A COMPETITIVE STUDY OF JURISPRUDENTIAL ASPECTS OF BIOMETRIC EVIDENCE IN INDIA, UK, USA

Chirag Chaudhary, Research Scholar, Law College Dehradun, Uttaranchal University, Uttarakhand

Satyam Sharma, Assistant Professor, Law College Dehradun, Uttaranchal University, Uttarakhand

ABSTRACT

Biometric evidence is an important tool that is used in legal systems today for identifying people investigating crimes and detecting crimes. Biometric evidence like fingerprints, DNA profiling, iris scans, facial recognition and voice recognition are being used more and more by governments police agencies and courts over the world. These technologies make criminal investigations more efficient and accurate. They also raise serious concerns about privacy, surveillance, human dignity and the misuse of personal biometric data.

This research paper looks at the aspects of biometric evidence by comparing how India, the United Kingdom and the United States use biometric evidence. The study examines how courts and legal systems in these countries collect, store and use information as evidence. In India the research paper focuses on what happened after the court case Justice K.S. Puttaswamy v. Union of India which said that privacy is a right and changed how biometric data is understood under the Aadhaar framework.

The paper also talks about the Indian Evidence Act, Sections 45 and 65B and how they decide if biometric and electronic evidence can be used in court. The paper compares this to the United States, where courts have allowed the police to collect data more widely especially after the case Maryland v. King. It also compares it to the United Kingdom and European courts which put emphasis on proportionality and protecting privacy especially in the case S. And Marper v. United Kingdom.

The research paper also identifies problems with biometric evidence, including mistakes in technology biases in algorithms lack of transparency in forensic methods weak rules to protect people and the risk of mass surveillance. It points out that India does not have a law to govern biometric evidence and stresses the need for stronger rules, independent oversight, and accountability in forensic science and safeguards to protect privacy.

The paper concludes that while biometric evidence can make the criminal

justice system stronger and investigations more efficient using it without checks can threaten the freedoms guaranteed by the constitution and the right, to a trial. Therefore we need a legal framework to ensure that technology is used within the limits of what is morally right follows due process and protects individual biometric evidence rights.

INTRODUCTION

The way technology is growing fast has changed how crimes are investigated and how people are identified. This is especially true for things like fingerprints and DNA. These things are unique to each person. Are being used more and more by governments and courts to keep people safe.

In the few years technology that uses things like fingerprints and DNA has become a big part of how we are governed and watched. For example in India they started using a system called Aadhaar, which collects a lot of information about people, including data. This has raised a lot of questions about whether this is okay and if people's privacy is being respected.

Biometric evidence, like DNA and fingerprints is being used more and more in cases because it is thought to be very reliable. There are still some problems with it. Sometimes the wrong person can be. The computers used to analyze the data can make mistakes. Also people are worried about how their personal information's being used.

This research paper is looking at how biometric evidence's used in India, the United Kingdom and the United States. It is comparing the laws and rules in these countries to see how they handle evidence. The paper is also looking at the challenges that come with using evidence like making sure peoples rights are respected. The goal is to figure out how we can use evidence to keep people safe while also making sure we are being fair and respecting people's rights.

The paper is studying evidence, in these countries to see how the laws are working. It wants to know if the laws are good enough to protect people's rights when it comes to evidence. The paper is looking at evidence to see how it can be used to help with justice and security while also making sure that people are treated fairly and that their rights are respected. The main goal is to make sure that biometric evidence is used in a way that's fair and respectful of people's rights and that it helps to keep people safe.

RESEARCH OBJECTIVES

This research paper is going to look at how biometric evidence's being used more and more in modern legal systems and what this means for the law.

The study wants to find out how things like fingerprints and DNA profiling are being used to solve crimes and what happens in court. It also wants to see if the laws we have now are good enough to protect peoples privacy and make sure they get a trial.

The research is also looking at how courts balance keeping people safe, with making sure individuals have their rights protected. By looking at what courts have said what the laws say and how other countries do things this paper is trying to find out what is going wrong with evidence and how we can make the legal system better and more transparent.

