ISSN (Print): 1060-6076
ISSN (Online): Applied

The Journal of African Development
2026; Vol 7: Issue 1
https://www.afea-jad.com/

Efficacy of DNA Databases in Criminal Justice: A Comparative Analysis of the USA and India.

Ms. Medha Singh [1], Dr. Kanchal Gupta [2]

[1]Ph.D. Scholar, School of Law, UPES Dehradun

[2]Sr. Associate Professor, School of Law, UPES Dehradun

Cite This Paper as: Ms. Medha Singh , Dr. Kanchal Gupta (2026) Efficacy of DNA Databases in Criminal Justice: A Comparative Analysis of the USA and India...*The Journal of African Development l, Vol.7, No.1*, 281-291

KEYWORDS
DNA, DNA database, privacy, framework.

ABSTRACT
DNA profiling has transformed criminal justice by enabling precise identification of individuals from biological evidence, leading many jurisdictions to establish forensic DNA databases. The United States emerged as an early adopter through the Combined DNA Index System (CODIS), whereas India is at a nascent stage of developing a comparable framework and continues to confront significant legal and ethical concerns. This paper undertakes a comparative analysis of the use of DNA databases in criminal justice in the U.S. and India. It examines the governing legal frameworks, including constitutional protections, procedural safeguards, and statutory regimes such as CODIS-related laws in the U.S. and the Criminal Procedure (Identification) Act, 2022 in India. The paper further explores ethical and social dimensions, including consent, privacy, surveillance risks, proportionality, and data retention. By evaluating challenges and institutional capacities, the study identifies best practices offers recommendations for strengthening India's emerging DNA database regime. in

1. INTRODUCTION

Legal Framework Governing DNA Databases

United States

In the United States, forensic DNA databases operate within a well-defined legal framework. The primary constitutional consideration is the Fourth Amendment, which guards against unreasonable searches. Collecting a DNA sample (usually via cheek swab) is a "search," but the U.S. Supreme Court has upheld certain DNA collection practices as reasonable in light of the government's interests in identifying suspects and solving crimes. In the landmark case Maryland v. King(2013), a 5-4 majority ruled that the warrantless collection of DNA from individuals arrested for serious offenses does not violate the Fourth Amendment . The Court reasoned that swabbing an arrestee's cheek is a minimal intrusion akin to fingerprinting, outweighed by the government's interest in accurately identifying arrestees and checking for links to unsolved crimes . Justice Scalia's dissent, by contrast, warned that this practice enables a general search for evidence of crime, contrary to Fourth Amendment principles . Despite such privacy concerns, King established that DNA collection at booking for serious charges is constitutional under a balancing test favouring law enforcement needs when the intrusion on personal privacy is relatively slight.

Beyond the Fourth Amendment, U.S. courts have held that DNA collection does not implicate the Fifth Amendment's self-incrimination clause, since providing a DNA sample is not testimonial. Thus, requiring an offender to submit a DNA sample is viewed similarly to fingerprinting or photographing an arrestee. With these constitutional backdrops, legislation provides the structure for DNA databases. At the federal level, the DNA Identification Act of 1994 authorized the FBI to create a national DNA index of convicted offenders and certain other categories, laying the foundation for CODIS. CODIS is a three-tiered system ,local, state, national, that allows DNA profiles to be shared and compared across jurisdictions. Initially, federal law and state laws focused on collecting DNA from convicted felons, especially violent and sexual offenders. Over time, statutes expanded the collection to include virtually all felons and, in many states, people arrested for serious crimes. By the mid-2000s, Congress and states had broadened the database's scope, for example, the 2005 DNA Fingerprint Act authorized collecting DNA from individuals arrested or detained under federal authority. As a result, the National DNA Index (NDIS) now contains over 18 million offender profiles and nearly 6 million arrestee profiles, and all 50 states participate in the system.

Accompanying this expansive scope are statutory safeguards and administrative rules. CODIS, by design, uses DNA markers located in non-coding regions of the genome that are presumed not to reveal personal health or trait information[1] The CODIS profiles are stored as numeric representations of these Short Tandem Repeat (STR) loci, and for privacy reasons, the database itself does not contain personal names or other identifying details of the offender; identifying information is held by the submitting laboratories. When a profile in the database matches a crime-scene sample, CODIS notifies the relevant lab or agency, which can then pursue the identification through legal channels. This separation adds a layer of privacy protection by ensuring that a DNA profile on its own cannot immediately be traced to a specific person without an official inquiry.

Laws and FBI policy also limit how DNA data can be used. CODIS is strictly for law enforcement identification purposes and certain humanitarian uses like identifying missing persons, searching the database for other reasons is prohibited[2]. There are penalties for misuse of DNA information. Furthermore, federal law provides mechanisms for expungement of DNA profiles in some circumstances. If an arrestee's charges are dropped or they are acquitted, or if a conviction is overturned, that person can seek to have their DNA profile removed from the database[3]. In practice, expungement requires the individual to initiate the process and provide documentation (e.g., a court order of acquittal), and studies have found that relatively few eligible profiles end up being removed. Nonetheless, the availability of expungement reflects an attempt to balance the database's reach with individual rights – acknowledging that people who are not convicted should not be permanently in the system.

At the state level, each state has its own statutes governing DNA collection and databasing, which complement the federal CODIS framework. While details vary, a common pattern is evident: all states mandate DNA collection from persons convicted of felonies and sometimes certain misdemeanors, and a majority of states collect from individuals arrested for particularly grave offenses, such as violent felonies. State laws also often address the logistics of DNA collection who may collect the sample, when it must be done, require laboratory accreditation and quality assurance, and impose confidentiality rules. Many states explicitly prohibit using DNA database information for non-law enforcement purposes and impose criminal penalties for improper disclosure or testing beyond identification. These provisions work in tandem with constitutional doctrines to govern DNA databases. In sum, the U.S. has developed a legal regime that aggressively uses DNA to advance criminal justice objectives, while embedding specific safeguards limited DNA markers, no personal identifiers in the database, expungement procedures to curb unwarranted intrusions on privacy.

