Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Advances in DNA Analysis: Fourth Amendment Implications

July 11, 2025

Law enforcement has used deoxyribonucleic acid, or DNA, as an investigative tool for decades. DNA is "the fundamental building block for an individual's entire genetic makeup" and may be "extracted from many sources, such as hair, bone, teeth, saliva, and blood." Investigators routinely compare DNA from known suspects with DNA recovered from crime scenes or victims, or look for matches between crime scene DNA and law enforcement databases of offender DNA profiles. Federal courts, including the Supreme Court, have generally upheld statutory DNA identification regimes against Fourth Amendment challenges.

This Sidebar provides legal background on DNA identification and the Fourth Amendment, with particular emphasis on the 2013 Supreme Court case *Maryland v. King*. It then examines selected Fourth Amendment issues, including lingering questions from *King* that could potentially be relevant to a newer DNA investigative technique, which the Department of Justice (DOJ) has called *forensic genetic genealogical DNA analysis and searching* (sometimes described as *investigative genetic genealogy* or *forensic genetic genealogy*). The Sidebar concludes with congressional considerations.

Maryland v. King: the Fourth Amendment and DNA Identification

The Fourth Amendment imposes limits on searches and seizures by the government. Courts have determined that a Fourth Amendment search occurs if "the Government obtains information by physically intruding on a constitutionally protected area" or "when the government violates a subjective expectation of privacy that society recognizes as reasonable." If a law enforcement activity qualifies as a search or seizure, then the Fourth Amendment requires that it must be reasonable, which ordinarily means that the search or seizure must be conducted pursuant to a warrant supported by probable cause, with some exceptions.

Congressional Research Service
https://crsreports.congress.gov
LSB11339

Combined DNA Index System (CODIS)

A prominent use of DNA by law enforcement is comparing biological material believed to be "deposited by a putative perpetrator" and "collected from a crime scene, a person, an item, or a location connected to the criminal event" (described by DOJ as a *forensic sample*) with "biological material from a known source" (termed a *reference sample* by DOJ).

This comparison can entail searching the Combined DNA Index System (CODIS), software created and distributed by the FBI that connects "DNA-profile databases maintained by local, state, and federal law enforcement authorities." In general, these law enforcement databases contain DNA profiles generated from "arrestees, convicted offenders, and forensic evidence found at crime scenes." In 1994, Congress authorized the creation of a national DNA database, which ultimately resulted in the National DNA Index System (NDIS), which CODIS is used to search (NDIS and CODIS are sometimes described interchangeably). Federal statute controls the types of DNA samples that may be included in NDIS and therefore be subject to a national search, although state laws govern the exact situations in which DNA records are included in the underlying state databases.

The Supreme Court has said that "[o]ne of the most significant aspects of CODIS is the standardization of the points of comparison in DNA analysis." Namely, DNA profiles entered into CODIS are created using STR DNA markers—noncoding DNA that "are not associated with human attributes such as height, eye or skin color, or susceptibility to a particular disease." According to DOJ, if "a CODIS search results in a confirmed match between a forensic profile and a known offender, a law enforcement lead is generated and the name of the matching offender is released. If the search does not result in a confirmed match, no lead is generated." Technical and policy discussion of CODIS may be found in CRS Report R41800, *The Use of DNA by the Criminal Justice System and the Federal Role: Background, Current Law, and Grants*, by Nathan James (2022).

In the 2013 case *Maryland v. King*, the Supreme Court examined the extent to which the Fourth Amendment limits law enforcement's collection and analysis of arrestee DNA. In *King*, police arrested the defendant for a 2009 assault and collected his DNA with a cheek swab as part of a routine booking procedure authorized under Maryland state law. Investigators uploaded the defendant's DNA record to a state database, which "was matched to [a] DNA sample collected in [an] unsolved 2003 rape case." In the resulting rape trial, the defendant sought to keep the DNA match from being used as evidence "on the grounds that Maryland's DNA collection law violated the Fourth Amendment."