Key Objectives of the Study

- The goal is to learn about evidence in legal systems, including what evidence is, how evidence works and how evidence is used.
- We need to look at how biometric evidence's accepted and valued in Indian law especially under the Indian Evidence Act and the principles of the Indian constitution.
- It is important to think about the issues related to surveillance, privacy and self-incrimination from a legal and constitutional point of view and what this means for biometric evidence.
- We will carefully examine court decisions about evidence in India, the United Kingdom and the United States to see what these court decisions mean for biometric evidence.
- Biometric technologies have problems, such as biased algorithms, mistakes in forensics, misuse of biometric data and spying on many people, which we need to think about when we use biometric evidence.
- We have to see how biometric technologies affect human rights like privacy, dignity, freedom and a fair trial and how biometric evidence impacts these human rights.

- We need to find the gaps and weaknesses in the forensic systems for biometric evidence in India so we can make biometric evidence better.

- It is necessary to think about whether we need laws to regulate evidence, independent oversight and rules to follow when using biometric evidence.

LITERATURE REVIEW (SELECTED THEMES)

1). Statutory Framing and Techno-Legal Governance

Legal scholarship identifies the Aadhaar framework and the Aadhaar Act, 2016 as a major development in India's techno-legal governance system. The large-scale collection of fingerprints and iris scans by the State normalized biometric identification in welfare delivery, banking, and public administration.

Scholars argue that Aadhaar improved administrative efficiency and reduced identity fraud, but also created concerns regarding surveillance, privacy, data misuse, and informational autonomy. The landmark judgment in Justice K.S. Puttaswamy v. Union of India strengthened privacy jurisprudence by recognising privacy as a fundamental right and introducing principles such as proportionality, purpose limitation, and data protection safeguards (UIDAI).

2). Evidentiary Doctrine

Scholars in India look at evidence under Indian law. They mainly focus on two sections of the Indian Evidence Act: Sections 45 and 65B. Section 45 says courts can use opinions in cases involving fingerprints and DNA profiling. These expert opinions are used for evidence. Section 65B is about records and whether they can be used as evidence.

After some court cases like Anvar P.V. V. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal experts started saying that electronic evidence needs a certification to be allowed in court. Researchers also point out that courts make a difference between allowing evidence and its value. This means judges have to check if biometric evidence's reliable and real before using it.

They have to do this check on their own. The biometric evidence and electronic records are two things judges have to be careful, with. Courts rely on evidence and electronic records every

day. it (Cyril Amarchand Blogs+1).

3). Forensic Reliability and Error

Forensic scientists and legal scholars say that biometric technologies can be wrong even though they are seen as reliable. Fingerprint analysis, Facial recognition systems, DNA profiling can all give results. This happens because the sample quality is poor humans make mistakes or the algorithm is biased.

Researchers are especially worried about recognition. They say it does not work well for women and people with darker skin. This raises concerns, about policing and people being wrongly arrested. The Brandon Mayfield case is often mentioned. In this case a fingerprint was misidentified. It shows the dangers of relying much on automated systems. Scholars think we need to be careful. They suggest we should have: Accredited laboratories, Human verification, and Clear methods review of forensic evidence. This can help prevent mistakes.

Biometric technologies can be very helpful. We need to use them carefully. Fingerprint analysis, recognition and DNA profiling are all useful tools. However we must make see they are used correctly. That is why we need laboratories and human verification. We also need to make sure that the methods are clear and transparent. An independent review can help ensure that everything is done correctly. By taking these steps we can trust technologies. They can help us solve crimes and keep people safe. (Federal Bureau of Investigation+1).

JUDICIAL APPROACH (INDIA) — DOCTRINES & TRENDS

1. Privacy as Foundational

The Supreme Court's decision in Justice K.S. Puttaswamy v. Union of India marked a turning point in

Indian constitutional jurisprudence by recognizing privacy as a fundamental right under Article 21 of the Constitution. The judgment established that any State intrusion involving biometric collection must satisfy the tests of legality, necessity, proportionality, and legitimate state interest. In the Aadhaar litigation, the Court upheld the constitutional validity of biometric identification for welfare purposes but imposed safeguards relating to data protection, purpose limitation, and restricted data sharing. Scholars consider this judgment foundational in defining

constitutional boundaries for surveillance, digital governance, and future biometric programs in India (UIDAI).

