COMMENTS TO THE DNA TECHNOLOGY (USE AND APPLICATION) REGULATION BILL, 2019

1. PRELIMINARY

This submission presents comments on the DNA Technology (Use and Application) Regulation Bill, 2019[1] ("**Bill**") introduced in the Lok Sabha on 8 July 2019. The submission highlights: (i) broad concerns with the Bill; and (ii) concerns with specific provisions of the Bill with recommendations to address the same.

2. OVERARCHING CONCERNS AND RECOMMENDATIONS

2.1. Overlap with existing laws

There is substantial overlap between the provisions of the Bill, the Indian Evidence Act, 1872 ("**Evidence Act**") and the Code of Criminal Procedure, 1973 ("**CrPC**"). For instance, the CrPC deals with the procedure for the examination of an accused person or a victim using DNA samples,[2] which are also envisaged under the Bill. There is also significant case law around these provisions in the Evidence Act and the CrPC, which has been developed over the years. If the Bill contains provisions governing the same subject as existing instruments, it would lead to ambiguity as to the correct position of law. This would also undo the jurisprudential effort invested into establishing the law on this subject as it stands today. Given that the Bill is a special law on the subject of collecting DNA evidence, it may prevail over existing provisions of the CrPC. We recommend that the Bill clarify any overlaps with existing laws and reflect principles relating to privacy and the right against self-incrimination that have developed over the years.

2.2. Broad ambit of the Bill

The Bill seeks to profile offenders[3], persons who are suspected of committing an offence or are under trial[4], persons who were present at the scene of a crime[5], persons who are being questioned in connection with the investigation of a crime[6], victims or suspected victims of a crime[7] (collectively, 'persons related to criminal proceedings'), and persons who want to locate their missing relatives[8], and unknown deceased persons[9] (collectively, 'persons not related to criminal proceedings'). We believe that distinct DNA profiling frameworks must exist for persons related to criminal proceedings as against persons who are not related to criminal proceedings. Pertinently, while the Magistrate may order collection of bodily samples of persons suspected or accused of committing a crime without their consent, s/he should not have this power over persons who are not related to criminal proceedings. Therefore, different consent and retention standards should be devised for these distinct categories of people. Pertinently, we believe that consent given for civil purposes or on a voluntary basis should be time capped to one year to strengthen privacy safeguards under the Bill.

2.3. Lack of safeguards against errors in DNA profiling

[1] The text of the Bill is available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/128_%202019_LS_eng.pdf.
[2] These include blood, blood stains, semen, swabs, sputum, sweat, hair samples and finger nail clippings by the use of modern and scientific techniques including DNA profiling under sections 53 and 53A of the CrPC.
[3] Section 26 (1) (c), Bill.
[4] Section 26 (1) (b), Bill.
[5] Section 22 (1) (a), Bill.
[6] Section 22 (1) (b), Bill.
[7] Proviso to Section 23 (2) (b), Bill.
[8] Section 22 (1) (c), Bill.
[9] Section 26 (1) (e), Bill.

2.3.1. DNA technology is not fool-proof[10] and may give false positives[11], which the Bill does not safeguard against. The Bill does not envisage an appeals process against the findings of a DNA laboratory which adversely affect people in court. There is only the limited exception for when an accused is able to prove that the sample was contaminated[12]. This is an extremely onerous burden, especially in light of the fact that DNA technology may not always give accurate results. The Bill should incorporate safeguards for people who may be adversely affected by such inaccurate findings in the course of criminal proceedings. This may take the form of having the same sample tested by multiple entities, stipulating a high threshold beyond which similarity in DNA profiles may be considered a 'match'.

2.3.2. As discussed, DNA profiling is not a foolproof method[13][14]. Hence, we recommend that the Bill contain an explicit prohibition against convicting a person solely on the basis of DNA evidence. For this, the Bill must distinguish between what is an acceptable and unacceptable sample and must also prescribe strict standards for the chain of custody of the evidence.

2.4. Technical competence of the DNA Regulatory Board ("**Board**")

In its current form the Bill empowers the central government to nominate nine out of twelve members of the Board. However, the Bill does not prescribe any basis like technical qualification or amount of experience for its nomination. This may compromise the technical competence of the Board. We recommend that the Bill prescribe technical qualifications for members to be nominated by the central government to ensure technical competence of the Board.

