APPENDIX 1

OUR ORIGINAL NOTE SUBMITTED TO THE UIDAI ON 13 JULY 2010

HIGH LEVEL SUMMARY OF CONCERNS WITH THE DRAFT NATIONAL IDENTIFICATION AUTHORITY OF INDIA BILL, 2010

a) **Scope –** There is a need to limit and define in the preamble and relevant sections of the Bill the powers and purpose of the Authority and the overarching scheme of the bill. Further definition will act to prevent uncontrolled or unwanted change in the project's scope, and will clearly limit the usage of the Aadhaar numbers to their stated purpose of facilitating the delivery of social welfare programs. Specifically, we find the language in the preamble too broad, indirect, and unclear and we are concerned that the overbreadth and generality will open up the opportunity for more information to be collected than originally stated.

b) **Voluntary not mandatory –** The bill should take measures towards ensuring that the Aadhaar number is truly voluntary. Accordingly a prohibition against the denial of goods, services, entitlements and benefits (private or public) for lack of a UID number – provided that an individual furnishes equivalent ID is necessary. The denial of services to an individual with adequate identity should be made an offense under the Bill.

c) **Governance v. rights –** We find that the Bill inadequately elaborates on the principles relating to identity data. Instead it is largely focused on setting up of the authority and its functioning. While practical details of technical measures, procedures for enrollment or error correction, etc. may well be laid out in rules and regulations, the principles relating to identity data should be within the Bill itself. These principles are as follows, and should function as a set of standards and best practices that are to be applicable to any entity that handles Aadhaar numbers and/or identity data in any manner :

1. Exact specification of what data fields will be collected
2. whether, by whom else and on what terms the data may legitimately be accessed and/or used,
3. whether and on what terms data can be shared/disclosed and combined with other data fields
4. by whom and for how long data may be stored (including back ups),
5. under what circumstances data ought to be enabled or disabled/deleted/ anonymized/obfuscated,
6. how Aadhaar number holders can access and update their own records and view transaction history,
7. how Aadhaar number holders will be notified when their data is

accessed or its integrity/security is breached,

8. under what circumstances Aadhaar numbers can and cannot be published

Any violation of these principles/standards should be made an offense under the Bill.

d) **Exceptions –** We find that the bill does not provide adequate specificity as to who will be exempt from the issuance of an Aadhaar number. For example, it does not take into consideration a person's sexuality/sexual orientation and marital status/history. The Bill should provide an additional section detailing the circumstances and categories of people who will be excused or accommodated with respect to the issuing of Aadhaar numbers or authentication of transactions. The bill should also spell out the situations in which anonymity will be preserved and/or an Aadhaar number should not be requested. These situations need to be specifically annotated. If anonymity is violated in these situations, such offenses should be penalized.

e) **Liabilities and obligations of all other players in the ecosystem –** We find that the Bill holds only the Authority accountable for violations; it does not oblige the Registrars, enrolling agencies and other service providers who handle identity data and Aadhaar numbers to protect privacy, ensure data security and integrity, prevent misuse and otherwise be liable towards either the Authority and/or the Aadhaar number holders.

f) **Transaction data –** We find that in the Bill there is inadequate protection of collected data. After being assured by the UIDAI that the ultimate safeguard in the system is that it only provides for a binary Y/N response, and does not require a person to enter data or other information in response to an authentication request. In this regard, we find it worrisome that language such as is found in 5(2) ("or with any other appropriate response") is still used in the draft. Vague language as this should be deleted. The Bill should require the Authority, Registrars, enrolling agencies and service providers to delete/anonymize/obfuscate transaction data according to defined principles after appropriate periods of time.

g) **Inadequacy of penalties –** We find that In the bill, the penalties provided are inadequate, because they do not cover several types of misuse. They are also flawed to the extent that they do not provide any relief to the person whose data was lost/stolen/abused etc. Furthermore, simply authorizing Imprisonment and fines against those who violate the bill does not sufficiently redress the offenses against the Aadhaar number holders who have suffered. Furthermore, the Authority, Registrars, and Enrolling Agencies should all be held to the same regulatory standards.

h) **Fees:** We find that there is inadequate definition in the bill of what fees shall be applied for authentication of Aadahaar numbers. Furthermore we find that it is incompatible with the bill's stated purpose to require an individual to pay to be authenticated. The Bill should provide that no charges will be levied for authentication by registrars and other service providers for certain categories of Aadhaar number holders (BPL, disabled, etc.), and that charges will be limited/capped in other cases. This will bring the bill in line with the statement in Chp II 3 (1) "Every resident shall be entitled to obtain an Aadhaar number on providing his demographic information and biometric information to the Authority in such a manner as may be specified by regulations" and Chp 3 (10) The Authority shall take special measures to issue Aadhaar numbers to women, children, senior citizens, persons with disability, migrant unskilled and unorganized workers, nomadic tribes or such other persons who do not have any permanent dwelling house and such other categories of individuals as may be specified by regulations. If a fee must be permitted, a cap/safeguard should be put in place to ensure that the fee does not become a mechanism of abuse.

i) **Rollback and Ombudsman –** we find that In the bill there is inadequate action taken for the remedying of transactions wrongly denied due to system errors. It is suggested that the Bill spells out a procedure for the rollback of transactions wrongly effected due to identity theft, other types of fraud or errors during authentication, as well as for the remedying of transactions wrongly denied due to false negatives or system errors (This procedure is analogous to processes followed by credit card issuers and financial institutions). The independent oversight and a redressal mechanism could be provided by an autonomous ombudsman *as an additional solution*.

j) **Structure and governance –** We find that In the bill, the process by which the Authority is appointed is inadequate, and that the bill inadequately sets forth the qualifications necessary,. In addition, the limited functions of the review committee,are not set forth in sufficient detail,. There also is not enough provision for appropriate judicial and parliamentary oversight. For example, the Authority has three members. If one member may abstain in circumstances where he/she has disclosed an interest, there may be a resulting deadlock when the remaining two members take a decision (found in section 18 (5). We recommend that the section provide a mechanism for the avoidance/resolution of deadlock situation. Adding such a provision will serve to bring the bill in line with the constitutional requirements for parliamentary oversight)

k) **Potential dilution of banking norms and other legislation –** In the bill, the proposed sufficiency of an Aadhaar number for account opening and banking transactions is in conflict with Know Your Customer norms and other banking norms followed by the Reserve Bank of India and the Securities and Exchange Board of India, as well as with other statutes and policies that require

identification*]*.

l) **<u>Responsibility for subcontracting/delegation</u> –** In the bill there is inadequate regulation of what data are outsourced. This is demonstrated by the lack of accountability that is placed upon subcontractors and service providers. We recommend that the bill prohibit the delegation and outsourcing of certain types of critical activities and functions. This would include hosting and maintenance of the CIDR. If information must be outsourced, safeguards should be included in the bill to limit the selection of such entities and to set forth in detail the criteria that should be used and the penalties if the outsourced or other entity violates any provisions in the bill.

Any violation of these principles/standards should be made an offense under the Bill.