CHAPTER VII – SMT. NIRMALA DEVI BAM INTERNATIONAL MOOT COURT COMPETITION 2025

MOOT PROPOSITION

In March 2023, M/s Zebra Technologies Private Limited, a preeminent technology enterprise, unveiled its pioneering smartwatch, "Zebra Pulse." Engineered with a sophisticated emergency detection system, the device was designed to perpetually monitor vital health parameters over time and, in instances of emergencies such as accidents or critical cardiac anomalies, automatically notify a pre-designated emergency contact via a connected mobile device while concurrently summoning immediate medical assistance. Further, the integrated cloud storage facility within the watch ensured that medical experts possessed unfettered access to comprehensive patient data in such emergency situations, thereby facilitating expedited and informed decision-making. As a result of these features, the innovative watch garnered widespread acclaim for its potential to save lives, and rapidly accumulated a substantial user base.

On June 5, 2024, Mr. X, having recently relocated to Dharmapura for professional obligations, designated his office colleague's mobile number as his emergency contact—a pragmatic decision necessitated by his transitional phase. He regarded the watch as particularly valuable, given his medical history, and belief that the device's emergency features would provide him with an added layer of security and reassurance in his new environment. However, unbeknownst to Mr. X, the "Zebra Pulse" smartwatch was designed to not only issue emergency alerts but also to perpetually record and store his sensitive health data. As initially stipulated in M/s Zebra's policy, announced in March 2023, users were assured that their personal health information would be safeguarded with utmost confidentiality and would not be divulged to unauthorized third parties.

However, on January 2024, the government notified the provisions of the Digital Personal Data Protection Act, 2023, along with its rules, thereby necessitating a subsequent policy update by M/s. Zebra Technologies Private Limited. Now, due to the stringent standards mandated by the aforesaid Act, the company was required to revise its terms, thereby authorizing the continuous transmission and storage of sensitive data to a designated State entity. Despite the policy revision in January 2024, Mr. X did not receive any direct notification or communication from M/s Zebra Technologies regarding the updated terms and conditions.

Over the ensuing months, Mr. X remained oblivious to this data sharing mechanism. Furthermore, on March 24, 2024, Mr. X's father temporarily came to stay with him and consequently, he transferred possession of the smartwatch over to him. Hence, from then on, the watch remained outside his possession.

On September 15, 2024, Mr. X embarked on an official business trip, necessitating his absence from his residence for a duration of 3 to 4 days. In preparation for his departure, Mr. X took meticulous precautions to ensure his ailing father's comfort and well-being, including informing his colleague of his father's condition as a precautionary measure. Notwithstanding these arrangements, an unforeseen accident occurred, resulting in Mr. X's father being rushed to a nearby hospital. This unforeseen event necessitated immediate medical attention and care, which was promptly provided by Mr. X's colleague. Mr. X was subsequently informed of the situation.

Upon arrival at the hospital, Mr. X's father was treated. However, during this treatment, there was development of complications, ultimately resulting in Mr. X's father experiencing paralysis below the waist. The attending physician relied on historical medical records transmitted by Zebra Pulse, which erroneously attributed hypertension and diabetes mellitus to Mr. X's father, leading to inappropriate treatment modifications. Hospital authorities bypassed Mr. X's colleague and directly accessed stored health data without verifying its accuracy or seeking consent.

The sudden onset of unforeseen circumstances compelled Mr. X to abruptly terminate his business trip and visit his father at the hospital. During a consultation with the attending physician, Mr. X was astonished to learn that his father's original treatment regimen had been modified to address the concurrent hypertension and diabetes mellitus. It was the resultant complications arising from this modified treatment that precipitated the paralysis. Mr. X, visibly distraught, expressed his profound dismay and disappointment to the physician, chiding the consultant for the perceived negligence that led to the complications. Mr. X revealed that he himself had been living with hypertension and diabetes mellitus and his father had no such diseases.

Upon conducting a more thorough inquiry, Mr. X ascertained that the medical professionals had accessed past medical records for treatment from the database of M/s Zebra Technologies Private Limited. It appeared that the smartwatch had indeed stored and transmitted all relevant health data to the hospital authorities. Furthermore, Mr. X discovered that despite being designated as an emergency contact, the hospital authorities had not deemed it necessary to solicit consent from his colleague, who had been providing care to his father during his absence. Furthermore, since the accident, Mr. X started receiving the call of some insurance company by the name of Mare Private Limited as well. Apparently, the patient's

data was also shared to this insurance company and hence, a smartwatch initially designed for safety purposes had inadvertently led to a substantial breach of privacy.

A subsequent investigation revealed that it was M/s Zebra Technologies Private Limited which had authorized unconsented commercial trading of the collected health data with Mare Pvt Ltd, a health insurance company in which Zebra held a significant stake. This clandestine transaction egregiously compromised the original assurance of data confidentiality, thereby facilitating further exploitation of the Mr. X's sensitive information for commercial purposes.