2. Admissibility vs. Weight

Indian courts generally admit biometric and electronic evidence under Section 65B of the Indian Evidence Act, provided procedural requirements such as certification, authenticity, and chain of custody are properly fulfilled. Judicial decisions including Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal reinforced the mandatory nature of Section 65B certificates for electronic evidence. However, courts clearly distinguish between admissibility and evidentiary weight. Even after admission, judges independently assess the reliability, integrity, and contextual relevance of biometric records before relying upon them for conviction, thereby ensuring procedural fairness and protection against misuse or manipulation (Cyril Amarchand Blogs+1).

3. Expert Testimony and Forensics

Indian courts depend a lot on opinions under Section 45 of the Indian Evidence Act to understand biometric evidence like fingerprints, DNA profiles, facial recognition results and forensic reports. They are being careful with evidence in criminal trials where people's freedom is, at stake. Courts have said that forensic labs should be accredited methods should be clear samples should be handled properly and experts should be questioned. Some people think courts are starting to see that forensic mistakes can happen and technology has limits, with automated systems. The courts are being careful to stop convictions and make sure biometric evidence is reliable, clear and trustworthy. (IJLMH).

CASE LAWS — DETAILED EXAMPLES

1. INDIA (SELECT, ILLUSTRATIVE)

- **K.S. Puttaswamy v. Union of India (2018)** — Landmark privacy ruling that shaped the constitutional limits on biometric data use (Aadhaar debate). The Court accepted the State's legitimate aims but mandated proportionality, purpose limitation, and safeguards for Aadhaar operations. UIDAI

- **Electronic evidence jurisprudence (post-2010s)** — A line of cases interpreting

Section 65B and emphasizing the requirement of certificates for admissibility of electronic records. Courts distinguish admissibility (existence/authenticity) from probative content. Cyril Amarchand Blogs+1

Note: India's case law on biometric evidence is still evolving; while Aadhaar litigation concerns largescale collection and privacy, criminal-procedure cases (fingerprints, DNA, facial recognition used in investigations and court) are decided on a blend of expert credibility, lab accreditation, and chain-ofcustody.

2. United States (select)

- **Maryland v. King (2013)** — U.S. Supreme Court held that DNA swabs taken from arrestees for identification purposes are reasonable under the Fourth Amendment, treating DNA cheek swabs analogously to fingerprints in booking procedures—an outcome that expanded state power to collect genetic identifiers at arrest. This case is a key comparative touchstone for debates over biometric sampling and privacy. Justia Law

- **Brandon Mayfield (FBI misidentification, 2004)** — A high-profile wrongful identification based on fingerprint database matching highlighted human and system errors in biometric matching, underscoring the need for verification, transparency, and remedies when automated matches drive investigations. Federal Bureau of Investigation+1

3. United Kingdom / Europe (select)

S. and Marper v. UK (ECHR, 2008) — The European Court of Human Rights found that indefinite retention of DNA and fingerprints of innocent persons violated Article 8 (privacy). The decision underscores proportionality and retention-limit principles that inform UK policy and offer a counterpoint to more permissive approaches. HUDOC

COMPARATIVE STUDY: UK & U.S LAWS — WHAT INDIA CAN LEARN?

1). US Model (Liberal on Collection, Constrained By Warrant/Fourth Amendment Corpus)

The US model uses a lot of data for law enforcement but it also has rules to protect peoples

rights. The Supreme Court made a decision in the case of Maryland v. King in 2013. They said that collecting DNA samples when someone is arrested is a search just like taking fingerprints. This helps police solve cases faster by checking DNA against crime databases. Some people are worried that collecting so much DNA data could lead to too much surveillance. The FBIs DNA database has grown really big. Thats making some people concerned about their privacy. The US model focuses on using DNA to help investigations. It also has to follow rules like getting a warrant or having a good reason to collect DNA. This is to make sure that the police don't misuse the DNA data. The US model tries to balance the need to solve crimes with the need to protect peoples rights. It relies on the Constitution to set limits, on how DNA data can be collected and used.

