5TH SYMBIOSIS LAW SCHOOL, HYDERABAD, NATIONAL MOOT COURT COMPETITION – 2021

MOOT PROBLEM

1. The Country of Republic of Zindia ("**Zindia**"), the laws of which are *para-materia* to the laws of Republic of India, is a country which has seen a huge population boom in few of its cities in the past few decades. Zindia is not only the country with the second largest population in the world but its ranking is also substantially high in population density. Problem arose when there was an unprecedented outbreak of a pandemic in February 2020 i.e. the novel coronavirus ("**COVID-19**") in the entire world and the densely populated cities of every country were the most affected, both healthcare and infrastructure wise. Similar to the situation in other countries, big cities in Zindia were badly affected by COVID-19. Since majority of Zindia's revenue comes from industries and offices located in its big cities and these big cities were the ones which were worst hit, the economic downturn inadvertently was a side effect of COVID-19. Like all other governments across the world, Government of Zindia ("**Government**") was grappling to get the situation under control and was leaving no stone unturned to contain and control the situation and get the economy back on its feet.

2. The Government has realized during the past few years that Zindia has a huge reservoir of data, due to its large tech-adopting population. The Government, through multiple policies and white paper, has expressed that the data of its citizen is a resource of the country (as valuable as oil) and the country and/or its Government has the right to tap that resource and prevent government of foreign countries and foreign entities from utilizing such resource in an unrestricted manner. The Government notified and enacted the Personal Data Protection Act 2019 ("**Act**"), immediately after the winter-session of the Parliament in 2019 i.e. on 31 January 2020, which laid the foundation for the ability of the Government to tap Zindia's data resources, by restricting the flow of Sensitive Personal Data (*as defined under the Act*) of its citizens outside its territorial boundaries.

3. In an effort to tackle the COVID-19 situation, the following notifications were issued in the form of executive orders from the respective offices of various ministries of the Government:

Key points of the notification	Concerned Ministry	Date of issuance
The nation shall be under complete lockdown and any violation of the lockdown order shall be a punishable offense under Section 188 of the Zindian Penal Code 1860.	Ministry of Home Affairs	Multiple orders across several dates.
The COVID-19 situation is a natural disaster that can be categorised as a disaster under the (Zindian) Disaster Management Act 2005.	Ministry of Home Affairs	24 March 2020
Parties to commercial contract may invoke force majeure event due to the COVID-19 situation.	Ministry of Finance	19 February 2020
Supply of all drugs allowed via online and doorstep delivery including Schedule H drugs.	Ministry of Health and Family Welfare	26 March 2020

4. Further, following the Singapore model, the Government introduced a medicine delivery app ("**App**") in tie-up with a foreign medicine company "**Cobalt**" for doorstep delivery of flu related drugs, masks, and sanitizers. Also, the App helped a user to avoid coming in contact with any person who has tested positive for or is possibly infected with COVID-19, by raising an alarm notification in the App. The key highlights of the App's privacy policy framed as per Section 22 of the Act ("**Privacy Policy**") are as follows:

(a) Clause 1 of the Privacy Policy, states that the App collects only the following Personal Data and Sensitive Personal Data (*as defined under the Act*) from a user when he is registering on the App: (i) name; (ii) phone number; (iii) age; (iv) sex; (v) profession; (vi) caste and religion; (vii) countries visited in the last 30 (thirty) days; (viii) smoking habits; (ix) person's current medical condition (collected through questions, microphone of the device, tracking activity such as coughing or sneezing); (x) live location data of the registered user; and (xi) Aadhaar Card details ("**Personal Data Sets**"). The users of the App are required to consent to the collection and processing of these Personal Data Sets as per Clause 2 of the Privacy Policy.

The Personal Data Sets which are collected from the users are transferred on a real time basis to and kept in the servers of a third-party cloud service provider (having their servers outside India), so that the data can be easily accessed anytime and from anywhere. However, a back-up copy of the Personal Data Sets was also stored by Cobalt in servers located within the territorial boundaries of Zindia, in order to comply with the Act.

(b) Clause 2 of the Privacy Policy states that: "*The Personal Data Sets collected will be used only by Cobalt and its users. The Personal Data Sets which is processed by Cobalt will be used for the purpose of informing the users or those people with whom the user has come in contact with, of possible infection, in an anonymized form, without disclosing the identity of the infected person. In case any user has tested COVID-19 positive, his/her Personal Data Sets may be shared by Cobalt with such necessary and relevant Governmental authority or Government appointed healthcare facility, as may be required, in order to carry out necessary medical and administrative interventions. The Personal Data Sets collected will not be used for any purpose other than those mentioned in this Clause, unless otherwise is required by an order of the Government for a lawful purpose."*

(c) Clause 7 of the Privacy Policy states that: "*The parties shall be exempted from performing their obligations in the case of a force majeure event*." However, a 'force majeure event' was not defined in the Privacy Policy.

5. During the initial phase of the lockdown in Zindia, certain posts were circulated on various media platforms, which demonstrated that a community belonging to a minority religion called '*ABC Jamal*" was the reason for the spread of pandemic in Zindia. This led to lynching of certain individuals from that community in various parts of the country. The Government through the Ministry of Home Affairs issued a notification under Section 35 of the Act dated 30 March 2020 ("**Notification**") which stated the following: "*Certain terrorist organisation sponsored by a neighbouring state 'Xina' are exploiting the COVID-19 situation to cause panic and riot in Zindia. Therefore, in order to protect the interest of sovereignty and integrity of Zindia and the security of the state of Zindia, (i) the Government may process the Personal Data Sets that is collected by Cobalt and/or the App in India, in any manner it may deem fit and the provisions of the Act will not be applicable to such processing of the Personal*

Data Sets by the Government; (ii) Cobalt is required to share the Personal Data Sets with the Government and the provisions of the Act will not be applicable to such sharing by Cobalt."