3. SPECIFIC CONCERNS AND RECOMMENDATIONS

3.1. Undefined and broad terms

3.1.1. Meaning of consent: The Bill allows certain entities to collect, process and store DNA related data of individuals by obtaining 'consent' of the individuals. It does not, however, clearly define consent. Data collected under the Bill can qualify as 'genetic data' and 'health data', both of which are considered sensitive personal data under the draft Personal Data Protection Bill, 2018 ("**PDP Bill**"). Collecting and using such data carries a higher risk of harm to individuals and should, thus, be subject to a higher set of safeguards. The Justice K.S. Puttaswamy vs. Union of India ("**Puttaswamy I**") judgement[15] lays down nine privacy

[10] The Guardian, DNA in the dock: how flawed techniques send innocent people to prison, dated 2 October, 2017, *available at* https://www.theguardian.com/science/2017/oct/02/dna-in-the-dock-how-flawed-techniques-send-innocent-people-to-prison; BBC News, DNA test jailed innocent man for murder, dated 31 August, 2012, *available at* https://www.bbc.com/news/science-environment-19412819.
[11] Matthew Shaer, The False Promise of DNA Testing, The Atlantic, June 2016 Issue, available at https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747/.
[12] Section 24, Bill.
[13] The Guardian, DNA in the dock: how flawed techniques send innocent people to prison, dated 2 October, 2017, *available at* https://www.theguardian.com/science/2017/oct/02/dna-in-the-dock-how-flawed-techniques-send-innocent-people-to-prison; BBC News, DNA test jailed innocent man for murder, dated 31 August, 2012, *available at* https://www.bbc.com/news/science-environment-19412819.
[14] Matthew Shaer, The False Promise of DNA Testing, The Atlantic, June 2016 Issue, available at https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747/.
[15] *Justice K.S. Puttaswamy* vs. *Union of India*, Supreme Court of India WP(C) 494 of 2012.

principles[16]: i) notice[17], ii) choice and consent[18], iii) collection limitation[19], iv) purpose limitation[20], v) access and correction[21], vi) disclosure of information[22], vii) security[23], viii) openness[24] and ix) accountability[25]. Specifically, for law enforcement agencies processing data (which is a State action), the three-part test discussed in *Puttuswamy*[26] should be met: (i) existence of a law; (ii) the law seeks to pursue a legitimate aim; and (iii) the law is proportionate to the aim sought to be achieved. Among other things, proportionality requires that an individual should not be disproportionately affected by the law. Given that DNA-related data is sensitive and carries a high risk of harm to individuals, the law should clarify what consent means, under what circumstances it would be considered free, and include sufficient safeguards to guard against coerced consent. Further, we suggest that the Bill should have adequate safeguards against investigation agencies taking forceful or coerced consent. One such method is to ensure that the consent is taken and recorded before the Magistrate.

3.1.2. Broad scope of 'associated': Section 2(1)(iv)(d) (definition of 'Crime scene index') includes DNA samples found on or within the body of a person, or on anything, or at any place, 'associated' with the commission of an offence[27]. The word 'associated' is excessively broad and empowers of the investigating authorities to collect bodily substances from *any* persons/places/things who they suspect is associated with the crime. The DNA molecule is stable in a variety of conditions and spreads easily making the presence of one person's DNA at a crime scene, a matter of chance[28]. Therefore, we recommend that section 2(1)(iv)(d) which gives an overarching definition of a crime scene index to include DNA samples on any thing, person or at any place 'associated' with the commission of an offence should be removed since it defeats the principle of collection limitations.