India

India is in the early stages of constructing a legal framework for DNA databases in criminal justice. For decades, the law that permitted collecting identifying information was the Identification of Prisoners Act, 1920 – a colonial-era statute allowing fingerprints, footprint impressions, and photographs of certain convicted or arrested persons. Recognizing the need to update the law for modern forensic techniques, Parliament enacted the Criminal Procedure (Identification) Act, 2022. This new law dramatically expands both the types of data that can be collected and the categories of individuals from whom data can be collected[4]

Under the CPI Act 2022, "measurements" include not only traditional fingerprints and photographs but also biometric and biological data. It specifically authorizes taking finger and palm prints, footprint impressions, photographs, iris and retina scans, signature and handwriting samples, and biological samples such as blood, saliva, hair and their analysis which would encompass DNA profiling[5]. The universe of people subject to these measures is very broad: any person convicted of an offense and any person arrested for an offense may be required to give these measurements. This is a significant change from the 1920 law, which limited collection largely to those convicted of or arrested for offenses punishable by at least one year in prison[6]. Now, even someone arrested for a relatively minor offense in theory falls under the Act. However, the Act does include a partial check on DNA collection: it provides that biological samples and their analysis can be taken forcibly only from persons arrested for offenses that are punishable by at least seven years of imprisonment or for crimes against women or children[7]. In cases of lesser offenses, a person "not obliged to submit" a biological sample may refuse. In practice, this means that for minor cases the police can still collect photographs, fingerprints, etc., but perhaps

[1] Jilsblognujs VAPB, "DNA Databases and the Right to Privacy: Analysing the Criminal Procedure (Identification) Act 2022 and CODIS" (The Journal of Indian Law and Society, August 21, 2023) https://jilsblognujs.wordpress.com/2023/08/21/dna-databases-and-the-right-to-privacy-analysing-the-criminal-procedure-identification-act-2022-and-codis/

[2] Ibid 6.

[3] Ibid 6.

[4] "The Criminal Procedure (Identification) Bill, 2022" (PRS Legislative Research) https://prsindia.org/billtrack/the-criminal-procedure-identification-bill-2022#:~:text=Data%20permitted%20to%20be%20collected

[5] Ibid 9.

[6] Ibid 9.

[7] Ibid 9.

not DNA without consent. Additionally, the Act allows a magistrate to order any person including a person not under arrest, such as a witness or victim to provide measurements if it is considered necessary for an investigation[8]. Non-compliance with a lawful direction to give measurements is made an offense under the Act as obstruction of a public servant.[9]

The CPI Act 2022 also lays the groundwork for setting up databases of the collected information. It designates the National Crime Records Bureau (NCRB) as the central agency to store and manage the records of measurements, and allows state governments to designate laboratories or agencies to collect and transmit data to NCRB[10] One of the most salient and controversial features of the Act is its rule on data retention: measurements may be retained for 75 years from the date of collection[11]. Seventy-five years essentially amounts to lifetime retention in most cases. The Act provides that records should be destroyed earlier if the person has no previous convictions and has been released without trial or acquitted of the offense, and if all appeals by the prosecution have been exhausted[12]. Even then, there is a caveat – a court or magistrate may order that the records be preserved despite an acquittal (the Act does not specify on what grounds this can be done)[13] Moreover, the onus appears to be on the acquitted person to request destruction of their data. In short, unless an individual actively pursues deletion, or a case concludes in their favor with no possibility of appeal, their data will remain on file for decades. This retention framework is far more sweeping than what is seen in many other jurisdictions and has raised concerns about privacy and proportionality.[14]

India's constitutional framework provides important context for evaluating this scheme. The right to privacy was affirmed as a fundamental right by the Supreme Court in *K.S. Puttaswamy v. Union of India* (2017), which held that privacy is protected by Article 21 of the Constitution and other fundamental rights. The Court in *Puttaswamy* laid down a test for laws that infringe privacy: there must be a law authorizing the intrusion, it must serve a legitimate state aim, and it must be proportional, meaning the law should be necessary and there should be no less-intrusive but equally effective alternative, and the infringement should not be excessive relative to the benefit[15]. The CPI Act 2022 is certainly a law meeting the legality criterion and its aim, improving criminal identification and investigation – is legitimate. The key question is proportionality and necessity. Observers have pointed out that aspects of the Act might fail this test[16]. For instance, *blanket collection* of data from all arrestees, regardless of the severity of offense, and *extremely lengthy retention* of even innocents' data, might be considered too broad and thus not the least restrictive way to achieve the law's aims. A more narrowly tailored law, for example, limiting DNA profiling to serious offenses and deleting data of those not convicted, would arguably achieve most crime-solving benefits with less impact on privacy. These arguments are central to legal challenges that have been mounted against the Act. As of 2025, petitions in the High Courts of Delhi and Madras challenge the CPI Act as unconstitutional on grounds including the right to privacy, the right against self-incrimination, and equality[17]. The Supreme Court declined to immediately entertain one such petition, advising petitioners to go to the High Court first[18]. so the issue is actively under judicial scrutiny at the High Court level.

Another constitutional aspect is Article 20(3), which protects an accused from being compelled to be a witness against themselves. The Supreme Court has long interpreted this to apply only to testimonial evidence something that communicates knowledge, like an oral confession and not to physical evidence. In *State of Bombay v. Kathi Kalu Oghad* (1961), the Court held that giving fingerprints, handwriting samples, or other physical measurements does not violate

[8] Ibid 6.
[9] Ibid 9.
[10] Ibid 6.
[11] George J Annas, 'Privacy Rules for DNA Databanks: Protecting Coded "Future Diaries"' (1993) 270(19) Journal of the American Medical Association 2346.
[12] Interpol, Global DNA Profiling Survey Results (report, 2019) https://www.interpol.int/content/download/15469/file/INTERPOL%20Global%20DNA%20Profiling%20Survey%20Results%202019.pdf
[13] Ibid 17.
[14] Ibid 16.
[15] Ibid 16.
[16] Tanmay Singh and Gayatri Malhotra, 'The Digital Data Protection Bill 2022 Does Not Satisfy the Supreme Court's Puttaswamy Principles' (web article, n.d.) https://internetfreedom.in/the-digital-personal-data-protection-bill-2022-does-not-satisfy-the-supreme-courts-puttaswamy-principles/
[17] "Examining the Constitutionality of the Criminal Procedure (Identification) Act, 2022" (Constitutional Law Society, October 15, 2023) https://clsnluo.com/2022/08/01/examining-the-constitutionality-of-the-criminal-procedure-identification-act-2022/#:~:text=Examining%20the%20Constitutionality%20of%20the,mechanism%2C%20being%20%E2%80%9Carbitrary%E2%80%9D%20and
[18] India Legal, "Supreme Court Refuses to Entertain Plea Challenging Constitutionality of Criminal Procedure Act, 2022" (India Legal, February 12, 2024) <https://indialegallive.com/constitutional-law-news/supreme-court-news/criminal-procedure-act-plea/#:~:text=,Identification%29%20Act%2C>

