

Moot Proposition

Mr. Aman & Ors. vs Union of Indiana & Anr.

Indiana is a federal democratic country with over 5000 years of history. After attaining independence in 1947 from Country X, Indiana was introduced to the LPG Policy in 1990 for various internal and external political reasons. Medicine.Co. is a well-established Government Company that deals with online buying and selling of pharmaceuticals at a subsidised rate. It also serves as the biggest online pharmaceutical service platform in Compton, the capital city of Indiana. Those who attain membership to this company through subscription are also entitled to health insurance policies at subsidised premiums offered by *Samaveta Indiana Insurance Company*. There are two ways to gain a subscription, *i.e.*, membership in Medicine.Co. The first method was that those interested can apply for membership on the official website of Medicine.Co., which requires sharing Bank Account Details. Another option the company introduced was to purchase the same *via* an online payment platform called *MajorPay*, which did not require feeding any Bank Account Details directly into the official website of Medicine.Co. There are many employees in Medicine.Co., and since it is an online platform, it is controlled by the Central Government's Ministry of Corporate Affairs and the Ministry of Information and Technology, and all its employees are Public Employees. Medicine.Co. recently came into the spotlight after it entered a Rs. 200 Crore deal with one of the most recognised AI Companies of Indiana, SafetyGPT, on 22nd March 2023, to ensure all the customer data that the company collects can be streamlined by the AI Software.

The services rendered by SafetyGPT include:

- Organizing and structuring data: SafetyGPT automatically categorizes and organises customer data (name, age, purchase history, etc.) to improve efficiency and search capabilities within Medicine.Co.'s systems.
- Automating fraud detection: SafetyGPT analyses customer transactions and flags potentially fraudulent activity based on pre-determined criteria.

- Facilitating recurring payments: For customers with subscriptions or repeat purchases, SafetyGPT securely stores payment details to enable one-click renewals, eliminating the need for repeated data entry.
- Providing personalised recommendations: SafetyGPT analyses customer purchase history and browsing data to suggest relevant products and improve the user experience on the platform.

Medicine.Co. announced that SafetyGPT is an excellent solution addressing the risk of data breaches and streamlining issues many companies face. Thus, it will handle all such sensitive data as a third-party security software between the company and its customers.

Due to many issues of data breach and privacy in Indiana, the incumbent government, the Sanatana Democratic Alliance, introduced Act 22 of 2023. This Act laid down the provisions for processing digital personal data in a manner that recognises individuals' right to protect their data and the need to process such data for lawful purposes. **This Act came into force on the 21st of January, 2023.** The government of Indiana subsequently released a notification stating since the Act 22 of 2023 was a newly enacted provision, it shall be exempting certain Companies and Agencies in accordance with Section 17(5) of the Act¹ till 2027.

On January 21st 2024, Mr. Aman and approximately 2558 other members of Medicine.Co. from all over the country woke up to find their bank accounts emptied of all their life savings. In the beginning, all these people were confused about what had happened. Since many of these people did not have any other source of income apart from their salary and savings, many went bankrupt, causing mass unrest in the public.

Once Medicine.Co. was made aware of this security lapse, it immediately conducted a meeting with the Board of Directors of Medicine.Co. and decided to direct SafetyGPT to erase all the data of the customers that it had collected, as there could be a risk of Data-Theft. However, before

¹ The list of the same companies is further mentioned in the Appendix attached to the Proposition.

SafetyGPT managed to erase all the data and ensure that the communicated order could be complied with fully, approximately 4500 bank accounts were already hacked and emptied.

Medicine.Co. commenced an internal investigation about the data breach and attempted to solve this issue before it disclosed the same to all the Data Principals and issue a public statement. Preliminary investigation revealed that the AI system was capable of not only taking the data which it had been granted the permission to receive, but also any data which was entered by the customers was listed and automatically stored by the AI software.

Mr. Samarth, a close friend of Mr. Aman, who worked in Medicine.Co. as the head of R&D, on the 14th of February casually told Mr. Aman while having tea that the company's AI Software, which was used to streamline the customer data of Medicine.Co. was breached on New Years' Eve, causing a lot of data to be stolen from the database. Until then, no Medicine.Co. user had any idea about such a breach. A few days later, Mr. Aman met with a few of his colleagues in his office, who had also lost their bank balance and were randomly discussing their mishap when they suddenly began talking about how Medicine.Co. has been such a successful company and how they wanted their company to succeed like it. They all said they have a Medicine.Co. membership because of its facilities and discounts. Mr. Aman told them that Medicine.Co. is not as secure and robust as they thought it was and told his colleagues about what his friend there had told him about the New Years' Eve data breach. Later that night, Mr. Aman met his neighbor Deepak on his way home, and stopped by to talk with him. Deepak too was one of those people who had lost their money in the same manner as Mr. Aman. Mr. Aman told him that everyone in his company who has a membership of Medicine.Co. have lost their money and to his surprise, even Deepak said he had a membership of Medicine.Co.

Mr. Aman then started a private page on the Social Media platform *Tracebook* calling for all the people who had lost their money to join the group to discuss further plans of action. By the 19th of February, more than 3000 people had followed the page. When he further inquired about his suspicions, Mr. Aman realised that all the people who had lost their money had a membership of Medicine.Co. When Mr. Aman found out about this, he was confused and surprised. He did not understand how the connection could be made between the membership and the loss of money.