[16] Para 184, Puttaswamy I.
[17] A data controller shall give simple-to-understand notice of its information practices to all individuals in clear and concise language, before personal information is collected.
[18] A data controller shall give individuals choices (opt-in/optout) with regard to providing their personal information, and take individual consent only after providing notice of its information practices.
[19] A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means.
[20] Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which it is processed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. Data retention mandates by the government should be in compliance with the National Privacy Principles.
[21] Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion of such information where it is inaccurate; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data. Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure.
[22] A data controller shall not disclose personal information to third parties, except after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information.
[23] A data controller shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorised access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure [either accidental or incidental] or other reasonably foreseeable risks.
[24] A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.
[25] The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the Privacy Commissioner and comply with the specific and general orders of the Privacy Commissioner.
[26] *Justice K.S. Puttaswamy* vs. *Union of India*, Supreme Court of India WP(C) 494 of 2012.
[27] Section 2 (1) (iv), Bill.
[28] The Wire, DNA Technology Bill: Why the Standing Committee Has Its Work Cut Out, dated 01 November 2019, *available at* https://www.bloombergquint.com/opinion/the-dna-bill-another-invasive-imperfect-databasehttps://thewire.in/government/dna-technology-bill-2018-databank-parliamentary-standing-committee-privacy-consent.

3.2. The role of a Magistrate

3.2.1. Specified offences: Under Section 21 (1) of the Bill, investigating officers are not required to obtain consent from individuals arrested for specified offences (which are offences punishable with death or imprisonment above 7 years). It also appears that a Magistrate's order is not required for collection of bodily samples in investigations relating to specific offences. We recommend that consent of the individual or at least a Magistrate's order should be required before collecting bodily substances from a person accused of a specified offence. This will ensure that investigation agencies do not abuse this provision in cases of specified offences.

3.2.2. Voluntary submission of bodily samples: Section 22 of the Bill allows certain people to voluntarily give their bodily substances for examination, such as people seeking to locate their missing relatives, persons present at a crime scene, and persons being questioned in connection with the investigation of a crime[29]. Under the Bill, a Magistrate may effectively bypass such a person's consent if s/he is below the age of 18 years[30]. This raises a few concerns. First, the section seeks to govern persons who are giving their bodily substances 'voluntarily'. If the voluntary nature of this act is missing, their bodily substances should not be collected to begin with. Collecting bodily substances of a person (who is not required to do so for investigative purposes) without the consent of that person effectively violates the principle of 'choice and consent'. This provision virtually takes away the opt-out option from the person providing the bodily substance. In the absence of any necessity the Magistrate should not be allowed to bypass consent even for minors.

3.2.3. Safeguards for collection of bodily samples without consent: In cases where bodily substances of an arrested person are sought for law enforcement (for non-specified offences) and if that person refuses consent[31], adequate safeguards should be built in to ensure that this provision is not misused by investigating authorities. Collection of bodily samples by investigating officers without consent must satisfy the triple test discussed in Puttuswamy I[32]("**Triple Test**"). The triple test comprises the following legs: i) the existence of a law, ii) legitimate state aim, and iii) proportionality. Existence of law requires that there must be a law to justify an encroachment on privacy. Legitimate state aim requires that nature and the content of the law which imposes the restriction must fall within the zone of reasonableness mandated by Article 14 of the Constitution of India. Proportionality requires that the means adopted by the legislature must be proportionate to the object of the restriction. We recommend that elements of the Triple Test be built into the provision to ensure any collection is consistent with an individual's right to privacy.

The proportionality test itself comprises four limbs[33]. First, any legislation restricting a fundamental right must have a legitimate goal; second, the restriction must be a suitable mean of furthering the legitimate goal; third, there should not be any alternative method which is less restrictive of the fundamental right, though equally effective; and fourth, the holder of the right should not be disproportionately impacted. To ensure sufficient checks, we recommend a person should be allowed a hearing before the Magistrate to explain his/her reasons for not consenting. After this, the Magistrate may decide whether to order collection, despite lack of consent by the individual. On similar footing, the Bill should include language suggesting that the Magistrate should have the power to order collection only when there are no other less restrictive and equally effective alternatives to achieve the desired goal. DNA technology may sometimes churn out false positives if it is not

[29] Section 22, Bill.
[30] Section 22 (2) and the proviso to section 23 (2) (b), Bill.
[31] Section 21 (1), Bill.
[32] Puttaswamy I recognized the fundamental right to privacy to be a part of Article 21 of the Constitution of India.
[33] Para 267, Puttaswamy I.

properly collected or processed[34] which indicates that it may not be the most reliable method[35] to establish the identity of a person correctly unless done as per prescribed standards. For instance, DNA testing is known to be marred both by untrained personnel[36] and contaminated samples[37]. This may lead to false convictions of the persons whose DNA is analyzed. Thus, its use should be limited to instances where other methods are unavailable.