The Supreme Court disagreed. The Court acknowledged that the Fourth Amendment usually encompasses government "'intrusio[n] into the human body,'" and it concluded that "using a buccal swab on the inner tissues of a person's cheek in order to obtain DNA samples is a search." Nevertheless, the Court held that "taking and analyzing a cheek swab of the arrestee's DNA" is analogous to routine booking procedures used for identification, such as fingerprinting or "matching an arrestee's face to a wanted poster of a previously unidentified suspect."

Thus, swabbing an arrestee for DNA is considered reasonable under the Fourth Amendment, although the Court limited its holding to "an arrest supported by probable cause to hold [a suspect] for a serious offense[.]" In reaching that conclusion, the Court weighed what it described as the "significant state interests in identifying" arrestees and in making "informed decisions concerning pretrial custody" against the "minor intrusion of a brief swab of [an arrestee's] cheeks."

The Fourth Amendment and Forensic Genetic Genealogical DNA Analysis and Searching (FGGS)

Forensic genetic genealogical DNA analysis and searching (FGGS) involves "DNA analysis combined with traditional genealogy research to generate investigative leads for unsolved violent crimes." FGGS garnered national attention in 2018, when law enforcement used a version of it to identify a suspect in a series of unsolved crimes attributed to the person commonly referred to as the Golden State Killer. According to one observer, "[t]he break in the case came when investigators compared DNA recovered from victims and crime scenes to other DNA profiles searchable in a free genealogical database called

GEDmatch," which "turned up a distant cousin of the Golden State Killer's, and through sleuthing in that family tree, investigators eventually homed in on [the suspect]." The suspect ultimately pled guilty.

DOJ has issued an interim FGGS policy, which allows investigative agency use of FGGS on DNA samples of "putative perpetrators" only for unsolved homicides or sex crimes, or for other violent crimes if they "present a substantial and ongoing threat to public safety or national security." The Interim FGGS Policy also allows use of FGGS by an investigative agency to identify human remains "of a suspected homicide victim." A prerequisite for FGGS under the policy is that law enforcement has exhausted reasonable investigative leads, including searching CODIS.

It appears that the interim FGGS policy is still in effect at the time of publication, as it has not been replaced and the press release announcing it was recently updated. The interim FGGS policy is potentially applicable beyond the federal government since it defines an investigative agency as "any federal, state, local, or tribal law enforcement agency that receives funding from the Department of Justice" for FGGS.

DOJ has said that FGGS diverges from CODIS-facilitated DNA identification in two key ways. First, FGGS involves the examination by outside "vendor laboratories" of "more than half a million single nucleotide polymorphisms ('SNPs')," which "span the entirety of the human genome." As one jurist explained, these "SNP profiles contain several hundred thousand informationally rich segments of DNA, which can be decoded to predict distant genealogical relationships, disease carrier status, and aspects of physical appearance." SNP profiles have therefore been described as more revealing than the type of DNA profiles ordinarily used for identification through CODIS.

Second, FGGS involves searching a different set of databases. FGGS relies not on CODIS and underlying law enforcement databases, but instead involves entering an SNP profile "into one or more publicly-available open-data personal genomics DNA databases or direct-to-consumer genetic genealogy services" (hereinafter *consumer DNA/genealogy services*). That profile is then "compared by automation against the genetic profiles of individuals who have voluntarily submitted their biological samples or entered their genetic profiles into [consumer DNA/genealogy services]" and a "computer algorithm is used to evaluate potential familial relationships between the (forensic or reference) sample donor and service users."

These two distinctions identified by DOJ might be relevant to Fourth Amendment analysis. A small pool of cases has examined the constitutionality of FGGS under the Fourth Amendment.

SNP Profiles and Reasonable Expectations of Privacy

As discussed above, "the touchstone of Fourth Amendment analysis is whether a person has a 'constitutionally protected reasonable expectation of privacy.'" If there is a reasonable expectation of privacy in SNP profiles, then FGGS may involve a search that would trigger the protections of the Fourth Amendment (requiring that the search in turn be reasonable). *King* leaves open at least three questions that could be relevant to determining whether a person has a reasonable expectation of privacy in an SNP profile.