2). UK/European Model (Privacy And Retention Limits)

In contrast, the UK and broader European model is characterized by a strong emphasis on privacy and proportionality in biometric retention. The landmark European Court of Human Rights case, S. and Marper v. UK (2008), established that the indefinite retention of DNA and fingerprints from innocent individuals violated Article 8 of the European Convention on Human Rights. The Court ruled that permanent retention without a defined time limit was a disproportionate violation of privacy rights. Scholars argue that this case created a model based on retention limits, data minimization, and regular review. In Europe, the GDPR similarly sets a high bar for biometric data, requiring explicit consent and regular deletion. Thus, unlike the U.S., the UK approach limits state power, ensuring that even powerful tools like DNA databases do not erode personal privacy.

3). Implication for India

India is doing something with biometric governance. It is not like the United States or the United Kingdom. India is of in the middle. They have a system called Aadhaar. It is used for things. The way it is used for criminal justice is still being looked at by the courts. The Supreme Court said that some safeguards need to be in place. These safeguards do not really deal with how long information is kept or how it is used in investigations. India does not let the police collect DNA like the United States does.

India also does not have strong laws like the United Kingdom to control how long information can be kept. India can learn from both the United States and the United Kingdom. They can

use the idea of getting a warrant before collecting information like the United States. They can use the idea of only keeping information for a limited time like the United Kingdom. This way India can make sure that they are solving crimes and also protecting people's privacy rights. India needs to find a balance between these two things so that biometric systems, like Aadhaar are used in a way.

US model (liberal on collection, constrained by warrant/ Fourth Amendment corpus):

- *Maryland v. King* shows an acceptance of DNA for identification at arrest; US practice thereby privileges law-enforcement utility, often at the cost of broad genetic databases. The U.S. debate focuses on balancing identification utility vs. genetic privacy and potential misuse. Justia Law **UK / European model (privacy and retention limits):**

- *S. and Marper* insists on proportional retention and the inadmissibility of permanent state retention for innocents—a privacy-protective stance that constrains mass retention even for powerful forensic tools. HUDOC **Implication for India:**

- India's model currently falls between these poles: large-scale biometric enrolment (Aadhaar) exists with privacy safeguards post-Puttaswamy, but criminal-law usage, retention policies, and lab governance need clearer statutory guardrails akin to European proportionality or U.S. constitutional constraints depending on the tactic chosen. UIDAI+1

CRUX OF THE ISSUE

Biometrics offer unparalleled identification power but:

- **Technical fallibility** (sensor error, poor samples, algorithmic bias);
- **Opacity of algorithms & labs** (black-box models, non-accredited testing);
- **Disproportionate retention & mission creep** (systems built for welfare or ID can be repurposed for policing without clear safeguards); and
- **Weak procedural protections** in many criminal workflows (overreliance on automated "matches" as conclusive).

These converge to create a classic legal tension: evidentiary efficiency vs. constitutional

safeguards (privacy, fair trial, protection against self-incrimination).

LOOPHOLES & GAPS (DIAGNOSIS)

1. **Statutory lacunae for non-DNA biometrics** — While Aadhaar and proposed DNA regulation touch specific modalities, there is no unified statutory regime governing collection, retention, access, admissibility standards, accreditation, and redress for all biometric modalities. UIDAI+1

2. **Admissibility procedure uneven** — Courts accept biometric material but the procedural standards for validation (accreditation of labs, reproducible methods, audit trails) are inconsistent across jurisdictions and cases. Cyril Amarchand Blogs+1

3. **Algorithmic opacity and vendor dependence** — Law enforcement's use of proprietary facial recognition and matching systems lacks transparency and independent validation. This creates risks of wrongful identification (illustrated abroad by Mayfield and systemic weaknesses). Federal Bureau of Investigation+1

4. **Retention & purpose-limitation risk** — Large databases (Aadhaar, DNA indices) may be repurposed without statutory clarity on retention periods, access logs, or deletion—contravening privacy best practices. UIDAI+1

5. **Remedies & oversight** — Limited independent oversight (data protection, forensic accreditation boards) and weak, technical standards for admissibility mean errors are difficult to detect and remediate.