When he confided this in Mr. Samarth, he told Mr. Aman that this might be because Medicine.Co. has been automatically saving the Bank Account details of all the members in the AI Database as soon as anyone pays for the membership. Mr. Aman told Mr. Samarth that as far as he remembered, the disclaimer and permissions page of Medicine.Co². had never informed the customers that it would be storing their details. Mr. Samarth told him that he had attempted to raise this issue to the Board of Directors that the AI had automatically stored data from the Payment Portal of Medicine.Co. The next day, Mr. Aman, along with a few of his friends and some of the members from his *Tracebook* group stormed the office of Medicine.Co., demanding answers as to why they took the details of the bank accounts of customers without their consent and blamed them for losing their money. This caused a massive fight in the office, and after security was called, Mr. Aman and his group were thrown out of the company office space.

Post the fiasco, the Board of Directors of Medicine.Co., decided to look into the matter of how the details of the data breach reached the public as the management of Medicine.Co. had resolved to keep this matter out of public view in fear of the backlash they would face regarding the breach. It was found that Mr. Samarth, the head of the R&D department of Medicine.Co., was Mr. Aman's close friend, and he had revealed these facts to him.

By this time, many news reporters and the general public were aware of the fiasco. To reduce the damage, Mr. Adithya, the head of Public Relations and Marketing of Medicine.Co. released an official public statement saying that:

“At Medicine.Co., all data collected during the membership process is in full compliance with the provisions of the New Act 22 of 2023. The Act does not mandate explicit consent from individuals whose data is being collected as long as it is used for legitimate purposes. Our AI system securely tracks and stores users' bank account details to facilitate recurring payments, ensuring subscribers can easily renew their membership with a single click.

The Membership-driven subscription model was introduced to offer benefits and subsidies to our members and is fully protected under the Legitimate Use Principle outlined in the Act.

² The permissions page of Medicine.Co. is attached as Appendix II

Medicine.Co. operates as a Government Company under the control of the Central Government and is protected against any legal action for actions taken in good faith. The use of bank account details is for a legitimate purpose, and the recent breach of data was an unfortunate but minor setback.”

The members of the *Tracebook* group were not satisfied with these explanations presented by Mr. Adithya, and they approached the Supreme Court regarding the validity and Constitutionality of certain provisions of the Act. The Supreme Court stated that since this matter concerns the actions of Medicine.Co. and the validity of provisions of the impugned Act, it is necessary to make both Medicine.Co. and the Union of Indiana parties to the suit.

The matter is posted for hearing on the issues mentioned below.

ISSUES:

1. Whether the provisions of Act 22 of 2023 that allow the processing of Personal data without the consent of the Data Principal under Section 6 and allied provisions violate the Right to Privacy?
2. Whether the processing of Bank Account Details constitute a Legitimate Purpose under Section 7 and allied provisions, as stated in Act 22 of 2023?
3. Does the provision that provides immunity to the Central Government under Section 35 on account of Good Faith violate the Petitioner's right to seek remedy?
4. Whether the exemption of certain data fiduciaries under Section 17(5) by means of notification is an arbitrary exercise of discretion and thus violative of Article 14 of the Constitution of India?

NOTE:

1. The Laws of India are *pari materia* to that of India.
2. Jurisdiction needn't be addressed. The assumption is that the Court has admitted the matter for a final hearing.
3. Only issues that are mentioned shall be addressed.

APPENDIX I

**LIST OF AGENCIES AND COMPANIES DECLARED BY THE GOVERNMENT BY
NOTIFICATION UNDER SECTION 17 (5)**

Sl. No	List of Agencies and Companies
1.	Indiana Railways Catering and Tourism Corporation
2.	Jeevan Insurance Corporation
3.	Indiana Gas Limited
4.	Indiana Thermal Power Corporation
5.	Samaveta Indiana Insurance Co.
6.	Medicine.Co.
7.	Reserve Bank of Indiana
8.	Indiana Electronics Limited
9.	Indiana Testing Agency
10.	Indiana Aeronautics Limited

APPENDIX II

DATA PERMISSIONS PAGE OF MEDICINE.CO.

The personal information that we collect depends on the context of your interactions with us and the Sites, the choices you make and the products and features you use. The personal information we collect includes but is not limited to the following:

Name and Contact Data. We collect your first and last name, email address, postal address, phone number, and other similar contact data.

Credentials. We collect passwords, password hints, and similar security information used for authentication and account access.

Payment Data. We collect data necessary to process your payment if you make purchases, such as your payment instrument number (such as a credit card number), and the security code associated with your payment instrument, etc.

All personal information that you provide to us must be true, complete and accurate, and you must notify us of any changes to such personal information.

We use the information we collect or receive:

1. To facilitate account creation and logon process. If you choose to link your account with us to a third party account, we use the information you allowed us to collect from those third parties to facilitate account creation and logon process.
2. To send you marketing and promotional communications. We may use the personal information you send to us for our marketing purposes, if this is in accordance with your marketing preferences.
3. To send administrative information to you [for Business Purposes, Legal Reasons and/or possibly Contractual]. We may use your personal information to send you product, service

and new feature information and/or information about changes to our terms, conditions, and policies.

4. Fulfil and manage your orders. We may use your information to fulfil and manage your orders, payments, returns, and exchanges made through the Sites.
5. Deliver targeted advertising to you. We may use your information to develop and display content and advertising (and work with third parties who do so) tailored to your interests and/or location and to measure its effectiveness. For more information, see our Cookie Policy
6. To enable user-to-user communications [with your consent]. We may use your information in order to enable user-to-user communications with each user's consent.
7. To enforce our terms, conditions and policies [for Business Purposes, Legal Reasons and/or possibly Contractual].
8. For other Business Purposes. We may use your information for any other Business Purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Sites, products, services, marketing and your experience.



I Accept the Terms Conditions