One question is the extent to which the creation of an SNP profile could itself be a Fourth Amendment search separate from DNA collection. At least one observer has described DNA analysis as a "separate Fourth Amendment event" from DNA collection, and prior to *King*, several federal courts had reached similar conclusions. For example, in a 2011 case, the Third Circuit said that "physical collection of the DNA sample" can be a search, as can "the processing of the DNA sample and creation of the DNA profile for CODIS." *King* potentially leaves ambiguity on this point, however. The *King* Court briefly considered DNA analysis as separate from collection, rejecting the argument that DNA processing in the CODIS context unconstitutionally intruded on the defendant's reasonable expectation of privacy. At least one federal district court has interpreted *King* to "not separate out the two steps in DNA identification." In other words, according to that district court, *King*'s holding that "DNA identification of arrestees is a

reasonable search" treats "the taking and analyzing as part of a single 'identification' process, rather than two independent searches." One observer has said that *King* could be read to either say DNA analysis is not a search, or that it is a search but not an unreasonable one, at least where it reveals only certain types of information.

A second question then is whether the more revealing nature of SNP profiles changes the Fourth Amendment analysis undertaken in *King*. Part of *King's* holding rested on its assessment that the DNA profile at issue—which conformed to CODIS standards—came from "parts of the DNA that do not reveal the genetic traits of the arrestee." The Court in *King* noted that "science can always progress further, and those progressions may have Fourth Amendment consequences." Some observers and jurists have suggested that SNP profiles represent exactly the type of scientific progression alluded to in *King*, since SNP profiles are more revealing than the junk DNA used in *King*.

The possibility that SNP profiles would be subject to a reasonable expectation of privacy was litigated, but ultimately not decided, in *State v. Carbo*. There, the Supreme Court of Minnesota examined whether law enforcement violated a defendant's Fourth Amendment rights by using FGGS. Although law enforcement did not obtain a warrant, the *Carbo* court concluded that the defendant had no subjective expectation of privacy in the underlying DNA, because he had "abandoned" it at the scene. Therefore, according to the court, "a Fourth Amendment search did not occur when the police had [the private company] perform a genetic analysis of the biological material [the defendant] left behind at the crime scene."

The *Carbo* court did not reach the issue of whether "the deeply personal and revealing information contained in a genetic profile falls within an expectation of privacy that society is willing to recognize as reasonable." Two justices wrote separately, however, to express their view that "the novel DNA analysis at issue in this case reveals deeply sensitive and personal information" in which a defendant has a "reasonable expectation of privacy" under the U.S. Constitution (and Minnesota state law). They focused in part on the distinctions between the CODIS-type of DNA profiles at issue in *King* and the more revealing SNP profiles typically used in FGGS.

The source of DNA used in FGGS raises a third question about the extent of reasonable expectations of privacy for SNP profiles. *King* rested in part on the fact that the DNA came from an arrestee with reduced expectations of privacy compared to those of a "free person." In contrast, the forensic samples of DNA used for FGGS generally come not from arrestees but instead from unidentified human remains or from "biological material reasonably believed by investigators to have been deposited by a putative perpetrator . . . collected from a crime scene, a person, an item, or a location connected to the criminal event." As stated above, the Supreme Court of Minnesota in *Carbo* rejected the idea that there would be a subjective expectation of privacy in DNA "abandoned" at a crime scene. At least one federal district court and one federal circuit court judge have expressed similar views.

The concept of abandonment of DNA is the subject of scholarly discourse. Ultimately the extent to which the *collection* of a particular DNA sample for FGGS implicates the Fourth Amendment will likely be a fact-specific inquiry, potentially influenced by considerations such as the status and characteristics of the source or location from which the sample was obtained.

Consumer DNA and Genealogy Services and Reasonable Expectations of Privacy

As described above, development of an SNP profile is only one aspect of FGGS. The process also involves entering the SNP profile into consumer DNA/genealogy services and searching for familial matches. For example, in one case "after receiving the SNP profile, police arranged for it to be uploaded to several commercial genealogical websites, including GEDmatch, Ancestry.com, and MyHeritage."

