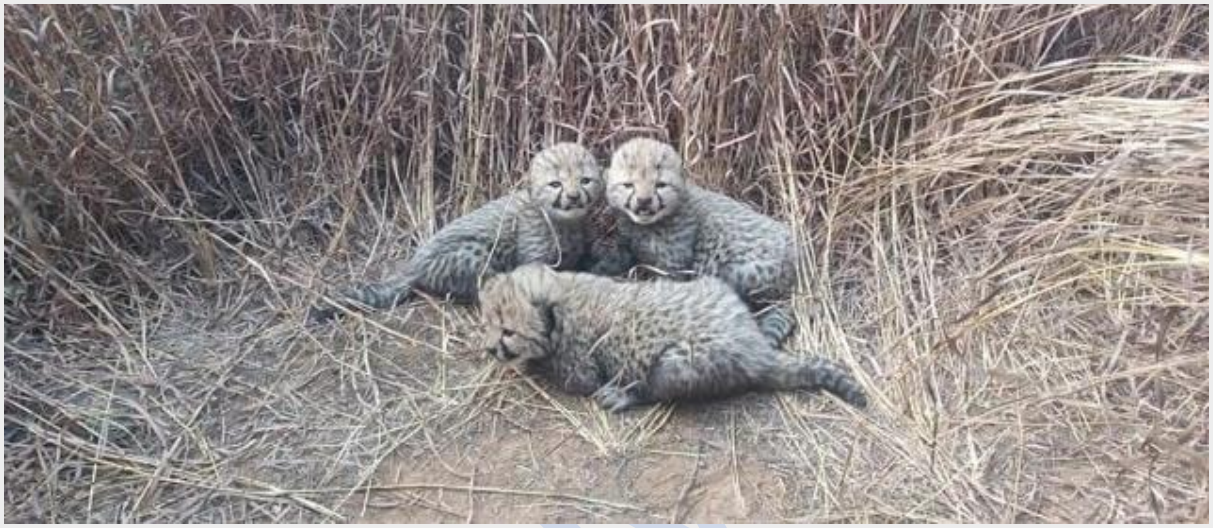
Daily News Juice 6th Feb,2024

To receive Daily news juice pdf on your WhatsApp, send name and city through WhatsApp on 75979-00000.

1. Seven cheetahs born in Kuno: Challenges, survival chances, and the wild-vs-protected debate



Three of the newborn Cheetah cubs

Birth of Cheetah Cubs in Kuno National Park
In January, seven cheetah cubs were born in Kuno National Park, Madhya Pradesh, marking a significant development for Project Cheetah, aimed at reintroducing cheetahs to India.

Life Stages of Cheetah Cubs
Cheetah cubs go through distinct stages in their lives, from birth to independence. Understanding these stages is crucial for their survival and successful reintroduction into the wild.

Wildlife Officials' Protocols for Pregnancy
Wildlife officials in Kuno National Park closely monitor cheetah pregnancies and ensure the well-being of expecting mothers through visual observations and supplementary feeding to maintain optimal health.

Standard Protocol for Cheetah Mother and Cubs
Experts emphasize the importance of allowing cheetah cubs to stay with their mothers to learn crucial survival skills, while also highlighting the necessity of vaccinations and proper nutrition for their development.