Article 20(3)[19]. This principle extends to DNA; obtaining a blood or saliva sample for DNA analysis is not considered self-incrimination since the accused isn't being forced to testify or confess, but merely to submit physical evidence. *Selvi v. State of Karnataka* (2010) reaffirmed this distinction, striking down compulsory lie detector and narcoanalysis tests which were deemed to invade one's mental privacy and require consent, but not treating DNA or fingerprint collection as similarly problematic[20]. However, *Selvi* did note that any involuntary physical intrusion must have clear legal basis and reasonableness which the CPI Act now provides on paper for DNA and other measurements.

Indian jurisprudence on DNA evidence itself as opposed to databasing has evolved through criminal trials. Courts have generally welcomed reliable DNA evidence as an aid to discovering the truth, but also exercise caution. For example, the Delhi High Court in *Santosh Kumar Singh* (2010) (the Priyadarshini Mattoo case) emphasized that a DNA test report, when properly obtained, is scientifically accurate and can be relied upon as strong evidence of guilt[21]. Conversely, the Calcutta High Court in a 2021 case, cautioned that the absence of the accused's DNA in samples from the victim did not by itself prove innocence, since there could be reasons why DNA wasn't detected[22]. These examples show that while Indian courts value DNA evidence, they don't consider it infallible or exclusively determinative.

In anticipation of a growing role for DNA, India has also considered more specific legislation: the DNA Technology (Use and Application) Regulation Bill, reintroduced in 2019 building on earlier versions from 2018 and a 2007 draft. This Bill, which remains pending, aims to establish a dedicated DNA Regulatory Board, standards for DNA labs, and a framework for DNA Data Banks at national and regional levels[23]. It classifies indices for DNA profiles crime scene index, offenders index, suspects, missing persons, etc. and prescribes some safeguards – for example, written consent for taking DNA from persons like victims or suspects in certain circumstances, and an obligation to remove the DNA profile of a suspect on the conclusion of investigation or proceedings if the suspect is not found guilty. The Bill has undergone scrutiny by a parliamentary committee and has drawn criticism from privacy advocates, particularly regarding broad definitions and insufficient safeguards on storage and use of DNA file. Notably, the Bill specifies that DNA profiles can only be used for specified purposes mostly relating to criminal cases or identifying missing persons and that violation of privacy like using DNA data for other purposes would be punishable. The Bill's fate is uncertain, but its presence indicates legislative awareness of the need for a more nuanced approach to DNA usage than the CPI Act alone offers. It's possible that if the Bill passes with amendments, it could work in tandem with or override parts of the CPI Act by focusing specifically on DNA profiling.

Additionally, although India currently lacks a comprehensive data protection law, a draft law (the Digital Personal Data Protection Bill, 2023) is under consideration. Under the earlier Personal Data Protection Bill 2019, genetic data was categorized as "sensitive personal data", suggesting that stringent protections and rights like the right to consent and the right to erasure) should apply. Privacy experts argue that having a data protection regime in place is crucial when implementing DNA databases. Such a law could impose duties on authorities like NCRB to ensure DNA information is kept secure, used only for legitimate purposes, and deleted when no longer necessary, under independent oversight.

In summary, India's legal framework for DNA databases is in flux. The CPI Act 2022 dramatically widens the state's power to collect and retain personal biometric and genetic data, raising important constitutional questions about how to reconcile this with privacy and liberty. The ultimate shape of India's DNA database policies will likely be influenced by the outcomes of court challenges and possibly further legislative refinements such as the DNA Bill or data protection legislation. As it stands, India's approach is more sweeping in scope than the U.S. model, reflecting a crime-control orientation, but it is tempered by the potential for judicial intervention to impose privacy-protective conditions. The ongoing dialogue between the branches of government in India will determine how efficacy and rights are balanced in the use of DNA for criminal justice.

Case Studies and Judicial Pronouncements

A comparative look at case studies and court rulings illustrates how DNA databases and evidence have been applied in

[19] Srivastava A and others, "Impact of DNA Evidence in Criminal Justice System: Indian Legislative Perspectives" (2022) 12 Egyptian Journal of Forensic Sciences https://doi.org/10.1186/s41935-022-00309-y

[20] Ibid 24.

[21] Das A and Law L, "Supreme Court Refuses to Entertain Challenge to Law Allowing Collection of Prisoners' Biometrics; Asks..." Live Law (February 15, 2024) https://www.livelaw.in/top-stories/supreme-court-pil-criminal-procedure-identification-act-internet-freedom-foundation-high-court-249253#:~:text=Supreme%20Court%20Declines%20to%20Hear,Awstika%20Das

[22] "In Rape Cases, DNA Evidence Would Not Be Conclusive Proof: Calcutta High Court – Child Rights Clinic – Every Child Counts" https://jgu.edu.in/child-rights-clinic/in-rape-cases-dna-evidence-would-not-be-conclusive-proof-calcutta-high-court/#:~:text=In%20rape%20cases%2C%20DNA%20evidence,man%20in%20a%20rape%20case

[23] Desk TW, "DNA Data Bank Still a Work in Progress - The Tribune" The Tribune (May 1, 2022) https://www.tribuneindia.com/news/himachal/dna-data-bank-still-a-work-in-progress-390888/#:~:text=The%20DNA%20Technology%20,to%20a%20question%20in%20Parliament

practice, and how the judiciary in each country mediates their use.

