to secure enforcement of the Rule.*** *Unless there is a clear indication to*

> *the contrary in the statute that the punishment provided in the statute is the only remedy, I would not be justified in holding that a breach of the Rule made, inter alia, to secure the safety of a passenger in a commercial aircraft would not give a cause of action to the passenger damnified by reason of the breach of the Rule."*

### *(D.3.1.1) Application of the Principle to Aadhaar Act*

clvi. It is submitted that on a true construction of the Aadhaar Act, it is clear that it does not exclude a remedy for damages or any other form of legal redressal. This is amply clear from Section 46 of the Act, which states that penalties imposed under the Act *shall not exclude* the imposition of penalties under any other law. Moreover, the statute makes clear that the provisions of the Aadhaar Act are in addition to and not in derogation of other statutes.

clvii. Secondly, it is submitted that the statutory duty under the Act is limited to a specific class of persons, i.e., the Aadhaaris, and not to the public in general. Given the same, the Petitioner and his fellow Aadhaaris have a valid cause of action and a right to claim damages for the breach of an important statutory duty to keep their data secure.

### **(D.3.2) Other Common Law Remedies**

clviii. Apart from an actionable breach of statutory duty, Petitioner is entitled to a slew of other common law remedies, as outlined below:

**(D.3.2.1) *Negligence***

clix. The tort of negligence refers broadly to a theory of legal liability wherein a person who owes a duty of care to his/her neighbor breaches the said duty, resulting in ensuing damages. In the instant case, the Respondents have been woefully negligent in securing the confidentiality of the Petitioner's private data, causing damages by way of extreme anxiety, mental pain/suffering and emotional distress.

clx. The tort of negligence has been invoked in data breach cases across some of the common law countries. Illustratively, in *Bell v. Michigan Council 25 of the American Federation of State, County, and Municipal Employees,* 2005 WL 356306, the Michigan Court of Appeals held that the Defendant Union which collected personally identifiable information of its members was liable to pay damages for its negligent handling of data. The Court affirmed the Plaintiffs' argument that the union owed a duty to its members to safeguard their private data. The following portions from the judgment are relevant to the present context:

> *"The relationship between the parties in this case is one of union-union member. Plaintiffs liken the relationship to a fiduciary one, where defendant was entrusted with the personal information of plaintiffs, similar to the relationship between a bank and its account holders or any financial institution and its clients. A person in a fiduciary relationship to another is under a duty to act for the benefit of the other as to matters within the scope of the relationship. Teadt v Lutheran Church Missouri Synod, 237 Mich.App 567, 580-581; 603*

> *NW2d 816 (1999). As plaintiffs' representative union, defendant has an obligation to act on behalf of, and in the best interests of, plaintiffs. See Sowels v Labors' Int'l Union of North America, 112 Mich.App 616; 317 NW2d 195 (1982). It follows that part and parcel of that relationship is a responsibility to safeguard its members' private information. And society has a right to expect that personal information divulged in confidence, especially to an organization such as a union whose existence is for the benefit of the union members, will be guarded with the utmost care. Moreover, from a control standpoint, defendant is in the best position to protect plaintiffs because it controls who has access to its membership lists. In regards to the foreseeability factor, defendant argues that Dentry's actions were not foreseeable. Plaintiff responds that defendant is mistakenly focusing on the foreseeability of a particular person's actions versus the foreseeability of the harm, identity theft. We agree. In determining whether to impose a legal duty, it is the foreseeability of the harm in general that is considered, not the foreseeability in regards to one particular person"*

clxi. A similar conclusion was reached in *Jerry Stacy v. HRB Tax Group Inc*. (Sixth Circuit, Court of Appeals), 516 Fed.Appx. 588 (2013), where the court adopted the reasoning from *Bell* and held as below:

> *"Having considered the matter and reasoning from the decision in Bell, we conclude that the Michigan courts would also determine that HRB owed a duty of care to safeguard the plaintiffs' confidential identifying information in this instance because of the special relationship between taxpayer and tax preparer. Further, we reason from Bell that the Michigan courts are prepared to recognize that economic and emotional injuries allegedly occasioned by reasonably foreseeable instances of identity theft that result from an employee's actions may serve as the basis for recovery in these types of cases, even in the absence of a physical injury"*

clxii. As with the above cases, Respondent No.1 owes a duty to all Aadhaaris to safeguard their data. More so, since it is in the position of a data custodian and owes a special fiduciary duty to its data subjects.

