Massive Aadhaar Data Breach

For Prelims: Massive Aadhaar Data Breach, Aadhaar**,** UIDAI, Personally Identifiable Information (PII), **Cyber Attack**, Dark Web, Deep Web, **IT Rules (2021).**

For Mains: Massive Aadhaar Data Breach, Government policies and interventions for development in various sectors and issues arising out of their design and implementation.

Source: TH

Why in News?

Recently, Resecurity, an American cyber security company, said that **Personally Identifiable Information (PII)** of 815 million Indian citizens, including **Aadhaar** numbers and passport details, were **being sold on the Dark Web.**

- The threat actors selling the data claimed it was sourced from the **Indian Council of Medical Research (ICMR)**, which has been subjected to **numerous Cyber-Attack attempts with 6,000 incidents** being reported in 2022.

What is the Dark Web?

- The dark web refers to sites **that are not indexed and only accessible via specialized web browsers.** Significantly smaller than the tiny surface web, the dark web is considered a **part of the deep web.**
    - Using our ocean and iceberg visual, the dark web would be the **bottom tip of the submerged iceberg.**
- The dark web is intentionally hidden and can only be **accessed with special software, configurations**, or authorization, making it a realm of the internet that is not easily accessible to the average user.

//

What is Personally Identifiable Information and How Did Threat Actors Gain Access to Sensitive Data ?

- **About PII:**
  - PII is information that **when used alone or with other relevant data,** can identify an individual.
  - PII may be direct identifiers like **passport information or quasi-identifiers** that can be combined with other information to successfully recognise an individual.
- **Access to Sensitive Data:**
  - Threat actors selling stolen data on the dark web **declined to specify how they obtained the data** without which any effort to identify the source of the data leak would be speculative.
  - Lucius, the second threat actor found selling data online claimed to have access to a 1.8 terabyte data leak impacting an unnamed “India internal law enforcement agency”. However, the claim is yet to be authenticated.
  - Data samples observed by researchers contain multiple references to **UIDAI (Unique Identification Authority of India)** and Aadhaar cards, as well as voter ID cards. It is also possible that **threat actors successfully breached a third-party aggregating** these details.
- **Threats Arising from Leaked Information:**
  - India being one of the fastest growing economies of the world, ranked 4th globally in **all malware detection in the first half of 2023,** according to a survey from Resecurity.
  - The unrest in West Asia and increase in attacks by threat actors capitalizing on the chaos exposed personally identifiable data significantly, increasing the **risk of digital identity theft.**
  - Threat actors leverage **stolen identity information to commit online-banking theft,** tax frauds, and other cyber-enabled financial crimes.

What are the Previous Instances of Data Breach?

- Aadhaar data leaks were also reported in 2018, 2019, and 2022, with three instances of **large-scale leaks being reported,** including one in which farmer’s data stored on the **PM Kisan website was made available on the dark web.**
- Earlier in 2023, reports emerged that a bot on the messaging platform Telegram was returning

personal data of Indian citizens who registered **with the** Covid-19 vaccine intelligence network (CoWIN) portal.

What are the Provisions Related to Data Governance in India?

- **IT amendment Act,2008:**
  - Existing Privacy Provisions India has some privacy provisions in place under the IT (Amendment) Act, 2008.
  - However, these provisions are largely specific to certain situations, such as restrictions on publishing the names of juveniles and rape victims in the media.
- Justice K. S. Puttaswamy (Retd) vs Union of India 2017:
  - In August 2017, a nine-judge bench of the Supreme Court in **Justice K. S. Puttaswamy (Retd) Vs Union of India** unanimously held that Indians have a constitutionally protected fundamental right to privacy that is an intrinsic part of life and liberty under **Article 21.**
- **B.N. Srikrishna Committee 2017:**
  - Government appointed a committee of experts for Data protection under the chairmanship of Justice B N Srikrishna in August 2017, that submitted its report in July 2018 along with a draft Data Protection Bill.
  - The Report has a wide range of recommendations to strengthen privacy law in India including restrictions on processing and collection of data, Data Protection Authority, right to be forgotten, data localisation **etc.**
- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021:**
  - **IT Rules (2021)** mandate social media platforms to exercise greater diligence with respect to the content on their platforms.
- **Proposal of** 'Digital India Act',2023 **to replace IT act,2000:**
  - IT Act was originally designed only to protect e-commerce transactions and define cybercrime offenses, it did not deal with the nuances of the current **cybersecurity** landscape adequately nor did it address data privacy rights.
  - The new Digital India Act envisages to act as catalysts for the Indian economy by enabling more innovation, more startups, and at the same time protecting the citizens of India in terms of safety, trust, and accountability.

Way Forward

- The UIDAI has recommended using a "masked Aadhaar" that displays only the last four digits of the Aadhaar number, enhancing privacy and security.
- Moreover, to ensure accountability, the Aadhaar Act should be amended to reintroduce independent oversight through a high-powered "Identity Review Committee."
- The government should limit mandatory Aadhaar usage to permissible purposes and provide alternative authentication methods when Aadhaar authentication fails.
- Users can further protect their Aadhaar data by locking it through the UIDAI website or mobile app, rendering biometric information useless even if compromised.

Legal Insight: Expanding Aadhar to Private Entities

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Q. Consider the following statements: (2018)

1. Aadhaar card can be used as a proof of citizenship or domicile.
2. Once issued, Aadhaar number cannot be deactivated or omitted by the Issuing Authority.

Which of the statements given above is/are correct?

(a) 1 only
(b) 2 only
(c) Both 1 and 2
(d) Neither 1 nor 2

Ans: (d)

Exp:

- The Aadhaar platform helps service providers authenticate identity of residents electronically, in a safe and quick manner, making service delivery more cost effective and efficient. According to the GoI and UIDAI, Aadhaar is not proof of citizenship.
- However, UIDAI has also published a set of contingencies when the Aadhaar issued by it is liable for rejection. An Aadhaar with mixed or anomalous biometric information or multiple names in a single name (like Urf or Alias) can be deactivated. Aadhaar can also get deactivated upon non-usage of the same for three consecutive years.

With reference to “Blockchain Technology”, consider the following statements: (2020)

1. It is a public ledger that everyone can inspect, but which no single user controls.
2. The structure and design of the blockchain is such that all the data in it are about cryptocurrency only.
3. Applications that depend on basic features of blockchain can be developed without anybody’s permission.

Which of the statements given above is/are correct?

(a) 1 only
(b) 1 and 2 only
(c) 2 only
(d) 1 and 3 only

Ans: (d)

Mains

Q 1. Two parallel-run schemes of the Government, viz the Adhaar Card and National Population Register (NPR), one as voluntary and the other as compulsory, have led to debates at national levels and also litigations. On merits, discuss whether or not both schemes need to run concurrently. Analyze the potential of the schemes to achieve developmental benefits and equitable growth. **(2014)**