United States

DNA database hits in the United States have helped solve countless crimes, including decades-old cold cases. CODIS has generated hundreds of thousands of investigative leads, often identifying serial offenders who might otherwise have escaped detection[24]. For example, the "Green River Killer", responsible for dozens of murders in the 1980s was finally caught after crime-scene DNA (preserved for years) matched a profile in the offender database. Similarly, numerous rapes and homicides that went cold have been solved when a DNA profile from evidence, entered into CODIS, matched an individual convicted of a different crime. The U.S. has also used DNA matches to exonerate wrongly convicted individuals through post-conviction DNA testing; many states now allow convicts to seek DNA testing of old evidence, and over 300 wrongful convictions have been overturned nationwide due to DNA, often with the real perpetrator identified via a database match[25]. These outcomes underscore that DNA databases promote accuracy in justice – helping convict the guilty and free the innocent.

Courts routinely accept DNA match reports as powerful evidence. When a CODIS hit identifies a suspect, investigators usually obtain a fresh DNA sample from that suspect to verify the match scientifically before trial. Once presented in court with a laboratory expert's testimony, such evidence often becomes central to the prosecution's case. U.S. judges have generally found DNA profiling to meet the standards of scientific evidence admissibility, given its well-established methodology and low error rates. While defense attorneys sometimes challenge the handling of samples or the statistical interpretation of partial DNA profiles, there is little dispute over the fundamental reliability of STR DNA matching. Notably, as DNA use has expanded, courts have also had to consider new investigative methods – for instance, familial DNA searching, looking in the database for profiles similar enough to suggest a relative of the perpetrator and the use of genetic genealogy databases which was famously how the "Golden State Killer" was identified in 2018, by searching a public genealogy DNA database. These techniques raise additional privacy questions, but they fall outside CODIS's standard operations. The mainstream use of CODIS – matching crime-scene DNA to offender profiles has been solidly upheld by courts as a legitimate and invaluable law enforcement tool.

An illustrative judicial pronouncement is the Supreme Court's reasoning in *Maryland v. King*, which explicitly likened DNA identification of arrestees to fingerprinting and photographing routine booking procedures that serve law enforcement interests in identifying the person and uncovering their criminal history[26]. By validating DNA collection at arrest, the Court effectively acknowledged the database's role in quickly linking arrestees to past unsolved crimes as happened in that case, where the DNA taken from Mr. King upon his arrest for assault solved an unrelated rape. Additionally, even though *King* concerned arrestees, convicted-offender DNA laws had been upheld in earlier cases in lower courts on similar reasoning: once someone is convicted or even just on supervised release, courts found the government's interest in monitoring and identifying recidivists outweighs the reduced privacy expectations of the offender. One of the few areas where courts have drawn a line is the DNA collection of persons not implicated in crimes, for example, there is no law and likely would be no support for taking DNA from the general population or from mere suspects without any arrest or warrant, as that would raise grave Fourth Amendment issues.

Overall, U.S. case studies demonstrate the effectiveness of DNA databases in practice: solving crimes that otherwise would remain unsolved, and doing so in a manner largely consistent with constitutional norms as interpreted by courts. The judiciary's role has mainly been to ensure procedural safeguards like confirming a match with additional testing and allowing cross-examination of forensic experts rather than to second-guess the policy of maintaining the database itself, which by now is widely accepted in the justice system.

India

DNA evidence has begun to play a significant role in India's criminal justice system, particularly in high-profile cases. In the *Nirbhaya* gang rape case, for example, DNA profiling conclusively identified the perpetrators and was instrumental in securing their convictions. Biological samples collected from the victim were matched to the accused, providing scientific corroboration of eyewitness and confession evidence. The success of DNA in that notorious case underscored to law enforcement and the public how valuable forensic evidence can be for ensuring accountability in heinous crimes. Indian courts generally regard DNA evidence as highly reliable, the Delhi High Court noted in *Santosh Kumar Singh* that a properly obtained DNA report is scientifically accurate and can be crucial in proving guilt[27]. As a result, courts have often urged investigators to use DNA tests wherever available, especially in sensitive cases like sexual offenses or murder, to bolster the evidence.

At the same time, courts acknowledge the limits and context of DNA evidence. For instance, in a 2021 rape case, the

[24] Ibid 1.
[25] Ibid 24.
[26] Ibid 2.
[27] Ibid 24.

Calcutta High Court refused to drop charges just because the accused's DNA was not found in the forensic samples, emphasizing that lack of a DNA match does not automatically exonerate an accused, rape can occur without leaving DNA traces the perpetrator might not ejaculate or might wear protection, etc.[28] This reflects a balanced understanding: DNA is a powerful tool, but it is not always available in every case, and a case can be proven or disproven with other evidence as well. It also shows judicial awareness that over-reliance on DNA alone could be problematic if, for example, the absence of DNA evidence starts being seen as proof of innocence regardless of other evidence.

As India builds a DNA database under the CPI Act 2022, these judicial attitudes suggest that while DNA matches will be a powerful investigative tool, their use will be scrutinized for fairness and accuracy. The judiciary is likely to insist that the foundational science is sound and that the rights of the accused are respected during DNA collection and analysis. One can expect courts to issue guidelines, as they have in other areas of criminal procedure, on how DNA evidence should be handled, possibly reinforcing the need for consent in certain situations or the prompt destruction of samples when not needed.

It is expected that as the national DNA database becomes operational, cases will emerge where database "hits" solve crimes by linking suspects to earlier offenses. Pilot projects in states like Himachal Pradesh have already begun to demonstrate this potential: Himachal authorities reported creating a local DNA database and, for example, matching a repeat offender's DNA from a new crime to a previous crime scene, thereby identifying him[29]. Once the national database is in place, similar matches could occur across state lines (e.g., an unknown DNA profile from a crime in State A matching an ex-convict's profile uploaded by State B). Such developments will test the Indian legal system's preparedness to handle DNA evidence at scale.