clxiii. In *Daly v. Metropolitan Insurance Company,* 782 N.Y.S.2d 530, 535 (N.Y. Sup. Ct. 2004), the New York County Supreme Court observed that a data custodian, who specifically represented to its data subject that her personal information would be protected and shall remain fully confidential, may be liable for breach of fiduciary duty if it fails to safeguard such information.

clxiv. In the present instance, the Respondent No.1 has specifically represented that it is a data custodian and holds the information of all Aadhaaris in trust. Thus, it is clear that by failing to put in place sufficient security practices and procedures and by allowing unauthorized third parties to access the personal data of Petitioners, the Respondents have breached the fiduciary duty owed to the Petitioner and other Aadhaaris.

(**D.3.2.2**) ***Misuse of Private Information and Damages***

clxv. Common law now recognizes a broad privacy tort titled "Misuse of private information". Recognized for the first time in *Campbell v MGN* [2004] 2 AC 457**,** the House of Lords observed:

*"Now the law imposes a 'duty of confidence' whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential. Even this formulation is awkward. The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private. The essence of the tort is better encapsulated now as misuse of private information."*

clxvi. In order to fasten liability under the tort of misuse of private information, the courts generally apply a two-fold test:

(a) Whether the Plainitiff / Petitioner had a reasonable expectation of privacy, and

(b) If so, whether the interference with such right of privacy by way of publication was justified in the circumstances.

clxvii. In the various breaches outlined in this Petition, it is axiomatic that Aadhaaris had a reasonable expectation of privacy in relation to their personal data. As to the applicability of the second limb, no reasonable justification has been furnished for the publication of the personal data of the Aadhaaris in the cases / incidents explained in this Petition (as in the case of websites unauthorisedly publishing data of Aadhaaris).

clxviii. The ambit of the tort of misuse of private information was elaborated upon by the UK Court of Appeals in *Gulati v. MGN Limited* ([2015] EWCA Civ 1291), where it noted that the essential principle of this tort is that by the misuse of private information, persons have been deprived of their right to control the use of private information.

clxix. US courts have also recognized the existence of a separate tort of 'public disclosure of private facts' that is intended to safeguard against the invasion of privacy of an individual. As per Section 652D of the US Restatement (Second) of Torts, *"…one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."* Further, US Courts have recognized the right to privacy in demographic information pertaining to an individual. For example, in the case of *Nat'l Ass'n of Retired Fed. Emps. v. Horner*, 879 F.2d 873 (D.C.Cir.1989) [as quoted in Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL.L.REV, 1805 (2010)], it was held that individuals had a privacy interest in avoiding unlimited disclosure of their names and addresses. Similarly, in *Benz v. Wash.Newspaper Publ'g Co.*, 2006 WL 2844896, the court found that the Plaintiff's address was a private fact, given that it was not published elsewhere.

clxx. The weight of common law precedent therefore clearly suggests that the Petitioner has an actionable claim against the Respondents for various data breaches and the consequent anxiety and mental distress inflicted upon him. Further, common law precedent also supports the proposition that in cases of data breach, damages may be presumed, i.e., data breaches are actionable per se, without having to demonstrate proof of actual physical / pecuniary damage of some sort. As noted by the Court of Appeal in Google Inc. *v. Judith Vidal Hall and Ors., [2015] EWCA Civ 311:*

> *[…] It would be strange if that fundamental right could be breached with relative impunity by a data controller, save in those rare cases where the data subject had suffered pecuniary loss as a result of the breach. It is most unlikely that the Member States intended such a result."*
>
> *[…] It is the distressing invasion of privacy which must be taken to be the primary form of damage (commonly referred to in the European context as "moral damage") and the data subject should have an effective remedy in respect of that damage.*

clxxi. Therefore, it is submitted that in view of the multiple security breaches in respect of the Aadhaar data maintained by the Respondent No.1 as data controller / custodian, resulting in the violation of the privacy of the Petitioner, the Respondents are liable to pay compensation *per se* without the Petitioner having to produce any proof of direct pecuniary loss. Further, the Petitioner is also entitled to exemplary punitive damages. The following extract from a scholarly article published as 'J C Love, *Presumed*

*Damages for Fourth Amendment Violations,* 129 U. PA. L. Ray. 192, 220 (1980)' is instructive:

> "*The awards in these cases undoubtedly contained a punitive element, which the English juries were not required to label separately. But they nevertheless illustrate the zealous protection at common law of intangible interests in liberty and security, a goal accomplished by awarding substantial damages for the infringement of such interests, even in the absence of physical or economic harm or evidence of unusual emotional distress.*"

clxxii. This principle of awarding punitive damages has found favour with Indian courts as well. In a privacy case titled *ABC v. Commissioner of Police* and *Ors*., bearing W.P. (C) No. 12730 of 2005, the Delhi High Court awarded punitive damages of Rupees six lakhs to a minor girl whose details had been leaked by the Commissioner of Police to media houses. Finding the said action to be a violation of the right to privacy of the Petitioner, the court elaborated that damages were awarded *"to set an example for others, so that it acts as a deterrent against such similar misadventures at the cost of victims of alleged sexual abuse."*

clxxiii. Drawing from the above, the Petitioner and other Aadhaaris, whose sensitive personal information has been lost/compromised due to wanton recklessness of the Respondents, are entitled to claim exemplary damages for the same, so that future breaches are prevented. This becomes all the more necessary given the repeated breaches and the failure of the Respondents to take responsibility

or any steps towards effective redressal including securing the Aadhaar ecosystem in a better way.

***(D.3.2.3) Nuisance***

clxxiv. The tort of nuisance is aimed at preventing an unreasonable interference with the use of one's property. As submitted earlier, ever since his Aadhaar enrolment and subsequent linkage with bank account etc., the Petitioner has been receiving numerous unsolicited e-mails, text messages and calls for a variety of different goods/services.

clxxv. Such unsolicited correspondence has interfered with the peaceful enjoyment of the Petitioner's property- his e-mail inbox, telephone and personal data-and is therefore actionable. Nuisance claims in a case of multiple unsolicited communications have been upheld in various common law jurisdictions, including by the US Courts in *MacCa v. General Telephone Co. of Northwest, Inc.* [495 P.2d 1193 (1972)] where the Supreme Court of Oregon, affirmed a nuisance verdict in favour of the Plaintiff who received multiple unsolicited telephone calls as a result of the Defendants' negligence.

clxxvi. The continued intrusion of different service providers, which is directly facilitated by the Respondents, has violated the right of the Petitioner to be let alone, as affirmed by the Hon'ble Supreme

Court in its judgement in ***Puttaswamy (supra)***, and is actionable under the common law tort of nuisance. Such unsolicited correspondences have substantially interfered with the productivity of the Petitioner and have caused tremendous nuisance to him. .

**(D.4) <u>Constitutional Torts</u>**

clxxvii. The Apex Court decision in ***Puttuswamy (supra)*** categorically casts the right to privacy as a fundamental constitutional right, noting as below:

> *"In the Indian context, a fundamental right to privacy would cover at least the following three aspects:*
>
> *[…]*
>
> *Informational privacy which does not deal with a person's body but deals with a person's mind, and therefore recognizes that an individual may have control over the dissemination of material that is personal to him. Unauthorised use of such information may, therefore lead to infringement of this right"*

clxxviii. From the numerous breaches and wanton dissemination of the personal information of Aadhaaris, it is clear that the Respondents have breached the right to informational privacy of the Aadhaaris.

clxxix. It is settled law that where the state violates the constitutional rights of a citizen, courts may award compensation, even in the absence of any specific statutory provisions. These are broadly known as constitutional torts.

clxxx. In *Municipal Corporation of Delhi vs. Association of Victims of Uphaar Tragedy and Ors.* (AIR 2012 SC 100, hereafter referred to as "**Uphaar**"), the Hon'ble Apex Court noted:

> *"But, in a case, where life and personal liberty have been violated, the absence of any statutory provision for compensation in the Statute is of no consequence. Right to life guaranteed under Article 21 of the Constitution of India is the most sacred right preserved and protected under the Constitution, violation of which is always actionable and there is no necessity of statutory provision as such for preserving that right. Article 21 of the Constitution of India has to be read into all public safety statutes, since the prime object of public safety legislation is to protect the individual and to compensate him for the loss suffered."*

clxxxi. As to the recovery of damages through a writ petition, the Supreme Court has clearly held that it is open to the courts under their writ jurisdiction to award damages/compensation and they need not confine themselves to the "*old conservative doctrine of civil courts' obligation to award damages*". In *MS Grewal and Anr. v. Deep Chand Sood and Ors.* (2001) 8 SCC 151, the Supreme Court, in the context of awarding damages under writ jurisdiction, held that "*Currently judicial attitude has taken a shift from the old draconian concept and the traditional jurisprudential system affectation of the people has been taken note of rather seriously and the judicial concern thus stands on a footing to provide expeditious relief to an individual when needed rather than taking recourse to the old conservative doctrine of civil courts obligation to award damages." [emphasis supplied]* It was also emphasised that technicalities cannot and ought not outweigh the course of justice and render the law courts inefficacious.

clxxxii. The Supreme Court in *Delhi Jal Board v. National Campaign for Dignity and Rights of Sewage and Allied Workers and Ors.*, (2011) 8 SCC 568, following a line of precedent, affirmed the principle that damages may be awarded to a person under writ jurisdiction in the event the person's injuries were a result of the state's negligence.

clxxxiii. Similarly, it has also been held that compensation by way of a public law remedy need not only be a palliative amount but can extend to exemplary damages, further bolstering the contention of the Petitioner above in respect of award of punitive damages to deter future breaches. The following observations in ***Uphaar* (*supra*)** are instructive in this regard:

> ***"****38. Therefore what can be awarded as compensation by way of public law remedy need not only be a nominal palliative amount, but something more. It can be by way of making monetary amounts for the wrong done or by way of exemplary damages, exclusive of any amount recoverable in a civil action based on tortuous liability."*

clxxxiv. In view of the above, the Petitioner humbly submits that the Respondents are liable to compensate the Petitioner, not only under various statutory provisions but also under constitutional law and common law.

## (E) THE RIGHT TO KNOW

clxxxv. It is submitted that Respondent Nos.1 and 2 have not only failed to secure the confidentiality of Aadhaar data, but have also violated the fundamental right to "know" of various data subjects i.e. the

right to know of the security practices pertaining to Aadhaar data, as also the right to know of any breaches of the Aadhaar database / data.

clxxxvi. Rather than disclosing the extent of the breaches and more importantly, the various security measures put in place to protect such sensitive information, Respondent No.1 has denied these breaches and issued press statements that are contradictory, self-serving and issued with the sole intent of covering up its failure to adequately secure the relevant Aadhaar data. Till date, it has not accepted or acknowledged responsibility for the various breaches or provided any information on the severity of such breaches, names of personnel responsible, disciplinary / punitive proceedings if any, and the potential future threats from such breaches. Most importantly, it has failed to indicate any preventive measures to ensure that future breaches of a similar nature do not occur.

clxxxvii. The Petitioner submits that Respondent No.1 has a legal obligation to inform data subjects of any data leaks or data breaches. This right to know stems from the fundamental right to privacy, which has been recognized by the Hon'ble Apex Court in the seminal judgment in ***Puttaswamy (supra)*****.** Any breach or unauthorized disclosure of private personal information (such as Aadhaar data) significantly harms the privacy rights of the Petitioner and

countless other Aadhaaris. As such, it is critical that data subjects have a right to know of the occurrence and extent of breaches, such that they are able to take some steps to prevent potential abuses in future.

clxxxviii. In this regard, it is submitted that 'Personal Data Breach Notification' is a well-accepted norm internationally. This norm dictates that data subjects have to be intimated forthwith of data breaches that implicate their private data. Illustratively, as per the European Union's General Data Protection Regulation, the controller is required to communicate the breach to the affected individuals as soon as is reasonably feasible. Similar standards exist in most other jurisdictions and typically, such notifications are to inform the data subject of the type of data breach, the estimated date of the breach and the general description of the security incident in a language that is comprehensible to the data subject. Such notification should also inform the data subject of the remedies available to him / her.

clxxxix. It is submitted that the Respondents have not only failed to put in place a credible mechanism to inform data subjects of breaches, but have also stonewalled any attempt to obtain information about the said breaches. In one such instance, the Respondent No.1, in response to a Right to Information application requesting information on the attempts made to illegally obtain Aadhaar data,

cited Section 8 (1) (a) of the Right to Information Act, 2005 and denied the said information. Thus, it is submitted that the Respondent No.1 has not only ignored standard international norms in relation to data protection, but also stonewalled attempts to obtain vital information that is critical to appropriately safeguarding a critical constitutional right.