RECOMMENDATIONS (BRIEF & ACTIONABLE)

1. **Unified Biometric Evidence Code** — Draft a statutory framework covering collection, consent (where appropriate), purpose limitation, retention limits, accreditation, audit trails, transparency, and remedies. Use DNA Bill templates but broaden scope to include fingerprints, facial recognition, iris scans, and algorithmic matching. Digital Sansad

2. **Mandatory lab accreditation & method disclosure** — For any biometric relied upon in court, require lab accreditation, chain of custody documentation, and

disclosure of matching thresholds and error rates to defense counsel. IJLMH

3. **Independent oversight body** — Create a forensic-science regulatory authority (with technical and civil-liberties members) to set standards, maintain an auditor registry, and handle complaints. Digital Sansad

4. **Retention and minimization rules** — Establish time-bound retention consistent with privacy proportionality (a la *S. & Marper*), with strict rules for access and compelled deletion on acquittal/closure. HUDOC

5. **Judicial practice directions** — Supreme Court / High Courts should issue practice directions: (a) expert evidence must include method, error rates, and validation; (b) automatic matches are prima facie leads—not conclusive proof; (c) defence must get access to algorithms/thresholds under protective orders. Cyril Amarchand Blogs+1

CONCLUSION

Biometric evidence is at an important point in today's legal systems. It helps identify people accurately but it also raises big questions about privacy, fairness and the power of the state. In India the Aadhaar system is a step towards digital governance. It does not have clear rules about keeping and using biometric data for crimes. The United States has an approach to biometrics but the Fourth Amendment protects citizens' rights. The United Kingdom focuses on privacy. Being fair.

India relies heavily on Aadhaar for governance. However without laws there is a risk of mass surveillance hurting basic rights. India can learn from the United States and the United Kingdom. It should set limits on collecting data and have strict rules on how long it can be kept. A clear and open legal framework is needed. This framework must balance the efficiency of investigations with the need to protect privacy and fairness.

This way biometric power can be used responsibly. The Aadhaar system and biometric evidence are very important for India's future. India's use of Aadhaar and biometric evidence must be balanced with the protection of rights. The use of evidence, in India must be done in a way that is fair and transparent.

Key Takeaways:

- Aadhaar is a transformative tool, but India needs clearer statutory safeguards.
- The U.S. model shows investigative utility but risks overreach.
- The UK model ensures proportionality, preventing indefinite retention of innocent individuals.
- India should adopt a hybrid approach, balancing civil liberties with technological innovation.

WORKS CITED & REFERENCES (EXPANDED STATUTORY & POLICY SOURCES)

Key Judicial Decisions & Reports

- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, Writ Petition (Civil) No. 494 of 2012 — Supreme Court of India, judgment (26 Sept 2018). UIDAI
- *Maryland v. King*, 569 U.S. 435 (2013) — U.S. Supreme Court. Justia Law
- *S. and Marper v. United Kingdom*, European Court of Human Rights (2008). HUDOC

Statutes, Bills, and Policy

- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act,

  2016 (full text and amendments). UIDAI+1
- The DNA Technology (Use and Application) Regulation Bill, 2019 (text and analyses; note: parliamentary history and withdrawal updates). Digital Sansad+1
- Indian Evidence Act, 1872 — Section 45 (expert opinion), Section 65B (electronic records) — authoritative commentary and recent case law summaries. Cyril Amarchand Blogs+1

Select Scholarly & Policy Sources

- NCBI: "Cultural, Social, and Legal Considerations — Biometric Identification" (overview of forensic and biometric evidence challenges). NCBI
- FBI Statement and investigative reviews on the Brandon Mayfield fingerprint misidentification (case study of biometric error). Federal Bureau of Investigation
- Reports and summaries on forensic evidence standards and admissibility (UK Parliament forensic evidence submissions; professional legal blogs summarizing Section 65B implications).