Ongoing legal challenges to the CPI Act are also part of the evolving case law. Petitioners have argued that the Act's provisions – like retaining biometric and DNA data of people who were never convicted infringe fundamental rights. The courts' responses to these challenges could directly impact how DNA databases operate. For example, a court might rule that retaining the DNA of an acquitted person violates the right to privacy and direct that such data be deleted, thereby altering the retention policy. Or the courts might uphold the law but read in safeguards as they did with the Aadhaar biometric ID system, by introducing additional privacy measures through their judgment. Thus, India's judiciary will likely shape the contours of the DNA database program through case-by-case decisions and possibly policy guidelines aimed at ensuring the system is used in a constitutionally permissible manner.

In summary, India's experience with DNA in criminal justice, though more recent and limited than that of the U.S., already demonstrates both the technology's promise and the importance of legal safeguards. Courts have embraced DNA when it strengthens the search for truth, yet remain vigilant that its use must align with constitutional values and evidentiary principles. As DNA databases are rolled out, the interaction between technological capabilities and judicial oversight will largely determine how effective and just they turn out to be.

Technical, Ethical, and Social Dimensions

The deployment of DNA databases implicates several technical and ethical considerations.

Privacy and Consent- Collecting DNA samples intrudes on bodily autonomy, yet in criminal justice this is generally authorized by law without individual consent (e.g. mandatory DNA swabs from arrestees or convicts)[30]. To mitigate privacy issues, databases like CODIS use only non-coding "junk DNA" markers and store profiles without personal names.This limits the information to identification purposes. Nonetheless, privacy concerns remain: a DNA profile is a unique identifier, and retention of someone's genetic data (especially if they were later acquitted) is seen as invasive. This has led to policies allowing removal of profiles of innocent individuals (expungement) and debates on how long profiles should be kept[31]. Ensuring robust data protection (encryption, access control, audit logs) is critical to prevent unauthorized use of DNA data.

Surveillance and Misuse Risks- A major concern is that expansive DNA databases could facilitate unwarranted surveillance. If profiles of a large portion of the population are stored (as could happen with broad arrestee databases), authorities might be tempted to use them beyond their intended scope. For example, indefinite retention of DNA from persons not convicted was deemed a privacy violation by the European Court of Human Rightsfile-t9mjdz73idhfcsndfxskty. There is also a fear of misuse – such as planting of someone's DNA at a crime scene or targeting certain communities. Disproportionate representation of minorities in DNA databases as seen in the U.S., can raise equity issues, since those communities effectively become subject to greater genetic monitoring[32]. These concerns underscore the

[28] Ibid 27.
[29] Ibid 27.
[30] Ibid 2.
[31] Ibid 6.
[32] "DNA Database Controversies | Research Starters | EBSCO Research" (EBSCO) https://www.ebsco.com/research-starters/computer-science/dna-database-controversies

need for strict purpose limitation using DNA only for legitimate investigations and oversight. Independent bodies or clear legal rules should supervise database use to ensure that it doesn't become a tool of general surveillance or harassment.

Accuracy and Quality Control- Technically, the effectiveness of a DNA database depends on the quality of DNA profiling and analysis. DNA matching is highly reliable when done correctly, but errors can occur through sample contamination, mislabelling, or misinterpretation. Both the U.S. and India have stressed lab accreditation and standard protocols to minimize errors. For instance, CODIS requires participating labs to meet quality assurance standards, and DNA reports are subject to verification. However, backlogs in testing can delay justice – India has faced significant DNA case backlogs due to limited lab capacity[33]. Addressing these requires investment in forensic infrastructure and training. Additionally, complex DNA mixtures or partial profiles require careful expert interpretation; undue reliance on DNA without context can be problematic. Courts in both countries maintain that DNA evidence, while powerful, must be weighed alongside other evidence and that the scientific processes behind it be open to scrutiny. Regular audits, proficiency testing of analysts, and the ability of defendants to challenge DNA evidence e.g., via independent re-testing are all important practices to uphold accuracy and fairness in the use of DNA databases.

Implementation Challenges and Data Retention

Practical challenges affect the efficacy of DNA databases. One issue is laboratory capacity and backlog. The U.S. had to invest heavily to eliminate backlogs of untested rape kits and expand lab capabilities; even today, timely analysis is essential to maximize database benefits. India faces a more acute challenge: a shortage of forensic DNA labs and trained personnel has led to significant delays with thousands of samples pending analysis[34]. Scaling up a national DNA database will require major investments in infrastructure, manpower, and training. Without sufficient capacity, the promise of fast DNA matches solving crimes could be undercut by slow processing times.

Data retention policies also pose implementation questions. The U.S. retains most convicted-offender profiles indefinitely but permits removing profiles of arrestees who are not charged or are acquitted though expungement is not always automatic[35]. This approach attempts to balance long-term utility with fairness to the innocent. In India, however, the default under the CPI Act is to retain all collected profiles for 75 years, effectively for life[36]. Records are removed only if a person is acquitted and all legal proceedings conclude – and even then, removal is not guaranteed without a specific request and court direction[37]. Such extensive retention is unprecedented internationally and raises concerns about proportionality[38] Implementing a massive database with lifelong retention will necessitate robust data management and security for decades. It may also invite legal and public scrutiny, increasing pressure to introduce more nuanced retention rules for example, automatic deletion of profiles of those not convicted, or time limits for certain categories. Striking the right balance in retention, preserving profiles long enough to be useful in solving crime, but not so long as to infringe on privacy unnecessarily remains an ongoing challenge as India operationalizes its database.

Balancing Crime Control and Individual Rights

Both the U.S. and India grapple with finding the equilibrium between utilizing DNA databases for crime control and upholding individual rights. The U.S. approach, reflected in court decisions like *Maryland v. King*, generally leans toward enabling law enforcement uses of DNA with privacy safeguards considered through a reasonableness balancing test[39]. The prevailing view has been that the benefits of solving crimes, deterring offenders, and exonerating the innocent justify the relatively modest intrusion of DNA collection from those in custody. Indeed, the success of CODIS in aiding hundreds of thousands of investigations[40] has bolstered public and judicial support for the system's crime-control value. American courts have nevertheless imposed some limits, for instance, requiring expungement procedures and not allowing DNA collection beyond certain categories such as not from mere suspects at large, only from arrestees under formal processing. In essence, the U.S. has tilted the balance toward public safety while carving out exceptions to protect those not convicted or not involved in crime.

