



Forensic Evidence

Policy Leads: Aditi Karthikeyan¹

Policy Analysts: Afomiya Dejene^{#2}, Alan Le^{#3}, Mehek Saini^{#4}, Rohan Manchada^{#5}

Criminal Justice Policy Team, Institute for Youth in Policy

aditik@yipinstitute.org,

Abstract — This brief analyzes the privacy implications of how different jurisdictions handle DNA and forensic evidence. It proposes policy options to ensure proper and private handling of all forensic evidence.

Keywords — DNA, fingerprints, privacy, biological, swabs, FBI

I. EXECUTIVE SUMMARY

Ever since DNA profiling entered criminal justice systems in the late 1980s, governments have had to balance using genetic evidence to solve crimes with respecting personal privacy. In the United States, privacy rights regarding forensic DNA focus mainly on Fourth Amendment search and seizure protections. The key legal turning point came with the Supreme Court decision in [Maryland v. King \(2013\)](#), where a 5–4 majority ruled that police can swab the cheek of anyone arrested for a serious crime. The Court decided that a swab during booking is similar to fingerprints or photos, thus law enforcement's need to verify identity outweighs an arrestee's expectation of privacy.

Conversely, privacy rights in Europe took a very different turn after the landmark ruling by the European Court of Human Rights (ECtHR) in [S. and Marper v. United Kingdom \(2008\)](#). The court

ruled unanimously that the UK's policy of keeping DNA samples indefinitely—even from people who were never convicted—violated Article 8 of the European Convention on Human Rights (the right to private life). This forced the UK Parliament to pass the [Protection of Freedoms Act 2012](#), which set up strict rules requiring police to destroy DNA profiles of unconvicted individuals.

Looking at both legal systems side by side highlights a clear divide in how privacy is viewed. While the US sees DNA collection at arrest as an acceptable routine procedure, European legal standards view keeping genetic records of unconvicted people as an unnecessary violation of personal privacy and identity.

II. OVERVIEW

In the United States, privacy concerns regarding forensic DNA revolve around how far the state can go in collecting, storing, and searching an individual's genetic material. The core legal debate stems from the [Fourth Amendment](#), which protects citizens against unreasonable searches and seizures. As national and state DNA databases expanded—most notably through the FBI's

[Combined DNA Index System \(CODIS\)](#)—law enforcement moved beyond collecting DNA solely from convicted felons to collecting biological samples routinely [from individuals upon arrest](#).

Critics and legal scholars argue that treating genetic material like traditional fingerprints overlooks the vast amount of sensitive personal information contained within human DNA, including health markers, ancestral traits, and familial relationships. Additionally, concerns have grown over [surreptitious collection](#) (where police gather discarded items like coffee cups or cigarette butts without a warrant) and the reliance on third-party consumer databases.

Consequently, the primary privacy problem in the U.S. is where to draw constitutional boundaries when government investigative interests clash with an individual's expectation of genetic privacy.

III. HISTORY

According to the National Institute of Justice, DNA was first used [“as evidence in the United States criminal court System in 1986.”](#) Generally, it may be said that urban areas have historically integrated these technologies more quickly than rural areas. The often highly stratified structure of urban law enforcement allows for biological data to be gathered more efficiently because urban environments tend to have specialized centers dedicated to portions of the general population. On the other hand, research has shown that smaller police departments, which are often found in rural areas, tend to have higher clearance rates than urban departments but typically also [“spend less money per officer per resident.”](#) Rural police departments may also not use technologies such as

digital fingerprinting, which [could extended to DNA use as well](#).

This technology gap can limit the use of DNA as forensic evidence in rural environments. While urban environments can use more advanced technologies, such as [swabbing DNA from stones](#), rural settings may lack this option completely. In fact, analyzing DNA samples often involves [complex biological and laboratory processes](#) that may not fit into the budgets of rural regions. These techniques also require trained professionals, further increasing costs in rural regions where employees may not be readily available. These factors may have contributed and may continue to contribute to a discrepancy in DNA use for forensic evidence in rural and urban settings.

IV. POLICY PROBLEM

Throughout history, the United States has had no uniform standard governing how long the government may retain, or for what purposes it may search the genetic information of those who have not been convicted of a crime. Following the court case of [Maryland v. King\(2013\)](#), which upheld arrestee swabs by likening them to fingerprinting, DNA expansion has expanded to arrestees; however, abandoned samples such as discarded coffee cups remain largely unregulated, and genetic genealogy searches reach relatives that never consented.

