PLUTUS IAS

CURRENT AFFAIRS

Argasia Education PVT. Ltd. (GST NO.-09AAPCAI478E1ZH)
Address: Basement C59 Noida, opposite to Priyagold Building gate, Sector 02, Pocket I, Noida, Uttar Pradesh, 201301, CONTACT NO:-8448440231

Date –9 Feb 2024

PERSONALLY IDENTIFIABLE INFORMATION

THIS ARTICLE COVERS 'DAILY CURRENT AFFAIRS' AND THE TOPIC DETAILS OF "PERSONALLY IDENTIFIABLE INFORMATION".THIS TOPIC IS RELEVANT IN THE "SCIENCE & TECHNOLOGY" SECTION OF THE UPSC CSE EXAM.

WHY IN THE NEWS?

The Ministry of Corporate Affairs has repaired a serious flaw in its online portal after a cybersecurity researcher reported it to India's Computer Emergency Response Team (CERT-In). The vulnerability allegedly exposed **Personally Identifiable Information (PII)** such as Aadhaar, Permanent Account Number (PAN), voter identification, date of birth, contact number, and communication address for over 98 lakh Indian company directors.

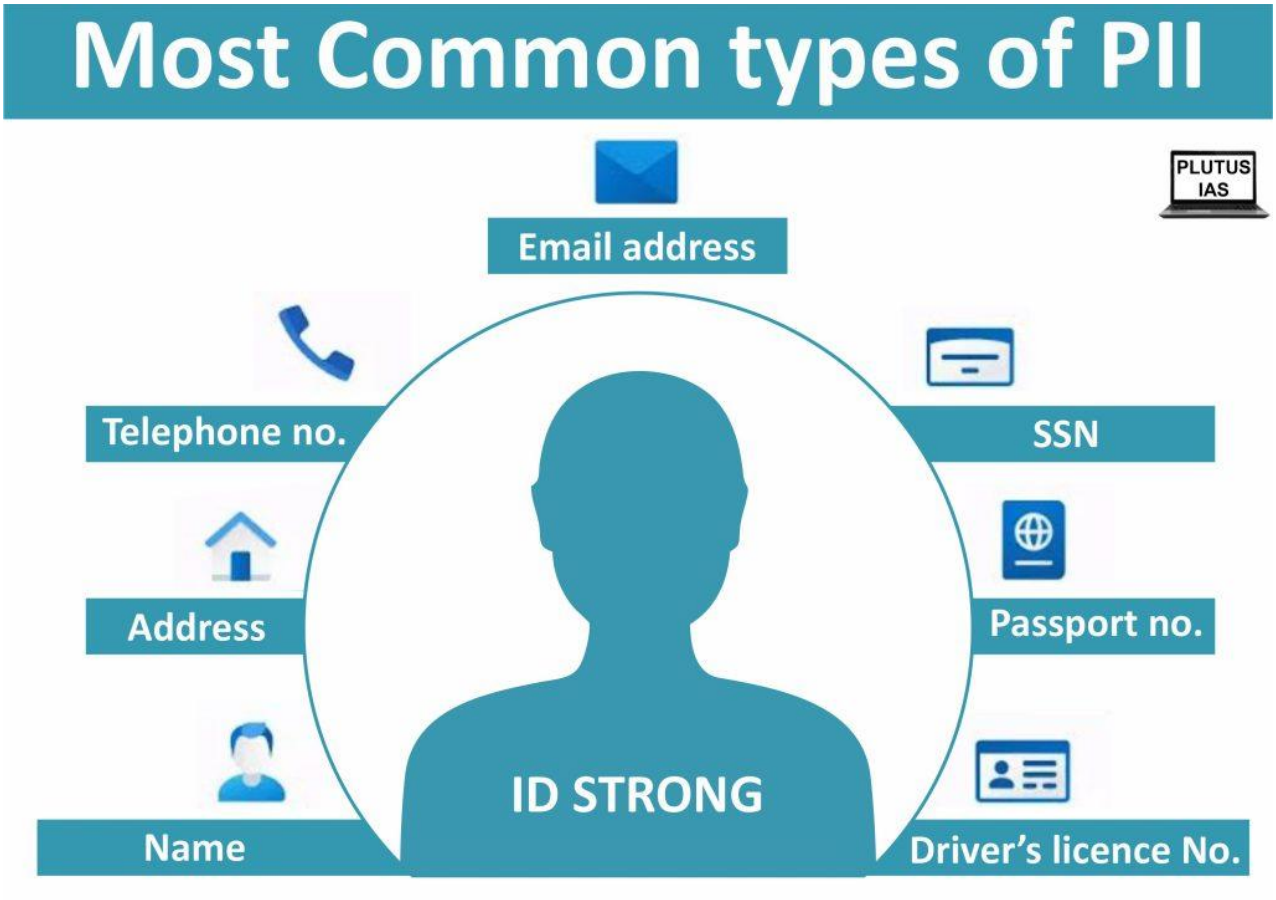
ABOUT PERSONALLY IDENTIFIABLE INFORMATION (PII)