[33] Gupta MD, "Over 12,000 Sexual Assault Cases Pending Due to Backlog at Forensic Labs | India News" Hindustan Times (April 26, 2018) https://www.hindustantimes.com/india-news/over-12-000-dna-samples-from-sexual-assault-cases-pending-examination-at-forensic-labs/story-AzD26fBHTEibaUu7OKinoN.html
[34] Ibid 38.
[35] Suter SM, "A LL IN THE FAMILY: PRIVACY AND DNA FAMILIAL SEARCHING," vols 23–23 (Harvard Journal of Law & Technology, 2010) https://jolt.law.harvard.edu/articles/pdf/v23/23HarvJLTech309.pdf
[36] Ibid 40.
[37] Ibid 40.
[38] Ibid 9.
[39] Ibid 2.
[40] Ibid 1.

In India, the balance must accord with the constitutional mandate of proportionality under the right to privacy[41]. The sweeping provisions of the CPI Act – broad collection and long retention will likely be tested against this standard. The fundamental question is whether the same public safety outcomes could be achieved with narrower measures that intrude less on individual rights. For example, could India restrict DNA collection to serious offenses and still solve the majority of crimes of concern? If so, retaining an all-encompassing approach might be deemed disproportionate. The Indian judiciary's interim responses (e.g., granting stay orders or expressing concerns during hearings) suggest an acute awareness of the need to protect privacy and prevent abuse. At the same time, courts cannot ignore the country's law-and-order needs – India faces low conviction rates in violent crimes and a DNA database is seen by many in law enforcement as a way to bolster investigations with scientific evidence.

A notable aspect of balancing in India is the emphasis on necessity and least intrusive means. This was highlighted in *Puttaswamy* and will inform analysis of the DNA database. If a less intrusive database with shorter retention or limited scope could significantly advance criminal justice, the more sweeping version may not pass muster. Additionally, the principle of accountability is crucial: having independent oversight and clear rules can help ensure that the use of the database is targeted at crime control and not, for instance, political surveillance. The courts may insist on such accountability mechanisms as part of what makes the system reasonable and fair just as the Supreme Court, in upholding the Aadhaar biometric ID program for certain purposes, also read in guidelines to prevent misuse.

From a comparative perspective, both countries recognize that DNA databases serve the public interest by increasing the effectiveness of law enforcement. The difference lies in how much weight is given to individual privacy and due process in the equation. The U.S., through its common law and pragmatic approach, has largely normalized DNA databases for criminals, reining them in with specific privacy tweaks. India's higher courts, armed with a newer and broader conception of privacy rights, are more poised to demand adjustments to the law to ensure a closer fit between means and ends. We might anticipate that India's final equilibrium will permit a robust DNA database but with stricter boundaries (perhaps more so than the U.S.), reflecting its constitutional ethos that fundamental rights can only be curtailed to the minimum extent necessary even for a compelling public interest.

Ultimately, the goal in both jurisdictions is to maximize justice: DNA databases should help catch perpetrators and prevent future crimes, thereby serving society's interest in security and justice, but they should not do so at the cost of wrongly ensnaring the innocent or unduly compromising the privacy and dignity of individuals. Achieving that balance is an ongoing process, requiring continual oversight and willingness to recalibrate policies in light of experience, technological changes, and evolving notions of rights.

Best Practices

Drawing on the U.S. experience and the current discourse in India, several best practices emerge to ensure DNA databases are effective in fighting crime while respecting individual rights. The following suggestions, aligned with international norms and jurisprudence, could improve India's framework and enhance the overall integrity of DNA database programs:

Clearly Define Scope and Purpose: The law should explicitly restrict DNA database use to legitimate criminal justice purposes. Profiles and samples should be collected and searched only for identifying suspects, exonerating the innocent, investigating specific crimes, or identifying missing persons and unidentified human remains[42]. Explicitly prohibit any use of DNA data for unrelated purposes such as general population surveillance, caste/community profiling, or unauthorized research. A well-defined scope builds public trust and ensures that the database remains a targeted tool, not a dragnet.

Use Minimal Genetic Information: Follow the CODIS model by using only non-coding DNA loci for profiling genetic markers that do not reveal sensitive personal information[43]. By limiting DNA profiles to these identification markers, the database avoids storing data about genetic traits or health conditions. Additionally, once a DNA sample is analyzed and a profile obtained, establish a policy to destroy or archive the biological sample in a manner that prevents any further testing beyond the identification markers. This prevents misuse of retained samples which contain full genomic information and adheres to the principle of data minimization.

Strengthen Data Protection and Security: Treat DNA profiles as highly sensitive personal data. Agencies managing the database (like NCRB in India or the FBI's CODIS unit) should implement state-of-the-art security measures: encryption of data at rest and in transit, strict user authentication, and role-based access controls so that only authorized personnel can input or search profiles. Every access to the database should be logged and subject to audit to detect any improper queries. Personal identifying information should be kept separate from the DNA profile database e.g., each profile can be tagged with a code, and a secure, separate system links the code to an individual's identity only when a match needs to be followed up. This separation means that even if the DNA data were compromised, it wouldn't be immediately clear whose data it is,

[41] Christine Rosen, 'Liberty, Privacy, and DNA Databases' (2003) 1 The New Atlantis 37. https://www.jstor.org/stable/43152851

[42] Ibid 46.

[43] Ibid 46.

adding a layer of privacy protection.

Proportionate Retention and Expungement Policies: Adopt a nuanced approach to data retention that balances public safety with individual rights[44]. For example:

Convicted offenders: Retain DNA profiles of persons convicted of serious violent or sexual offenses indefinitely or for a very long period, as these individuals have a higher likelihood of reoffending or being linked to past crimes. For minor offenses, consider a finite retention period (e.g., retain for X years after sentence completion) to avoid lifelong stigma for low-level crimes.

Arrestees and suspects: If a person's DNA is collected at arrest but they are not charged or are acquitted, their profile should be removed from the database promptly[45]. Implement automatic expungement procedures – for instance, require that whenever charges are dropped or an acquittal becomes final, the investigating agency or court informs the DNA database custodian to purge the person's DNA record. This relieves the individual from having to navigate bureaucratic hurdles to get their data removed.