Because a DNA sample can reveal health, ancestry, and family relationships, the real privacy risk lies less in the moment of collection than in what happens afterward: retention, re-analysis, and sharing. Across the world, Europe took a

different course in *S. and Marper v. United Kingdom*, where the [European Court of Human Rights](#) held that indefinite retention of unconvicted people's DNA violated Article 8, prompting the EU to implement the UK's Protection of Freedoms Act 2012.

This policy brief asks how US laws can regulate retention, secondary use, and cross-database searching of forensic DNA, especially for people never convicted, so DNA's crime-solving is preserved without making genetic surveillance a routine consequence of arrest or relatives' choices.

V. POLICY OPTIONS

Some proposed policy solutions in the United States include deletion of DNA evidence when a person has no qualifying offense or pending charges, specifically in the state of California under [California Penal Code 299](#). In addition to that, another way that the United States has dealt with this is that citizens who have been convicted can request that the FBI have their personal DNA evidence removed and deleted from the [Combined DNA Index System \(CODIS\)](#).

In other countries, such as the United Kingdom, the [Protection of Freedoms Act 2012](#) requires that all DNA samples be destroyed within 6 months after being sampled. This further ensures that personal DNA is not leaked and protects privacy.

VI. CONCLUSIONS

The rise of DNA evidence in the 1980s has helped bring criminals to justice, but with the rise of this new technology, many concerns have arisen, especially around privacy. Many have concerns about privacy, especially with regard to

their DNA being potentially leaked or mishandled. Many new policy solutions have tried to combat these issues by requiring the deletion of DNA evidence in order to prevent misuse.

VII. ACKNOWLEDGEMENT

The Institute for Youth in Policy wishes to acknowledge Cathy Jiang for editing this policy brief.

VIII. REFERENCES

- [1] "DNA Fingerprint Act of 2005 Expungement Policy." n.d. Federal Bureau of Investigation. Accessed October 3, 2026. <https://www.fbi.gov/how-we-can-help-you/dna-fingerprint-act-of-2005-expungement-policy>.
- [2] European Court of Human Rights. *S. and Marper v. United Kingdom*. Applications nos. 30562/04 and 30566/04. Judgment of December 4, 2008.
- [3] Federal Bureau of Investigation. "CODIS and NDIS Fact Sheet." Federal Bureau of Investigation, U.S. Department of Justice. Accessed October 1, 2026. <https://www.fbi.gov/how-we-can-help-you/dna-fingerprint-act-of-2005-expungement-policy>.
- [4] Great Britain. Protection of Freedoms Act 2012. c. 9. London: The Stationery Office, 2012.
- [5] Home Office. 2016. "Protection of Freedoms Act 2012: How DNA and Fingerprint Evidence Is Protected in Law." GOV.UK. October 20, 2016. <https://www.gov.uk/government/publications/protection-of-freedom-act-2012-dna-and-fingerprint-provisions/protection-of-freedom-act-2012-how-dna-and-fingerprint-evidence-is-protected-in-law>.
- [6] Lopez, Andryck. "People Sitting and Standing Inside Building with Numbers on Floor." Unsplash. August 11, 2019. https://unsplash.com/photos/people-sitting-and-standing-inside-building-with-numbers-on-floor-2f_2sGwchPI.
- [7] National Conference of State Legislatures. "DNA Collection After Arrest Laws." August 31, 2026. <https://www.ncsl.org/civil-and-criminal-justice/dna-collection-after-arrest-laws>.
- [8] National Institute of Justice. 2012. "DNA Evidence: Basics of Analyzing." National Institute of Justice, August 8. <https://nij.ojp.gov/topics/articles/dna-evidence-basics-analyzing>.
- [9] National Institute of Justice. 2023. "What Every First Responding Officer Should Know About DNA Evidence." National Institute of Justice, June 5.

<https://nij.ojp.gov/nij-hosted-online-training-courses/what-every-first-responding-officer-should-know-about-dna/dna-evidence-overview>.

- [10] Sorg, Aileen. 2023. "Human Background DNA on Stones in an Urban Environment." Forensic Science International. Genetics 65: 102880. <https://doi.org/10.1016/j.fsigen.2023.102880>.
- [11] Supreme Court of the United States. Maryland v. King, 569 U.S. 435 (2013). Justia Law.
- [12] U.S. Constitution. amend. IV. <https://constitution.congress.gov/constitution/amendment-4/>.
- [13] United Data Connect. "Fourth Amendment DNA Cases." Accessed October 1, 2026. <https://www.uniteddataconnect.com/fourth-amendment-dna-cases>.
- [14] Weisner, L., H. D. Otto, and S. Adams. n.d. Issues in Policing Rural Areas: A Review of the Literature. Illinois Criminal Justice Information Authority.