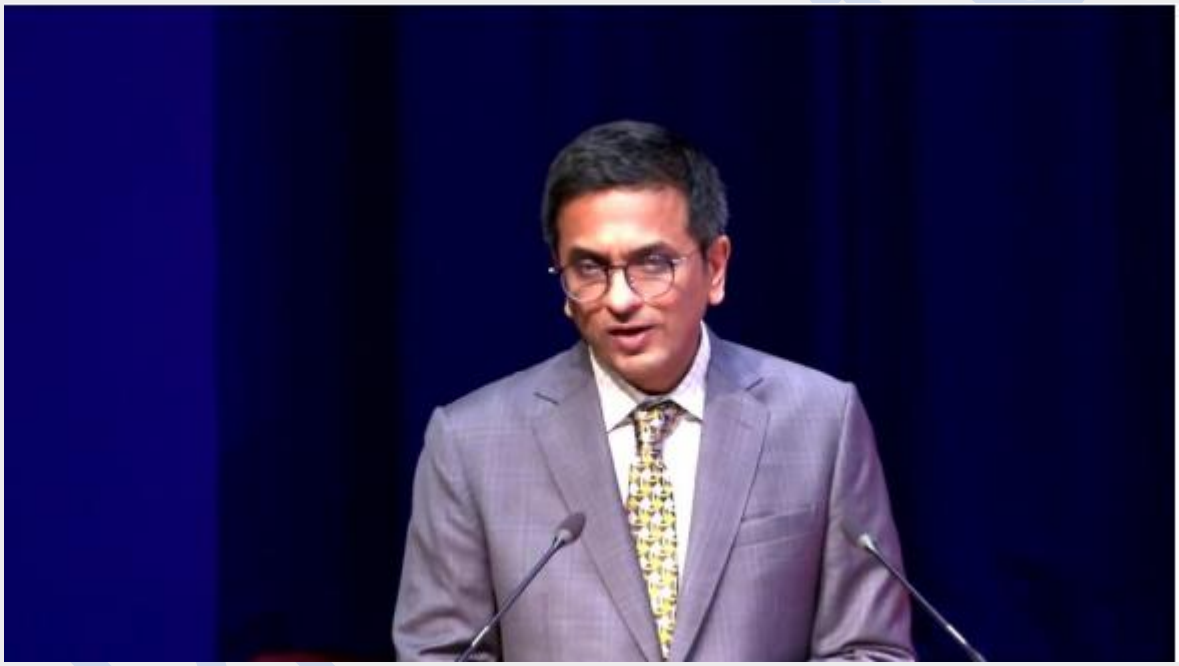
Intervention and Management
Officials intervene when necessary, particularly in cases of neglect or harm by the mother, to ensure the survival of the cubs and their successful integration into the cheetah population.

Survival Challenges and Reintroduction Debates
Cheetah cubs face significant survival challenges, and there is ongoing debate regarding the best approach to their reintroduction into the wild, weighing the benefits of protected enclosures versus free-ranging conditions.

Conclusion
The decision regarding the management and reintroduction of cheetah cubs in Kuno National Park involves careful consideration of various viewpoints and factors to ensure the long-term success of Project Cheetah and the conservation of cheetah populations in India.

Relevance: GS Prelims & Mains Paper III; Environment
Source: Indian Express

2. The four issues CJI DY Chandrachud highlighted within the legal profession



Why in news?
Delivering the Foundation Day address on the Supreme Court's 75th year of establishment on January 28, the CJI highlighted four issues within the judiciary that will have to be addressed through "difficult conversations".

These were "adjournment culture" among lawyers, limiting the length of oral arguments, the length of court vacations, and providing a level playing field for first-generation lawyers from diverse backgrounds.

1. What "adjournment culture" is; its effect on justice delivery
This address was far from the first time a Supreme Court judge has singled out the practice of lawyers asking for repeated adjournments as a cause for concern.

An adjournment refers to the court practice of delaying a scheduled hearing to a later date. Order XVII of the Civil Procedure Code, 1908 provides rules for courts to follow when faced with adjournment requests. Among other rules, it states that courts shall not grant an adjournment to a party more than three times during the hearing of a suit, that sufficient cause must be shown and that the circumstances are beyond the control of the party.

While adjournments are often necessary, the delay caused has a cascading effect of increasing the number of pending cases. The 239th Law Commission Report (2012) listed causes for delay in criminal cases at the trial court stage. It stated, "The heavy workload in the courts is taken advantage of by the advocates to press for adjournments." This presents a vicious cycle where adjournments lead to heavier workloads, which lead to even more adjournments. Similar is the case with the apex court.

2. Keeping the length of oral arguments in check

Often in constitutional bench matters (cases that require 5 or more SC judges to decide an important question of law), the court will direct the parties to confer and create a time schedule for oral arguments. This is to ensure efficiency and so that arguments are not repeated by lawyers on the same side.

Another option is adopting an approach similar to the Supreme Court of the United States, where lawyers are instructed to strictly limit their arguments to 30 minutes a side. This was considered in the 99th Law Commission Report (1984). However, a majority of the people whose opinions were sought were against imposing a strict limit. In 2009, the 230th Law Commission Report suggested limiting oral arguments to one-and-a-half hours, unless the case involved constitutional interpretation or a complex question of law.

