High Level Summary and Critique to the Leaked Right Privacy Bill 2011

The leaked Right to Privacy Bill 2011, drafted by the Ministry of Law, seeks to create a privacy right for the citizens of India. Though the Bill begins to establish a strong framework for the protection of the right to privacy in India, there are many ways in which the Bill can be improved and changed to bring about a more comprehensive right that ensures that privacy does not generate over- or under-inclusive remedies. Below is a high level critique of the Bill and recommendations as to how it could be improved.

1. Definitions Section 2

- *(ix) 'Data Controller' is any entity that processes personal data...*
  We recommend that the definition of a data controller be changed from anyone who processes personal data to anyone who directly or indirectly uses, has access to, and or can see and modify personal data. Additionally we recommend that the distinction between Data Controller and Data Processor is eliminated, as any entity who processes personal data should be held to the same standards and obligations as any entity that controls personal data.
- *(xvii) 'Interception of Communication' means if a person in the course of transmission by means of a telecommunicataion system: (a)modifies or interferes with the system, (b) monitors transmission made by means of the system, (c), monitors transmission made by a wireless telegraph"*
  We recommend that the interception of communications should broadly include the 'monitoring of transmissions', rather than the 'monitoring of transmissions made by means of the system.
- *(xxi)'Person' means any natural or legal person*
  We recommend that the Bill is consistently use of the term 'person' – sometimes using natural and sometimes using legal.
- *(xxii) 'Personal data' means any data which relates to a living, natural person if that person can, either directly or indirectly in conjunction with other data from that the data controller has or is likely to have, be identified from that data and includes any expression of opinion about that person."*
  We believe that the definition of 'personal data' is better limited to "any data which relates to a living, natural person if that person can by identified from that data. Data does not need to be held by a data controller to be personal data.
- *(xxiv) "Processing" means any operation or set of operations whether carried out through automatic means or not that relates to: (a) the organization, collation, storage, updating, modification, alteration, or use of personal data (b) the merging, linking, blocking, degradation, erasure or destruction of personal data.*
  Throughout the Bill, the term 'processing' is used as an enabler. Specifically, Section 12(1) lists circumstances by which entities or institutions do not need prior authorization to process personal sensitive information. In this context, we believe that standard processing of personal data should not entail the merging or linking of data. Data should be collected and used only for the stated purpose, and if merging or linking will take place, this should be stated. Furthermore, we recommend that this definition is revised and broken into two sections. One section that states the privacy enforcing actions that relate to the processing of data including: organization, collation, storage, updating, modification and one section that states the processes that detract from individual privacy including: merging, linking, blocking, degradation, erasure or destruction.
- *(xxvii) 'Sensitive Personal Data' of an individual means personal data relating to: Unique*

Identifier as Aadhaar number or PAN number, physical and mental health including medical history, biometric or genetic information, criminal convictions, banking credit and financial data, narco analysis and/or polygraph test data.

To the definition of sensitive personal data we recommend that 'location, race, religion, and sexual preference' is added.

- *(xxix)'Surveillance' means obtaining personal data about an individual and his private affairs...*

  We recommend that to the definition...'which capture images to identify or monitor individuals' – sounds be added as sounds can be mapped and also used to identify individuals.
- We recommend that a definition of "public places" be included in the Bill.

2. Citizens vs. Residents Section 3: Currently, the Bill extends the right privacy and the protection over personal data to the citizens of India. We recommend that the Bill extend the right to privacy and protection of personal data to all residents of India.

3. The Right to Privacy Section 3&4: As first noted by Apar Gupta in his critique of the first leaked version of the Bill,[i] the Bill provides for the Right to Privacy and establishes that every individual has a right to privacy, which is subject to any law for the time being in force. This works to weaken the right of privacy, as any existing law which is in conflict with the mandates of the Privacy right will override the provisions of the Bill. Section 4 of the Bill also specifies six instances as to when the right to privacy can be infringed upon. Similarly, Article19(1)(a) of the Constitution of India has established six circumstances under which the Right to Freedom of Speech can be infringed upon.

- in the interests of the sovereignty and integrity of India
- the security of the State
- friendly relations with foreign States
- public order
- decency or morality
- or in relation to contempt of court, of defamation or incitement to an offence.

