



1212 New York Ave. NW,
Suite 900
Washington, DC 20005
202.525.5717

Free Markets. Real Solutions.
www.rstreet.org

Testimony from:

Jesse Kelley, Government Affairs Manager, Criminal Justice & Civil Liberties, R Street Institute

Regarding HOUSE BILL 1209, “AN ACT AN ACT concerning Public Safety – DNA Collection, Records, Analysis, and Reporting.”

March 3, 2020

House Judiciary Committee

Chairman and members of the committee,

My name is Jesse Kelley and I am the government affairs manager for Criminal Justice at the R Street Institute. R Street is a nonprofit public policy research organization with a Criminal Justice and Civil Liberties team that focuses on evaluating policies related to the criminal justice and juvenile justice systems. HB 1209 is therefore of special interest to us.

Emerging technology and science impact the criminal justice system every day, and sometimes those shifts can affect the due process and privacy rights of individuals. This piece of legislation will ensure that required protections are not circumvented.

Due process is critically important for all Americans, not only those who have been accused of a crime. This constitutional protection ensures that basic rights apply in all federal and state government proceedings that could result in a person’s deprivation of freedom. By passing HB 1209 and limiting the overreach of government gathering and distribution of private DNA information, we can strengthen the criminal justice process.

The Supreme Court has established that individuals have a constitutional right to privacy, even though such a right is not explicitly enumerated within the text of the Constitution.¹ This bill would help to protect the privacy rights of millions of Americans who have uploaded their genetic data to sites with the expectation of finding long-lost relatives. It will also protect the millions of Americans who *have not* uploaded their DNA or consented to have their genes exposed, but were exposed anyway because genes link everyone in a given family. Finally, there’s another piece to the privacy puzzle: a suspect’s right to privacy. Indeed, suspects in these scenarios have no idea that law enforcement is uploading their DNA to a public website.

¹ *Griswold v. Connecticut*, 381 U.S. 479 (1965).

Exactly what tests law enforcement uses in preparation for uploading a DNA profile to a public website, and exactly which points are used in the testing process, have not been publicly disclosed.² Law enforcement may collect DNA from a crime scene that officers believe belongs to a suspect but in reality belongs to someone else. This could lead officers to upload an innocent person's DNA to a public database, thus compromising that individual's identity without their consent. And even if the state tries to delete the open-source database file after discovering the mistake, there is no guarantee that a citizen sleuth, a hacker or an insurance company hasn't already copied the DNA data file for their own gain.

DNA testing done by law enforcement can potentially reveal sensitive medical information when a DNA profile is uploaded to an open-source database. Due to a lack of law enforcement transparency in this respect, the extent of the information revealed by that test may be difficult for the public to determine.

Anyone can upload genetic information—even if it's not their own—to open-source sites. Officers can create a user profile for a crime suspect, upload the suspect's DNA and find a match all without a court order of any kind.

When mistakes are made with DNA, the cost is higher than ever. Unlike other pieces of information that have been improperly released—such as credit card numbers—biometric information like DNA cannot be changed. And even if the government does submit the correct person's file, uploading a suspect's DNA to an open database has significant repercussions and could affect a person's ability to get a job or insurance, as both employers and insurance companies might discriminate against those with genetically determined risks.

Sincerely,

Jesse Kelley, Esq.

Government Affairs Manager
Criminal Justice & Civil Liberties
R Street Institute
jkelly@rstreet.org

² Christine Guest, "DNA and Law Enforcement: How the Use of Open Source DNA Databases Violates Privacy Rights," 68 Am. U. L. Rev. 1015 (2019).