3. Alternatives to long court vacations

Here, the CJI referred to the possibility of alternatives like flexi-time for lawyers and judges. This is a practice where employees are allowed to choose their daily working hours so long as they work for a set total number of hours in a given period.

In the past, the Parliamentary Standing Committee on Personnel, Public Grievances, Law and Justice, headed by BJP MP Brij Lal, suggested in its 133rd report that High Court judges take turns going on vacation to tackle the mounting pendency of cases. The report stated that court vacations are a "colonial legacy" that "causes deep inconvenience" to litigants.

The central government has also brought up the issue of court vacations earlier. In 2022, then-Law Minister Kiren Rijiju criticised the judiciary for taking long vacations even as pending cases hit record levels every year

The last time the Supreme Court took action on vacation length was in 2014. The court notified the new Supreme Court Rules which state that summer vacation shall not exceed seven weeks (reduced from 10 weeks). This was in line with suggestions in the Malimath Committee Report (2003), which recommended an increase in working days at the SC by three weeks.

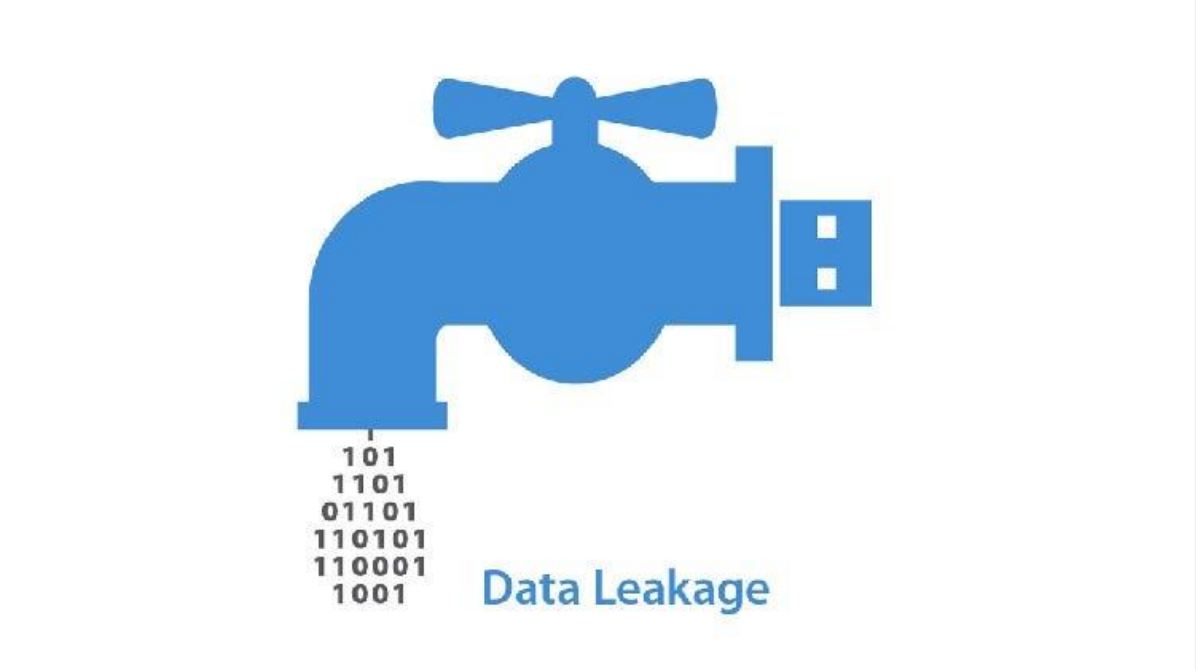
4. A level playing field for first-generation lawyers

CJI Chandrachud also stressed the need to provide a level-playing field for first-generation lawyers and those from marginalised segments who have the "will to work" and "potential to succeed".

The Supreme Court Annual Report (September 2023) took note of the Supreme Court Advocates-on-Record Association's (SCAORA) efforts to facilitate more diversity in the legal profession. This included providing better facilities for women lawyers, giving more "weightage" to first-generation lawyers when designating Senior Advocates, and allowing lawyers to appear via video conference on all working days so that first-generation lawyers and women lawyers with young children can appear with fewer obstacles.

Relevance: GS Prelims & Mains Paper II; Governance
Source: The Hindu

3. The importance of keeping personally identifiable information safe



Why in news?