The six circumstances laid out by the Privacy Bill are not analogous to those laid out in the constitution, and in some cases go beyond the circumstances established in the constitution. These include:

- strategic, scientific, or economic interest of the state
- protection of rights and freedoms of others
- Any other purposed specifically mentioned in the Act.

We recommend that the circumstances by which individual privacy can be infringed upon be brought in line with the circumstances laid out in the Constitution. Specifically, we recommend that the condition found in section 4 (vi) 'any other purposed specifically mentioned in the Act' be deleted.

4. Infringement of Privacy Section 5: This section establishes that unauthorized: collection, processing, storage, and disclosure of personal data, interception of personal communications, surveillance of an individual, and unsolicited communications constitutes and infringement of privacy. The subsequent provisions of the Bill focus on elaborating these areas of infringement. In the process, the Bill creates a legal structure of privacy that focuses both on the protection of informational and personal privacy, but does so in a disjointed and unconnected way that overlooks protections such as defamation and protection against unreasonable search and seizure. We recommend that the Bill synergize the two seemingly separate protections of informational privacy and personal privacy by

recognizing that for both, the right of privacy is a property right. By using property as the starting definition of privacy, the Bill will not give an individual a fundamental right to privacy that is then eroded or sporadic. Protection of privacy as one's property will allow the Bill to protect both data that are related to and generated by individuals (by requiring their consent and, in proper cases, compensation for its use), and it will allow for an individual to be protected from unreasonable search and seizure, allow for his name not to be defamed or misused, and allow for privacy over information related to his private and family life – all of which can be readily analogized to someone's property.

5. Collection of Personal Data Section 9: This section establishes that personal data does not need to be collected directly from the individual in the case that the information is already public or the data subject has already consented to the collection of personal data from another source. We recommend that this section require that the consent given by the data subject from another source include: applicability, purpose, and duration of the consent given.

6. Processing of Sensitive Personal Data Section 12(1): This section states that personal data cannot be collected or processed unless authorized by the authority. The Bill then lays out instances when authorization for the collection and processing of personal data by the authority is not needed. Of these we find the following concerning:

(v) "data relating to biometrics, physical or mental health, prior criminal convictions is processed by the employer of the data subject for the purpose of an in connection with the employment of the data subject". We believe that employees should have limited access to personal information, and that is not necessary for them to access the health or biometric information of potential employees.

(vii) "data relating to criminal convictions, biometrics, and genetic is processed and collected by law enforcement agencies." We believe that though law enforcement agencies should be allowed to verify an individuals biometrics, they should not be allowed to collect and process biometrics and genetic information without prior permission and without following a specified procedure.

(viii) "sensitive personal data is processed by schools or other eduction institutions in connection with the imparting of education to the data subjects." We believe that the types of personal sensitive information that is required by education institutions need to be specified as it is not necessary for educational institutions to have access to an individuals banking information, biometric or genetic information, or narco anaylsis/ polygraph information.

(ix) 'the authority has by a general or specified order permitted the processing of specified sensitive personal data for specific purposed and if possible is limited to the extent of such permission. This section is in direct conflict with section 10(2) which states 'A data controller shall collect and process only such type and amount of of personal data as is absolutely necessary to fullfill the documented purpose.' To bring these two sections into agreement we recommend that the phrase ' if possible' is deleted from section 12(ix)

7. Retention of Personal Data Section 13: This section establishes standards and circumstances for the retention of personal data. We recommend that of these 13(1)(iv) 'it is required to be so retained for historical, statistical, or research purposes' be deleted as it is too easy for sites such as Facebook to claim that the retention of personal data is necessary for statistical or research purposes.

8. Security of Personal Data Section 15: Specifically, section 15(3) holds the data processor and data controller responsible for ensuring that personal data is used only for the purpose for which it was collected, it is kept secure, and that it is not disclosed to a third party. Section 15 (4) maintains that if any violation of the provisions takes place, both the data controller and the data processor will be held

jointly and severally liable under the act. Similarly, section (2) holds the data controller responsible and liable for any security breach of data that is transferred outside of the territory of India. Though we believe that it is important that data processors and data controllers are responsible for designing and adhering to a security architecture, and that it reasonable to hold the data processor and controller liable for compliance with contractual agreements and third party disclosures, we do not believe that it is reasonable to hold them souly liable for a breach of security, as these are often out of the hands of the controller and processor.