Periodic review: For profiles that are retained, especially those not linked to convictions (e.g., from persons held under preventive detention or from volunteers), consider periodic review to decide if continued retention is necessary. If a profile has not matched any crime in, say, 10 or 15 years and the person has no subsequent criminal record, a case could be made for purging it to protect privacy without materially harming law enforcement.

These retention guidelines, if enacted, ensure that the database remains focused and fair aiding in catching criminals but not indefinitely holding data on those who posed little demonstrable risk or were not found guilty. They also align with constitutional principles of proportionality by not retaining data longer than needed.

Independent Oversight and Accountability: Establish an independent oversight body or empower existing human rights/data protection institutions to oversee the DNA database's operation. This body could include retired judges, forensic experts, scientists, and citizen representatives. Its functions would be to audit compliance with the law e.g., ensuring profiles are deleted when they should be, handle grievances or complaints such as an individual alleging their DNA was taken or kept unlawfully, and periodically review and report on the database's performance and privacy impact. For instance, the oversight body can publish annual statistics on how many profiles are in the database, how many were added or removed in the year, how many crime scene-to-person matches were made, and any incidents of misuse. Independent oversight adds transparency and assures the public that the database is not a black box of police powers. The U.K.'s Biometrics Commissioner model – which scrutinizes police retention decisions – is a useful example: a similar mechanism in India could review, for example, any magistrate orders to retain acquitted persons' data[46] to check for abuse.

Quality Assurance and Training: The credibility and efficacy of a DNA database rest on the quality of its data. Therefore, enforce rigorous quality assurance standards for every step from collection to analysis: Only trained personnel should collect DNA samples, following standard operating procedures to avoid contamination or mix-ups. Providing police and medical staff with DNA collection kits and clear protocols as India's government has done for sexual assault evidence kits[47] is essential. Forensic laboratories analysing DNA must be accredited to international standards (such as ISO 17025) and participate in regular proficiency testing. Quality audits (internal and external) should be conducted to ensure they meet the required standards in techniques and interpretation. Implement measures like "elimination databases" of DNA from laboratory staff and first responders, so any accidental contamination can be recognized if their DNA appears in a crime sample[48]. Invest in reducing backlogs by increasing lab capacity and manpower. A DNA database loses effectiveness if crime-scene samples wait months or years to be processed. Using a portion of public safety funds (like the Nirbhaya Fund in India) to modernize labs and hire/train analysts pays dividends in faster turn-around and more timely database hits. Train judges, prosecutors, and defense attorneys in the basics of DNA evidence. Stakeholders should understand what a "match" means statistically, how to interpret probability estimates, and how to handle complex scenarios (like mixed DNA profiles). This ensures that DNA evidence is evaluated correctly in court and that lawyers can make pertinent arguments or ask the right questions of experts.

By maintaining high technical standards and expertise, wrongful inclusions or exclusions based on DNA are minimized, thereby protecting individuals from miscarriages of justice and reinforcing the database's integrity.

Transparency and Public Awareness: Proactively share information to demystify the DNA database and demonstrate its value. Publishing regular reports (without compromising case confidentiality) that show, for example, how many crimes

[44] Ibid 46.
[45] Ibid 46.
[46] Ibid 46.
[47] Ibid 27.
[48] Biological Data Interpretation & Reporting Subcommittee, Biology/DNA Scientific Area Committee, and Organization of Scientific Area Committees (OSAC) for Forensic Science, "Best Practice Recommendations for the Management and Use of Quality Assurance DNA Elimination Databases in Forensic DNA Analysis" (2019).

were solved with DNA matches each year, and detailing any notable successes or errors, will inform public debate. Transparency about the number of profiles collected, how many belong to convicts vs. arrestees, and how many have been removed due to acquittal etc., can help gauge whether the system is functioning as intended. Publicize safeguards in place: the government can, for instance, highlight that only non-coding DNA is used, or that innocent people's profiles are deleted, to alleviate fears. Engaging with civil society and privacy commissioners in these disclosures can add credibility. Public awareness campaigns can also educate people on their rights related to DNA (such as the right to request removal if acquitted) and encourage support for the database by focusing on its role in justice (for example, sharing stories where DNA evidence identified a repeat offender or freed an innocent person). When citizens perceive the DNA database as both effective and well-regulated, cooperation with DNA collection and trust in forensic justice will be higher.

By incorporating these best practices, India can move toward a framework that mirrors the strengths of the U.S. system (and other international examples) while avoiding pitfalls. The U.S., too, can continue to improve by learning from critiques – for instance, simplifying expungement procedures or carefully evaluating any expansion to new categories (like misdemeanor arrestees). Fundamentally, best practices strive to make the DNA database a precision instrument of justice: targeted, accurate, secure, and rights-respecting. Such a balanced approach will improve the efficacy of DNA databases in delivering on their promise – solving crimes and enhancing public safety – without unduly compromising the values of a free and fair society.

2. CONCLUSION

DNA databases have emerged as powerful tools in criminal justice, markedly improving the ability of law enforcement to identify perpetrators and solve crimes, sometimes decades after the fact. The United States' experience with CODIS demonstrates that when these databases are leveraged properly, they can bolster public safety – CODIS has aided over half a million investigations, bringing offenders to justice and providing closure in cold cases[49]. At the same time, DNA technology has exonerated innocent individuals, underlining its role in enhancing the fairness and accuracy of the justice system[50]. India, seeking to modernize its criminal justice apparatus, stands to benefit greatly from integrating DNA analysis and databases, particularly given challenges like low conviction rates for violent crimes. A well-implemented DNA database could help identify repeat offenders, deter crime, and ensure that the guilty are caught while the innocent are not wrongfully punished.

However, the expansion of DNA databases must be carefully calibrated to respect individual rights. The potential for misuse – whether through unwarranted surveillance, data breaches, or retention of DNA profiles of innocents – is a real concern that needs to be addressed through law and oversight. India's current legislative experiment with the CPI Act 2022 will test how a balance can be struck under a constitutional framework that is very protective of personal liberty and privacy. The comparative insights from the U.S. (and other countries) suggest that it is possible to harness DNA for its crime-fighting benefits **and** impose sensible limits to protect civil liberties. For instance, limiting DNA collection to what is necessary, not retaining profiles longer than justified, and providing transparency and remedies (like expungement) are measures that allow a database to function without becoming a tool of oppressive surveillance.