Recently, the Ministry of Corporate Affairs fixed a critical vulnerability in its online portal months after a cybersecurity researcher reported it to the Computer Emergency Response Team of India (CERT-In). The vulnerability reportedly exposed personal details — like Aadhaar, PAN, voter identity, passport, date of birth, contact number and address — of more than 98 lakh directors of Indian companies. The vulnerability also exposed the personal data of top industrialists, celebrities, and sports personalities in the country.

What is Personally Identifiable Information?

Personally Identifiable Information (PII) is any data or information maintained by an organisation or agency that can potentially be used to identify a specific individual. This could

include information such as Aadhaar, PAN, voter identity, passport, date of birth, contact number, communication address, and biometric information. The constituents of PII vary depending on an individual's home country. However, non-PII in tandem with additional information can be used to identify an individual. Non-PII information includes photographic images (especially of the face or other identifying characteristics), place of birth, religion, geographic indicators, employment information, educational qualifications, and medical records.

All this information can be used to identify individuals accurately. And while access to one set of PII may be enough to compromise online security, access to multiple databases can be used to identify and target individuals.

What is the difference between sensitive and non-sensitive PII?
Non-sensitive PII is publicly available information and can be stored and transmitted unencrypted. This includes information such as zip code, race, gender, and religion. They cannot be used to accurately identify an individual.

Sensitive PII, when exposed, can be used to identify individuals and potentially cause harm. Some of the most important components that constitute sensitive PII are stored by employers, government organisations, banks, and other digital accounts used by individuals.

What are the risks of PII exposure?
Cyberattacks and weaknesses in digital infrastructure can lead to the exposure of citizens' PII. Threat actors can gain access to exposed PII and misuse it to launch targeted attacks on individuals. These attacks could range from phishing attacks with messages curated with PII information, to fraudulently opening bank accounts, and siphoning funds from accounts allotted to beneficiaries of government welfare programmes.

Threat actors may also use such information to obtain cellular connections, credit cards, and compromise the security of an individual's digital accounts. Threat actors are also known to sell exposed PII information on the dark web.

What are the recent events where PII was compromised?
In 2023, reports emerged that a bot on Telegram was returning the personal data of Indian citizens who registered with the COVID-19 vaccine intelligence network (CoWIN) portal for vaccination purposes. A similar data breach was reported when an American cybersecurity company said that the PII of 815 million Indian citizens, including Aadhaar numbers and passport details, were being sold on the dark web. At the time, a cybersecurity company, Resecurity, said it contacted multiple victims who verified the validity of their data. The government of India denied allegations of a biometric data leak, as well as a breach in the CoWIN portal. It did, however, launch an investigation into the allegations that led to the arrest of a man in Bihar, along with a juvenile in June 2023. A data breach was also reported in the RailYatri platform in January 2023.

Additionally, 67% of Indian government and essential services organisations experienced over a 50% increase in disruptive cyberattacks, a report from Resecurity said. Furthermore, a survey

of 200 IT decision-makers noted that 45% of Indian businesses experienced more than a 50% increase in cyberattacks.

How can one protect PII?

Individuals may not be able to prevent leaks in databases of government organisations or service providers. However, they can take steps to ensure that their PII is not readily available to threat actors.

Look for HTTPS in URLs when visiting unknown websites. The "S" stands for secure and is used by legitimate websites to secure collected information from unsecured connections. Some browsers may also use a lock symbol in the URL bar to signify that a website is secure.

Use a VPN when accessing sensitive information using public networks. A VPN helps protect PII and other vital data by securing your online connection from prying eyes on public networks.

Keep a tab on your PII like Aadhaar, passport, PAN, Voter ID, and other important proofs of identity. Avoid sharing or accessing images or details of identity documents through unknown devices.

In case you do access them at a photocopy shop or devices owned by others, make sure to delete the documents even from recycle bins to ensure they are not misused. Avoid sharing personal information on social media platforms.

In case your PII is leaked, be on the lookout for phishing attacks, that may use leaked information to convince you they are legitimate.

Keep a tab on your bank account transactions, credit cards, and credit score; a hit in the score could mean your PII has been misused to procure credit cards in your name.

Relevance: GS Prelims & Mains Paper III; Science & Technology
Source: The Hindu