A copy of the news article highlighting the position of Respondent No. 1 in relation to the RTI query as aforementioned is annexed herewith and marked as **ANNEXURE P/26.**

cxc. Apart from the lack of a data breach notification mechanism, Regulation 7 of the Data Security Regulations also serves to deny the Petitioner and other Aadhaaris their fundamental right to know. Specifically, the policies and protocols, including the information security policy, governing the Aadhaar data and its security, are sought to be made confidential by way of the said Regulation. However, since a constitutionality challenge to the Aadhaar Act and its related Rules/Regulations is presently pending in W.P. (C) 494 of 2012, the Petitioner refrains from challenging the constitutionality of the above regulation.

**(F) THE RIGHT TO LEGAL REDRESSAL**

cxci. As per Section 47 (1) of the Aadhaar Act, a court can take cognizance of an offence punishable under the Act *only* upon a

complaint filed by the Respondent No.1. There is no other remedy available to an aggrieved data subject under the terms of the Aadhaar Act.

cxcii. This lacuna is violative of the constitutional right to adequate legal redressal. The Supreme Court in ***Bhagubhai Dhanabhai Khalasi and Anr. v. The State of Gujarat and Ors.*** **(2007) 4 SCC 241** held that:

> *"A party having a grievance must have a remedy. Access to justice is a human right. When there exists such a right, a disputant must have a remedy in terms of the doctrine ubi jus ibi remedium."*

cxciii. Further, section 47(1) also suffers from the vice of arbitrariness and illogic, ridden as it is with a severe conflict of interest. The section stipulates that Respondent No.1, who is in charge of the Aadhaar database, and who has a clear vested interest in obfuscating the occurrence of breaches is the only entity capable of filing a complaint under the Act. As such, Respondent No. 1 has no incentive for bringing these breaches to light through a formal complaint. More so when the erring individuals are its own personnel or those employed by its close partners/affiliates such as Respondent No. 3. As submitted earlier, in a number of instances of data breach, such as the public display of Aadhaar numbers by 210 websites and the Srivastava Spoof, the Respondent No.1 failed to take any steps against the concerned government departments/agencies who were clearly in contravention of the

security standards, even under the terms of the Aadhaar Act and associated regulations.

cxciv. Therefore, Section 47 of the Aadhaar Act is susceptible to being struck down as unconstitutional, in as much as it denies the Petitioner a direct statutory right to file a complaint even when his own privacy rights have been violated through a data breach. It is also manifestly arbitrary, as it vests the exclusive right to file complaints with the very same authority who is likely to be the transgressor.

cxcv. Nevertheless, the Petitioner does not press the above challenge in this petition on account of the fact that the constitutionality of Section 47 is already under challenge before the Supreme Court of India in W.P. (C) No. 494 of 2012. However, he humbly prays that till such time as a credible statutory mechanism for legal redressal is worked out, the Hon'ble Court be pleased to direct the appointment of a neutral ombudsman comprising a variety of stakeholders in the Aadhaar ecosystem, who are able to address the complaints and grievances of Aadhaar data subjects at the first instance.

cxcvi. The idea of a neutral ombudsman is not new and has been invoked by courts in other areas of law such as copyright law. In ***Eros International Media Limited and Anr. v. Bharat Sanchar Nigam***

***Limited and 49 Ors*., bearing Suit (L) No. 2147 of 2016**, the Bombay High Court suggested the creation of a neutral ombudsman to help resolve disputes arising in the context of John Doe orders in copyright disputes.

cxcvii. A similar ombudsman like body could be conceived of in the Aadhaar-data breach context as well to help aggrieved data subjects such as the Petitioner to lodge complaints at the first instance. The said ombudsman could help ascertain the existence and extent of breach, particularly in relation to the complainants' data. This finding could then help data subjects take appropriate steps to protect against further fraud and also to file formal petitions seeking damages etc with courts of law, invoking their fundamental constitutional rights as also other rights and remedies available under the law, such as common law.

cxcviii. The proposed ombudsman could be vested with other related tasks as well to effectively function as a neutral watchdog of the Aadhaar system. This will not only help allay the fears of billions of aggrieved Aadhaar users such as the Petitioner, but also make data custodians such as Respondent No. 1 more accountable and committed to safeguarding the privacy rights of their data subjects.