In conclusion, the efficacy of DNA databases in criminal justice should be measured not only by the crimes solved and offenders apprehended, but also by the extent to which the system upholds the rule of law and individual rights. A DNA database that helps convict the guilty while scrupulously avoiding infringement on the innocent represents the ideal balance. The U.S. and India, through their evolving laws and court decisions, are converging on that principle from different starting points – the U.S. from a pragmatic expansion tempered by specific safeguards, and India from a rights-based scrutiny ensuring any expansion is justified and proportionate. The trajectory in both countries underscores an important lesson: technology in the service of justice works best when guided by the values of justice. With prudent legal frameworks and vigilant oversight, DNA databases can indeed serve as a cornerstone of modern criminal justice, a tool that helps convict the guilty, exonerate the wronged, and ultimately, uphold the rule of law.

References

[1] FBI Laboratory, 'CODIS–NDIS Statistics' https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis/codis-ndis-statistics accessed 10 December 2025.

[2] Maryland v King' (webpage, n.d.) https://epic.org/documents/maryland-v-king-2/ accessed 10 December 2025.

[3] Jilsblognujs VAPB, "DNA Databases and the Right to Privacy: Analysing the Criminal Procedure (Identification) Act 2022 and CODIS" (The Journal of Indian Law and Society, August 21, 2023) https://jilsblognujs.wordpress.com/2023/08/21/dna-databases-and-the-right-to-privacy-analysing-the-criminal-procedure-identification-act-2022-and-codis/

[4] "The Criminal Procedure (Identification) Bill, 2022" (PRS Legislative Research) https://prsindia.org/billtrack/the-

[49] Ibid 1.
[50] Ibid 24.

criminal-procedure-identification-bill-2022#:~:text=Data%20permitted%20to%20be%20collected

[5] George J Annas, 'Privacy Rules for DNA Databanks: Protecting Coded "Future Diaries"' (1993) 270(19) Journal of the American Medical Association 2346.

[6] Interpol, Global DNA Profiling Survey Results (report, 2019) https://www.interpol.int/content/download/15469/file/INTERPOL%20Global%20DNA%20Profiling%20Survey%20Results%202019.pdf

[7] Tanmay Singh and Gayatri Malhotra, 'The Digital Data Protection Bill 2022 Does Not Satisfy the Supreme Court's Puttaswamy Principles' (web article, n.d.) https://internetfreedom.in/the-digital-personal-data-protection-bill-2022-does-not-satisfy-the-supreme-courts-puttaswamy-principles/

[8] "Examining the Constitutionality of the Criminal Procedure (Identification) Act, 2022" (Constitutional Law Society, October 15, 2023) https://clsnluo.com/2022/08/01/examining-the-constitutionality-of-the-criminal-procedure-identification-act-2022/#:~:text=Examining%20the%20Constitutionality%20of%20the,mechanism%2C%20being%20%E2%80%9Carbitrary%E2%80%9D%20and

[9] India Legal, "Supreme Court Refuses to Entertain Plea Challenging Constitutionality of Criminal Procedure Act, 2022" (India Legal, February 12, 2024) <https://indialegallive.com/constitutional-law-news/supreme-court-news/criminal-procedure-act-plea/#:~:text=,Identification%29%20Act%2C>

[10] Srivastava A and others, "Impact of DNA Evidence in Criminal Justice System: Indian Legislative Perspectives" (2022) 12 Egyptian Journal of Forensic Sciences https://doi.org/10.1186/s41935-022-00309-y

[11] Das A and Law L, "Supreme Court Refuses to Entertain Challenge to Law Allowing Collection of Prisoners' Biometrics; Asks..." Live Law (February 15, 2024) https://www.livelaw.in/top-stories/supreme-court-pil-criminal-procedure-identification-act-internet-freedom-foundation-high-court-249253#:~:text=Supreme%20Court%20Declines%20to%20Hear,Awstika%20Das

[12] "In Rape Cases, DNA Evidence Would Not Be Conclusive Proof: Calcutta High Court – Child Rights Clinic – Every Child Counts" https://jgu.edu.in/child-rights-clinic/in-rape-cases-dna-evidence-would-not-be-conclusive-proof-calcutta-high-court/#:~:text=In%20rape%20cases%2C%20DNA%20evidence,man%20in%20a%20rape%20case

[13] Desk TW, "DNA Data Bank Still a Work in Progress - The Tribune" The Tribune (May 1, 2022) https://www.tribuneindia.com/news/himachal/dna-data-bank-still-a-work-in-progress-390888/#:~:text=The%20DNA%20Technology%20,to%20a%20question%20in%20Parliament

[14] "DNA Database Controversies | Research Starters | EBSCO Research" (EBSCO) https://www.ebsco.com/research-starters/computer-science/dna-database-controversies

[15] Gupta MD, "Over 12,000 Sexual Assault Cases Pending Due to Backlog at Forensic Labs | India News" Hindustan Times (April 26, 2018) https://www.hindustantimes.com/india-news/over-12-000-dna-samples-from-sexual-assault-cases-pending-examination-at-forensic-labs/story-AzD26fBHTEibaUu7OKinoN.html

[16] Suter SM, "A LL IN THE FAMILY: PRIVACY AND DNA FAMILIAL SEARCHING," vols 23–23 (Harvard Journal of Law & Technology, 2010) https://jolt.law.harvard.edu/articles/pdf/v23/23HarvJLTech309.pdf

[17] Christine Rosen, 'Liberty, Privacy, and DNA Databases' (2003) 1 The New Atlantis 37. https://www.jstor.org/stable/43152851

[18] Biological Data Interpretation & Reporting Subcommittee, Biology/DNA Scientific Area Committee, and Organization of Scientific Area Committees (OSAC) for Forensic Science, "Best Practice Recommendations for the Management and Use of Quality Assurance DNA Elimination Databases in Forensic DNA Analysis" (2019).