Following the series of events that compromised his privacy, Mr. X notified M/s Zebra Technologies Private Limited of his decision to terminate the contract and withdraw his consent for the collection, storage, and use of his personal data. Pursuant to the Digital Personal Data Protection Act and the agreement, Mr. X requested that the company delete all his sensitive data. Although M/s Zebra Technologies Private Limited partially complied with Mr. X's request by deleting some of his data, the company retained certain sensitive information. Despite Mr. X's explicit withdrawal of consent, Zebra retained biometric data including cardiac patterns and emergency alert timestamps. Furthermore, Mr. X discovered that his data was still being shared with other insurance companies, despite his explicit withdrawal of consent.

In October 2024, Mr. X, owing to his dissatisfaction, Mr. X approached Data Protection Board. In the case against M/s Zebra Technologies Private Limited, Mr. X challenged the smartwatch's privacy policies and alleged a breach of his right to privacy. M/s Zebra Technologies Private Limited responded, arguing that Mr. X had voluntarily designated his emergency contact and that the data-sharing process was in accordance with the user's consent and the revised terms and conditions of January 2024. The company maintained that Mr. X had provided consent during device setup, thereby precluding any claim of privacy breach. Mr. X countered that the smartwatch's system was designed for safety purposes, not surveillance, and that there was no need of storing medical data beyond minimum necessity. He argued that the company's actions were unlawful and constituted a breach of his privacy rights. He argued that the company's failure to obtain explicit consent for data sharing and its continued sharing of his data with third parties, despite his withdrawal of consent, were clear violations of his privacy rights.

On February 12, 2025, the board rendered a verdict in favor of M/s Zebra Technologies Private Limited, affirming that the sharing of health data with the designated emergency contact did not constitute a breach of privacy. The judgment, which ignored the legality of the terms of privacy, underscored the notion that

Mr. X had deliberately designated his emergency contact and had provided informed consent during the setup process.

Dissatisfied with the decision of the Data Protection Board and the egregious procedural irregularities that characterized the proceedings, Mr. X was compelled to seek redress through a writ petition before the Hon'ble High Court. In light of the egregious violations of his privacy rights, Mr. X now respectfully submitted that the Hon'ble Court declare that the continuous collection, indefinite retention, unauthorized dissemination, and commercial trading of his health data by M/s Zebra Technologies Private Limited constitute a blatant infringement upon his constitutional right to privacy under Article 21 and are patently inconsistent with the protective mandates of the Digital Personal Data Protection (DPDP) Act. Mr. X also prayed that the Court direct M/s Zebra Technologies to institute a stringent protocol mandating the periodic purging of all personal health data from its servers at intervals not exceeding three months, ensuring that such data is neither stored indefinitely nor exploited for commercial purposes. The petitioner further sought an order restraining M/s Zebra Technologies from transferring, selling, or otherwise trading his personal health information to any third party, including Mare Pvt Ltd, without obtaining explicit, informed, and revocable consent, in clear violation of the DPDP Act. Moreover, the petitioner requests the Hon'ble Court to issue appropriate interim orders suspending the ongoing practices of unauthorized data retention and commercial data trading pending a final resolution of the issues herein.

The matter is listed before the High Court of Dharmapura on May 11, 2025, with the following issues:

1. ***Whether M/s Zebra Technologies violated Mr. X's fundamental right to privacy under Article 21 by failing to obtain explicit and informed consent for continuous collection, retention, and dissemination of sensitive health data?***
2. ***Whether M/s Zebra Technologies' privacy policies and practices contravene the Digital Personal Data Protection (DPDP) Act or any other Statutory law by retaining sensitive health data despite withdrawal of consent and failing to adhere to legal requirements for data sharing?***
3. ***Whether M/s Zebra Technologies is liable for unauthorized commercial exploitation of personal health data through its partnership with Mare Pvt Ltd, thereby violating user trust and ethical standards.***
4. ***Whether the reliefs sought by Mr. X, including stricter data retention policies, deletion protocols,***

and regulatory oversight mechanisms, are enforceable under existing legal frameworks.

Note: All the laws, rules, regulations, by-laws, and other legal instruments of the Union of Indica are in pari-materia with those of the Union of India and the State of Dharmapura is equivalent to NCT of Delhi. The participating teams are permitted to draft sub-issues relevant to the issues outlined above.

Annexure 1 (Privacy Policy)

CONSENT TO DATA COLLECTION, STORAGE, AND USE

By activating and using the "Zebra Pulse" smartwatch (hereinafter referred to as the "Device"), the User, hereby consent to the collection, storage, and use of his sensitive health data, including detailed biometric readings and cardiac patterns, by M/s Zebra Technologies Private Limited (hereinafter referred to as the "Company") for the purpose of emergency response, device optimization, public health and research, and allied matters, on the given terms and conditions.