## GROUNDS FOR RELIEF

A. The various acts and omissions of the Respondents amount to a serious breach of legal obligations, both under the Constitution of India, as well as the relevant statutes and common law principles governing the security of the Aadhaar database. As such, the Petitioner prays for a declaration that his constitutional rights have been breached. More specifically, the Petitioner seeks damages including exemplary/punitive damages for the losses caused due to the wanton negligence of the Respondents.

B. Given the opacity with which the Respondents have dealt with the scope and extent of such breaches, the damage caused to the Petitioner and countless other Aadhaaris cannot be determined with any degree of precision. It is therefore humbly prayed that the court appoint an independent committee comprising multiple stakeholders/experts to investigate the scope and extent of breaches and the magnitude of harm, both current and future.

C. In any event, the data breaches have caused severe mental agony and emotional suffering to the Petitioner, as he fears potential misuse of his data at the hands of unscrupulous third parties. The Petitioner reserves the liberty to seek appropriate compensation from the Respondents for all existing and future security risks arising out of this issue.

D. The court ordered committee may also be directed to:

(a) audit the security policies, practices, operations, infrastructure, systems and procedures of the Respondent No.1 and its partners/affiliates.

(b) investigate the extent of breach of statutory duties/obligations.

E. Furthermore, the Respondents must be mandated to inform the Petitioner and other Aadhaaris of the number of data breaches/illegal disclosures which have taken place since the inception of the Aadhaar scheme, the extent/scope of such data breaches, and specifically the manner/scope/extent of the breach in so far as it compromises the Petitioner's personal data. The Respondents must also be asked to indicate the various steps taken towards remedying and rectifying their security practices pursuant to such breaches. This mandatory disclosure ought to be reviewed by the court appointed committee above mentioned.

F. Given the repeated breaches over time and the fact that the Petitioner's Aadhaar number and various other demographic and other details are now in the possession of unauthorized third parties, the Petitioner cannot be reasonably expected to continue with the existing Aadhaar number. The Petitioner therefore prays that he be granted the liberty to opt-out of the Aadhaar system and the Respondent No.1 be directed to permanently deactivate his number

and delete all the data relating to the Petitioner from the CIDR. In the alternative, the Petitioner prays that the Respondents be directed to issue a new Aadhaar number to the Petitioner after permanently deleting the earlier one and all data associated with it.

G. The Petitioner further submits that Section 46 of the IT Act violates the separation of powers doctrine and the independence of the judiciary, for the reasons elaborated hereinbefore. Therefore, this case cannot be adjudicated upon by an Adjudicating Officer under the IT Act, and may be brought before this Hon'ble Court for consideration.

H. Despite the public's entitlement to know of data breaches under the constitutional right to privacy, Respondent has failed to provide any information pertaining to the various data breaches. Therefore, it is humbly prayed that this Hon'ble Court direct the independent court-appointed audit committee to investigate into the affairs of Respondent No.1.

I. Given that the Respondent No.1 has consistently denied its wrong-doings and failed to address the concerns of the Aadhaaris, it is humbly submitted that a direction may be given to the Respondents to appoint a neutral ombudsman for addressing all concerns and complaints at the first level, which may arise in the future in relation to violations of, *inter alia*, the Aadhaar Act and associated

regulations as well as the IT Act and associated rules, by the Respondents as well as any data breaches of the Respondent's systems and the security measures and steps to be adopted to contain these breaches.

18. The Petitioner humbly submits that there is no other remedy available to it, except for approaching this Hon'ble Court by way of the present petition.

19. Respondent No.1 carries on its business in New Delhi where its office is situated. Accordingly, this Hon'ble Court has the territorial jurisdiction to entertain and decide the present Petition.

20. The Petitioner states that he has not filed any other proceeding in any court seeking the relief sought in the present Petition.