9. Interception of Communications Sections 23, 24, 25: Though we agree with the standards laid out under this section, it is unclear if how these provisions will comply with the regulations laid out in the Telegraph Act, the Lok Pal Bill, or the Information Technology Act. Will the most recent Act take precedence? Will the sector specific Act take precedence? Furthermore, we recommend that the standards safeguarding the interception of communications be kept at the same level as the Telegraph Act. Specifically 24(1)(ii) 'interception shall only be undertaken with the sanction of the competent authority and only after the **competent authority** has satisfied itself that the required information could not be reasonably obtained by other means and that the intended interception is proportionate to the objective sought to be achieved' and 24(1)(iv) interception shall be for **minimum period required for achieving the objective** for which it is authorize and the permission to intercept will cease immediately thereafter" are both lower standards than established in the Telegraph Act. For example, the 2007 rules of the Indian Telegraph Act, 1885 mandate that an order must be issued by an officer not below the rank of 'Home Secretary Ministry of Home Affairs, Government of India and the Home Secretaries of the State Governments'[ii] while Section 24(1)(ii) of the leaked Bill mandates that an order be sanctioned by a 'competent authority'. Additionally, the 2007 Telegraph Rules maintain that interceptions can only take place for a duration of 6 months before the intercept order must be re-approved.[iii] In a dilution of this standard, section 24(1)(iv) of the leaked Bill holds that interceptions can take place for the minimum period required for achieving the authorized objective. Lastly, we recommend that section include regulations for transparency and breach notification. Thus, at the end of a certain amount of time, the authority will publicly disclose how many intercepts it has undertaken and for what duration. Additionally, after an interception has been completed the individual under investigation will be made aware of the purpose and duration of the intercept.

10. Surveillance Section 26, 27, 28, and 29: These sections regulate the use of CCTV cameras and covert surveillance. Section 26 specifically addresses the installation & use of CCTV cameras, but leaves the exact procedure to be later defined in subsequent regulations. We recommend that certain safeguards specifying what constitutes a 'legitimate objective', 'proportionate objective', and 'prescribed procedure' be laid out in the Bill itself. The section also states that the operation of CCTV cameras will not be undertaken to identify an individual. We recommend this phrase is deleted as the purpose of CCTV cameras is for law enforcement to record crime, and to identify and stop the perpetrator. In section 27 'Protection of CCTV images' we recommend that the terms 'video and audio' also included. Section 28 prohibits covert surveillance unless authorized to do so for any of the following objectives: (i)National Security or public safety, (ii) Prevention or deletion of a crime, (iii) Apprehension of offenders, (iv)Economic well being of the State (v) Protection of public health (vi) Assessment or collection of any tax, duty, or other government charge. These exceptions are different from the exceptions to privacy laid out in section 5, and still go beyond the circumstances laid out in section 19(1)(a) of the constitution. We recommend that all exceptions in the Act be made the same and are reflective of section 19(1)(a) of the constitution. Additionally we recommend that the provision establishes an appropriate framework for surveillance to take place in the case of sting operations and investigative journalism. Lastly, we recommend that the section on surveillance be placed in a broad framework that requires that surveillance be undertaken in a way that is: proportional, transparent, and

imminent.

12. Sections to be added:

- *Right to request personal information from the government:* We recommend that a provision is added providing individuals with the right to request from the government 1. personal information that they have previously given 2. information relating to how their personal information was used 3. and notification as to who accessed their information and for what purpose.
- *Permitted Circumstances for Governmental Collection of Information:* We recommend the creation of a provision that lays out the circumstances under which personal information can be collected by a government institution including: 1.upon written request by an investigative body for the purpose of enforcing any law or for carrying out lawful investigation, 2.collection for research and statistical purposes after execution of a written agreement assuring the individual that no subsequent disclosure of the information will be made in a form that could lead to identification of the individual, 3. for collection and aggregation prior to dissemination to the public, 4. for the provision of welfare services, 5. for the collecting and recording of taxes.

i http://www.iltb.net/2011/06/analysis-of-the-privacy-bill-2011/
ii 2007 Interception Rules to the Telegraph Act Section 2 http://www.dot.gov.in/Acts/English.pdf
iii 2007 Interception Rules to the Telegraph Act Section 6