DATA COLLECTION AND STORAGE

The Company is committed to safeguarding user privacy and security, and to that end, shall collect and store sensitive health data pertaining to the user in a secure and encrypted format. This data shall include, but not be limited to, biometric readings such as heart rate and blood pressure, cardiac patterns including electrocardiogram (ECG) readings, and emergency alert data, including location and timestamp, in the event of an emergency.

The Company shall store this data on its central servers, which are protected by robust security measures. Specifically, the data shall be encrypted using the Blowfish algorithm, a widely recognized and respected encryption standard, ensuring the confidentiality and integrity of user data. Furthermore, the Company shall implement stringent access controls, including multi-factor authentication and role-based access, to prevent unauthorized access to user data.

DATA USE

The Company shall utilize user data exclusively for the following purposes:

Firstly, the Company shall employ user data to provide emergency assistance and alert designated emergency contacts in situations where the user's health and safety are at risk. This shall enable prompt medical attention and ensure the user's well-being.

Secondly, the Company shall leverage user data to enhance the performance and functionality of the Device. By analyzing user behavior and feedback, the Company shall identify areas for improvement and optimize the Device's capabilities to better serve user needs.

Thirdly, the Company shall utilize user data for research and development purposes, with the aim of enhancing the Device's capabilities and innovating new features.

DATA SHARING PROVISIONS

The Company shall not share user data with third parties without obtaining explicit consent from the user. However, in cases where disclosure is required by law or necessary to protect public health, the Company shall comply with applicable regulations and disclose user data as necessary.

DATA PROTECTION AND SAFEGUARD MEASURES

The Company is committed to safeguarding user data and shall take all reasonable measures to protect it from unauthorized access, disclosure, or loss. This shall include, but not be limited to, implementing robust security protocols, conducting regular security audits, and ensuring the confidentiality, integrity, and availability of user data.

COMPLIANCE WITH DATA PROTECTION LAWS

The Company shall comply with all applicable data protection laws and regulations. The Company shall also adhere to industry standards and best practices for data protection, ensuring the highest level of security and confidentiality for user data.

CONSENT WITHDRAWAL

The User reserve the right to withdraw his consent to the collection, storage, and use of his data at any time, without penalty or adverse consequence. This right shall be exercised by providing written notice to the Company, specifying the scope of withdrawal.

Upon receipt of written notice of consent withdrawal, the Company shall promptly delete User data from its servers, except where retention is required by law or to comply with regulatory obligations. The Company shall ensure that all data deletion processes are secure, verifiable, and compliant with applicable data protection laws.

DATA RETENTION

The Company shall retain the user data for a period of 6 months from the date of collection, or as required by law. After this period, the Company shall delete user's data, unless the latter has provided written consent for continued retention or unless retention is required for legal, regulatory, or public health purposes.

USER OBLIGATIONS

The User agrees to immediately notify the Company of any changes in his circumstances, including but not limited to changes in his medical condition, emergency contact information, or other similar situations.

The User acknowledges that failure to inform the Company of any aforementioned changes may result in unauthorized use or disclosure of his personal health data. In such cases, the Company shall not be liable for any consequences arising from such unauthorized use or disclosure.

Further, by using Company's services, the User expressly acknowledges that it is his responsibility to regularly review and stay informed about any updates or changes to Company's Privacy Policy. The Company reserve the right to modify or update its Privacy Policy at any time, and it is the User's duty to periodically visit Company's website and ensure he is aware of any such changes.

Annexure 2

UPDATED POLICY TERMS

1. Policy Revision: M/s. Zebra Technologies Private Limited has revised its policy to ensure conformity with the stipulations of the Digital Personal Data Protection Act, 2023, and its ancillary regulations, thereby ensuring adherence to the prevailing legal framework.
2. Data Dissemination: under the revised policy, the User sanctions the transmission and storage of sensitive data to a designated State entity, as mandated by the current legislation in force, and thereby agrees towards the continuous monitoring and analysis of his data. By continuing use, the User expressly consents to data sharing for public health and commercial purposes.
3. User Ratification: By continuing to utilize the Zebra Pulse smartwatch, the User ratifies his awareness and acceptance of the revised policy and its stipulations, thereby acknowledging his understanding of the updated terms and conditions.
4. Binding Nature: The revised policy shall possess binding effect upon the User and his successors, assigns, or transferees, thereby ensuring continuity and consistency in the application of the updated policy and its stipulations.
5. Jurisdictional Governance: These Terms shall be governed by and construed in accordance with the laws of India, thereby ensuring adherence to the prevailing legal framework and jurisdictional requirements.
6. Reference to Earlier Contract: This updated policy is an integral part of the original contract entered between the User and M/s. Zebra Technologies Private Limited. In the event of any inconsistency or conflict between the original contract and this updated policy, the terms of this updated policy shall prevail.