**PRAYER**

In view of the above facts and circumstances, the Petitioner humbly prays that this Hon'ble Court may be pleased to grant the following reliefs:

(i) Declare that the Respondents have breached the fundamental right of the Petitioner (as also all other Indian citizens holding an Aadhaar number) as guaranteed under Article 21 of the Constitution and as affirmed in *Justice KS Puttaswamy v Union of India*;

(ii) Declare that the Petitioner and other data subjects have the right to know of any breach of his/her data, as a part of the above said fundamental right(s);

(iii) Issue a writ of Mandamus directing the Respondents to release information on the number of data breaches which have taken place since the inception of the Respondent No.1 and the Aadhaar scheme, the extent/scope of such data breaches, the scope/extent/manner in which the Petitioner's data has been specifically compromised, and the steps taken by the Respondents towards remedying and rectifying their security practices pursuant to the breaches;

(iv) Issue a writ of mandamus directing the Respondent No.1 to comply with all its statutory duties/obligations to safeguard the Aadhaar data;

(v) Issue a writ in favour of the Petitioner directing the Respondents to immediately ensure compliance with the RSP Rules, including (a) publication of a privacy policy, and (b) laying down of an information security policy for itself and its core operations;

(vi) Issue a writ in favour of the Petitioner directing the Respondent No.2 to immediately form the agency mentioned under Rule 8 of the RSP Rules, if not already formed;

(vii) In the event the Respondent No.1 establishes that it has a comprehensive documented information security policy, direct the Respondent No.1 to demonstrate before the agency mandated under the law that it has implemented all reasonable security control measures as per the said policy;

(viii) Direct the Respondent No.1 and its personnel to undertake compulsory legal training on all aspects relevant to the protection of security/confidentiality/ privacy of Aadhaar data and the various rights of data subjects under the law;

(ix) Direct Respondent Nos.1, 2 and 4 to initiate appropriate action against Respondent No.3, including filing of a criminal complaint, for its failure to adhere to the security practices in violation of provisions of the Aadhaar Act, IT Act, and associated regulations in connection with the Srivastava Spoof;

(x) Appoint an independent investigative/audit committee comprising multiple stakeholders/experts to investigate and audit *inter alia* (a) all security and privacy breaches of the Aadhaar database, including the breaches outlined in this Petition and **ANNEXURE P/3**, (b) the robustness of the security systems and processes instituted by the Respondent No.1 and its affiliates/partners, as well as their security policies and practices,

operations, infrastructure, and procedures, and their compliance with the same (c) the extent of monitoring of affiliate/partner activities and security systems by Respondent No.1 including audits etc., (d) the extent of non-compliance by Respondent No.1 and its various affiliates/partners with the various statutory duties in relation to the security of the Aadhaar ecosystem, (e) the efficacy or otherwise of steps taken by Respondent No.1 in remedying and rectifying their security practices pursuant to the breaches, and any lapses in this regard and (f) the loss/destruction/unauthorized disclosure of/access to the Petitioner's own Aadhaar data by acts/omissions of the Respondents.

(xi) Award exemplary damages to the Petitioner in order to deter the Respondents from future negligent behavior that compromises constitutional /statutory/common law rights of the Petitioner and other Aadhaaris;

(xii) Grant liberty to the Petitioner and other Aadhaaris to claim more appropriate legal redressal including additional damages, where appropriate, based on the findings of the Investigative/Audit Committee;

(xiii) Grant the Petitioner the liberty to opt out of the Aadhaar system and issue a writ of mandamus to the Respondent No.1 directing the deletion of all the data relating to the Petitioner from the CIDR. As also the purging of this data or parts of it from all other systems where such data is available;

(xiv) In the alternative, issue a writ of mandamus directing the Respondent No.1 to deactivate the existing Aadhaar number of the Petitioner, permanently delete all data associated therewith, and re-issue a new Aadhaar number. Since the Aadhaar data of all Aadhaaris have been compromised, further direct the Respondent No.1 to permanently deactivate all existing Aadhaar numbers of the Aadhaaris and to not reallocate their old Aadhaar number to any other party;

(xv) Direct the Respondent No.1 to appoint a neutral ombudsman / verification authority for addressing all concerns and complaints at the first level, which may arise in the future in relation to violations of, *inter alia*, the Aadhaar Act and associated regulations as well as the IT Act and associated rules, by the Respondents as well as any data breaches of the Respondents' systems and the security measures and steps to be adopted to contain these breaches;

(xvi) To declare Section 46 of the Information Technology Act as unconstitutional and grant only a constitutionally competent court / tribunal the power to adjudicate a matter relating to the IT Act;

(xvii) Award costs of the proceedings in favour of the Petitioner; and

(xviii) Pass any such other and further orders in favour of the Petitioner as this Hon'ble Court may deem fit and proper in the facts and circumstances of the present case.

PETITIONER

Through