- **Personally Identifiable Information** (PII) refers to any data or details maintained by an organization or agency that has the potential to identify a specific individual. This may encompass various details such as Aadhaar, PAN, voter identity, passport, date of birth, contact number, communication address, and biometric information. The constituents of PII vary based on an individual's home country.

- **Types of PII:** PII is categorized into **two types**: **direct identifiers and indirect identifiers**. Direct identifiers, like passport numbers or driver's license numbers, are unique to a person and can individually establish someone's identity. Indirect identifiers, such as race and place of birth, are not unique, but a combination of them can be used to identify an individual.

- **Sensitive vs. Non-sensitive PII**: Within PII, certain pieces of information are more sensitive than others. Sensitive PII directly identifies an individual and could lead to significant harm if leaked or stolen. Non-sensitive PII, on the other hand, would not cause substantial harm on its own if exposed. Examples of non-sensitive PII include a social media handle, zip code, race, gender, and religion.

- **Non-PII**: Non-personally identifiable information (non-PII) is data that, on its own, cannot be used to trace or identify a person. However, when combined with additional information, non-PII can contribute to identifying an individual. Examples of non-PII include photographic images, place of birth, religion, geographic indicators, employment information, educational qualifications, and medical records.



CONCERNS OF PERSONALLY IDENTIFIABLE INFORMATION (PII) EXPOSURE.

IDENTITY THEFT:

PII exposure increases the risk of identity theft, where criminals use stolen personal information for fraudulent activities. Cyberattacks and vulnerabilities in digital infrastructure can result in the exposure of citizens' PII.

FINANCIAL FRAUD:

Exposed PII, such as bank account numbers or credit card information, can lead to financial fraud. Criminals may access bank accounts, make unauthorized transactions, and siphon funds from government welfare programs.

DATA BREACH FALLOUT:

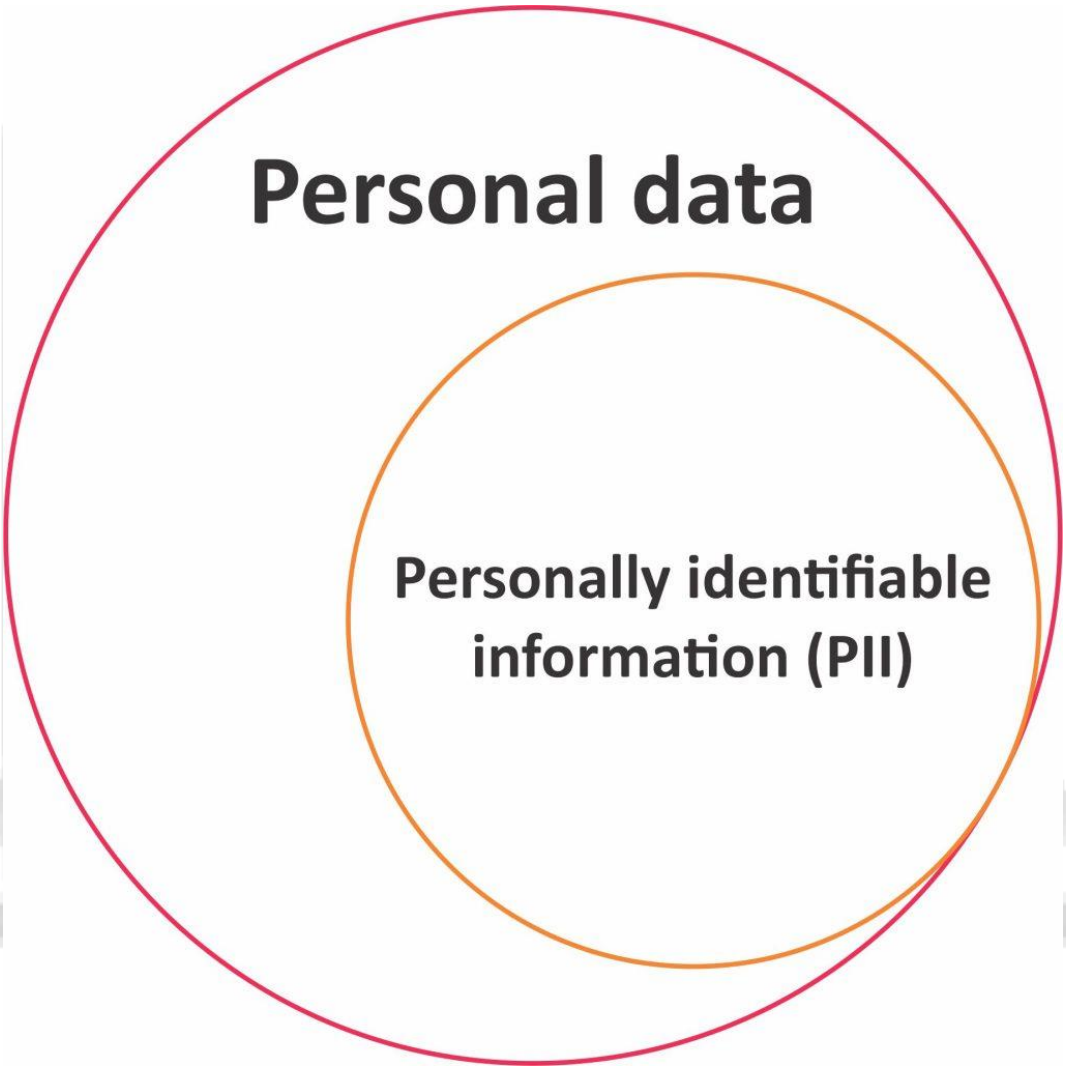
PII exposure through data breaches can lead to significant financial losses, remediation costs, and damage to an organization's reputation. Organizations may experience decreased customer trust, revenue loss, and increased scrutiny from regulators.

REPUTATION DAMAGE:
Exposure of sensitive PII, such as compromising photos or personal messages, can damage individuals' reputations and relationships. Information leaked online may be used for blackmail, extortion, or public humiliation, resulting in social and professional consequences.

PRIVACY VIOLATIONS:

PII exposure can compromise individuals' confidentiality and autonomy, leading to privacy violations.

PHISHING AND SOCIAL ENGINEERING ATTACKS:
Cybercriminals may use exposed PII for phishing attacks, tricking individuals into disclosing more sensitive information or clicking on malicious links. Social engineering attacks exploit exposed PII for impersonation scams or pretexting.



CHALLENGES IN SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII)

- **Varied Origins**: PII might be housed and managed across numerous sites, a consequence of the expanding use of cloud computing and Software as a Service (SaaS) solutions.

- **Escalating Data Quantities**: The anticipated doubling of sensitive data stored in public clouds by 2024 presents difficulties in ensuring its security.

- **Dynamic Threat Landscape**: A range of tactics, such as social engineering attacks and the acquisition of data from the dark web, is employed by cybercriminals to pilfer PII.

- **Intricate Regulatory Framework**: Organizations encounter the complexity of diverse data privacy regulations, necessitating customization of protective measures in accordance with specific regulatory requirements.

PRELIMS PRACTICE QUESTIONS

Q1) In India, it is legally mandatory for which of the following to report on cyber security incidents? (UPSC Prelims-2017)
1) Service providers
2) Data centres
3) Body corporate
Select the correct answer using the code given below:
a) 1 only
b) 1 and 2 only
c) 3 only
d) 1, 2 and 3

ANSWER: D

MAINS PRACTICE QUESTION

Q1. What are the different elements of cyber security? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. (UPSC Mains 2022)

Q2. Discuss different types of cybercrimes and measures required to be taken to fight the menace. (UPSC Mains 2020)

Himanshu Mishra