6. Following incidents happened immediately after the Notification was issued by the Ministry of Home Affairs:

(a) Due to the nationwide lockdown, employees of Cobalt were asked to work from home and all of them were able to access the Personal Data Sets from their take-home device. As the transition was done quickly to maintain continuity of service, proper security safeguards were not used at the time of transition. This resulted in a data breach from the device of 3 (three) employees of Cobalt working from their respective homes in the neighbouring country Xina. Such employees were accessing the Personal Data Sets from the cloud server located outside India. It was reported that Personal Data Sets of approximately 50,000 (fifty thousand) users were breached. The Personal Data Sets of such users resurfaced in social media in the form of trolls and memes, which resulted in such users facing social stigma and mob lynching.

(b) Government in an effort to create awareness and in a desperate attempt to curtail the situation, in association with a news channel called "**Freepublic**" released an online yellow book, containing the names, location and health data of people who tested COVID-19 positive and also a list of such people those who were likely to be infected with COVID-19. Resultantly, many individuals faced social stigma, some were outcast, and some were even asked to move out of their houses by their landlords/ housing societies. Rumours spread that to tap into data resources, the Government had sold its citizen's personal data to Freepublic.

7. Aggrieved by the aforesaid events, a body of individuals of the affected persons ("**BOI**") approached the Authority (as defined under the Act) claiming that: (a) Cobalt had stored the Sensitive Personal Data (*as defined under the Act*) outside the territorial boundaries of India in violation of the provisions of the Act and also failed to maintain security safeguards as mentioned under the Act, which resulted in the breach of Personal Data Sets of the users of the App; (b) Cobalt had shared the Personal Data Sets with the Government, for a purpose which breached the terms based on which consent was given by the users and also violated the terms of the Privacy Policy; and (c) the Government by sharing the Personal Data Sets with Freepublic, breached the terms on which consent was given by the users and

also violated the terms of the Privacy Policy. The Authority forwarded the complaint to an Adjudicating Officer (*as defined under the Act*) to adjudicate on the matter.

8. The Government in its reply claimed that: (a) it has immunity under the Act to do away the requirement of obtaining consent if they have to take any measures during an epidemic, outbreak of disease, at the time of threat to public health, disaster or any breakdown of public order; and (b) it has immunity under the Notification issued by the Ministry of Home Affairs. Further, Cobalt in its reply claimed that: (a) it has immunity under the aforesaid Notification issued by the Ministry of Home Affairs; (b) it has transferred the Personal Data Sets outside India for processing only and copies of such Personal Data Sets has been stored within India, thereby complying with the provisions of the Act; and (c) it has been unable to fulfill the terms of the Privacy Policy due to a force majeure event (Cobalt relied on the notification by Ministry of Finance dated 19 February 2020 for the definition and interpretation of a force majeure event). The Adjudicating Officer, upon hearing both sides, held that the neither the Government nor Cobalt have violated any provisions of the Act and neither of them should be liable to pay any penalty or compensation under the Act.

9. Aggrieved by the order of the Adjudicating Officer, BOI filed a Writ Petition before the Supreme Court of Zindia under Article 32 of the Constitution of Zindia claiming that their fundamental right to privacy has been violated. The Supreme Court of Zindia admitted the petition and framed the following issues:

(a) Whether the Notification lacks force of law and is unfair and unreasonable and fails to satisfy the test for imposing a valid restriction on the fundamental right to privacy.

(b) Whether Cobalt sharing the Personal Data Sets with the Government and the Government sharing the Personal Data Sets with Freepublic, was in breach of the terms based on which consent was given by the users and also in violation of the terms of the Privacy Policy; and

(c) Whether storage of the Sensitive Personal Data (*as defined under the Act*) outside the territorial boundaries of Zindia by Cobalt and its failure to maintain security safeguards as per the provisions of the Act, which resulted in the breach of Personal Data Sets, is in violation of the provisions of the Act.

(d) Whether there is lack of separation of power within the Authority formed under the Act, as the Adjudicating Officer is appointed by the same Authority which appoints the Inquiry Officer (as per the provisions of the Act).

(e) Whether the power to perform adjudicatory functions being vested in an Adjudicating Officer, who is not a member of any judicial body, has led to usurpation of judicial power and conferment of the same on such non-judicial body of the Adjudicating Officer.

Notes:

1. Since the Act has been recently enacted and there is a dearth of jurisprudence on the same, participants may rely on judgments from other jurisdictions having similar legislations eg European Union, Australia, etc.; provided that, the judgments are based on provisions of foreign legislations which are similar to the provisions of the Act.

2. Framers of the problem have drafted the problem in a manner that the Personal Data Protection Bill 2019 has been enacted, as is, in the form of an Act. Therefore, the fact that the Personal Data Protection Bill 2019 has not been enacted, cannot be used as an argument.

3. Please do not refer to any real-life applications or their terms and conditions for any arguments.

Disclaimer: All facts mentioned in the above proposition are purely fictious and any resemblance to any person, place, situation is purely coincidental.