Accordingly, we recommend that section 22 (2) and the proviso to section 23 (2) (b) (which deals with the collection of bodily substances for DNA testing of a victim or a person reasonably suspected of being a victim who is alive) should be amended to give a proper opt-out option to the individual whose bodily substances are sought. The provisions should also contain sufficient safeguards or grounds basis which a Magistrate may grant an order for obtaining bodily substances of an individual.

3.3. Databanks to store obtained data

3.3.1. The Bill states that all DNA data, including profiles, samples and records shall only be used for identifying a person and not for any other purpose[38]. Further, the Bill provides for retention of DNA data contained in the crime scene index[39]. The Bill lays down the procedure to remove DNA data from National DNA Data Bank in certain specific cases[40] such as DNA data of a suspect after the police report is filed and of an under trial as per the order of the court. However, a person who is neither an offender nor a suspect or an under trial must make a written request to the National DNA Data Bank to have his/her DNA data removed from the crime scene index or missing persons' index[41]. These provisions raise a few concerns.

3.3.2. This suggests that DNA data of some persons is not automatically deleted once it has served its purpose, but requires an express request to this effect.[42] The Bill does not require the national or regional DNA Data Banks to convey this option to the person whose DNA sample has been collected. A person who is not aware of this right, may not exercise it which may allow the data to be used for purposes other than those mentioned in the Bill[43]. These risks may be exacerbated in cases of data breach, through which data may fall in the wrong hands. There is also no way of verifying whether a person's DNA profile is deleted even after requesting the same.

3.3.3. We recommend that a person whose DNA is being obtained should be informed that they have a right to request for their DNA data to be removed in certain circumstances. This intimation should be done at the time of the 'collection' by the person collecting the sample and by the Magistrate during the 'trial'. Further, we recommend that section 31 (2) (i) should be amended to ensure that a suspect's DNA data is removed from both the suspects' index and the crime scene index.

[34] The Guardian, DNA in the dock: how flawed techniques send innocent people to prison, dated 2 October, 2017, *available at* https://www.theguardian.com/science/2017/oct/02/dna-in-the-dock-how-flawed-techniques-send-innocent-people-to-prison; BBC News, DNA test jailed innocent man for murder, dated 31 August, 2012, *available at* https://www.bbc.com/news/science-environment-19412819.
[35] Matthew Shaer, The False Promise of DNA Testing, The Atlantic, June 2016 Issue, available at https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747/.
[36] Matthew Shaer, The False Promise of DNA Testing, The Atlantic, June 2016 Issue, available at https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747/.
[37] Stephen Leahy, Alleged Golden State Killer Busted by DNA. But Are Tests '100%' Accurate?, National Geographic, dated 25 April 2018, available at https://www.nationalgeographic.com/news/2018/04/dna-testing-accuracy-golden-state-killer-science-spd/.
[38] Section 33, Bill.
[39] Section 31 (1), Bill.
[40] Sections 31 (2), (3) and (4), Bill.
[41] Section 31 (3), Bill.
[42] Section 31(3), Bill.
[43] Section 33, Bill.

3.3.4. The option of obtaining DNA samples data without proper consent and its retention creates concerns of enabling a surveillance state. To counter this, we recommend that a section for auto-destruction of DNA data, once its purpose has been served, should be added. This should be done within a reasonable time frame and conform to the privacy principles as laid down in the Puttaswamy I judgement.

ABOUT IKIGAI LAW

Ikigai Law is a law firm that specializes in representing technology businesses, investors, and start-ups, to more mature companies focused on new business models. We work with our clients on regulatory and policy issues, private equity and venture capital investment transactions, mergers and acquisitions and other commercial transactions, intellectual property, and disputes. Our work is at the intersection of law, policy, regulation, technology and business, engaging with crucial issues such as data protection and privacy, fin-tech, online content regulation, platform governance, digital competition, cloud computing, net neutrality, health-tech, blockchain and unmanned aviation (drones), among others.

***