So far, courts have had seemingly few opportunities to examine whether law enforcement access to consumer DNA/genealogy services could itself be a search implicating the Fourth Amendment. In large part, this may be due to the DOJ interim FGGS policy, which states that "[i]nvestigative agencies shall identify themselves as law enforcement to [consumer DNA/genealogy services] and enter and search" profiles only in services "that provide explicit notice to their service users and the public that law enforcement may use their service sites . . . to investigate crimes or to identify unidentified human remains." Changes to the interim policy could spur Fourth Amendment litigation, especially given that some consumer DNA/genealogy websites have reportedly said they would resist requests for data from law enforcement absent a warrant or other valid legal process.

There has been at least one case, *State v. Hartman*, where a defendant challenged law enforcement access to consumer DNA/genealogy services, arguing that "a warrant is required to analyze . . . public profiles by comparing them with DNA left behind by an unidentified killer." A Washington appellate court disagreed, doubting there would be "a privacy interest in the segments of [a defendant's] DNA that his relatives had in common with him." Although it is only an initial data point, *Hartman* suggests a number of Fourth Amendment questions that could be raised by law enforcement access to consumer DNA/genealogy services. Resolution of these questions in future cases could ultimately depend not only on the nature of the law enforcement access, but also on whether the challenge is brought by the defendant, a relative, or the consumer DNA/genealogy service.

One question involves the applicability of the third-party doctrine, which directs that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." In similar reasoning, the *Hartman* court observed that consumers often upload DNA for the purpose of sharing it with strangers and lose control of it once they do so. A related question involves the applicability of *Carpenter v. United States*, a Supreme Court case recognizing a "narrow" limit to the third-party doctrine for certain types of sustained technological surveillance. (The *Hartman* court rejected the applicability of *Carpenter* to consumer DNA/genealogical records.)

Another question might be whether the terms of service of consumer DNA/genealogy services influence the Fourth Amendment analysis of FGGS. In passing, the *Hartman* court observed that when the defendant's relatives uploaded their DNA information, GEDmatch had "terms of service expressly stat[ing] that it would let law enforcement use its service to identify perpetrators." The company now has an opt-in process, and other companies have terms of service limiting law enforcement access. One Fourth Amendment scholar has argued that terms of service are generally irrelevant to Fourth Amendment rights, writing that "[a]greements cannot create Fourth Amendment rights" or "take them away."

Congressional Considerations

Congress and states have legislated on various DNA issues for decades, and FGGS has generated legislative interest at the state and federal levels. For example, in the 119th Congress, the Carla Walker Act (H.R. 3591; S. 1890) would, among other things, authorize grants administered by DOJ "for the purpose of purchasing equipment to deploy [FGGS] to generate investigative leads for criminal investigations or unidentified human remains."

Congress could also limit the use of FGGS by codifying the interim FGGS policy or enacting other restrictions on federal law enforcement. It could also seek to influence state and local use of FGGS through conditioning grant funds (an approach reflected in the interim FGGS policy). At least one state has independently taken steps that could limit FGGS within its border: Minnesota enacted a law that requires genetics companies to obtain consent from consumers for "the collection and testing of their genetic information" and prohibits those "companies from disclosing genetic information to law enforcement without first obtaining express written consent, a search warrant, or a court order."

There may be data privacy policy considerations for FGGS collection and use of consumer DNA information beyond the criminal law focus of this Sidebar. Some Members raised privacy considerations in this space following the March 2025 bankruptcy filing of the consumer DNA-testing company 23andMe. 23andMe has reportedly required law enforcement to obtain a search warrant or other valid legal process to access its data. The company has said that it aims to find "a partner who shares our commitment to customer data privacy," and the sale of the company is currently the subject of litigation. In testimony for a June 10, 2025, hearing of the House Committee on Oversight and Government Reform on the pending sale of 23andMe, one witness said that the extent to which the company's previous privacy promises are "reneged" is "now in the hands of bankruptcy law." At least one bill in the 119th Congress seeks to address the extent to which genetic information may be transferred during bankruptcy.

FGGS is in its nascency and caselaw examining the technique remains scarce. Congress could also choose to defer to courts to resolve any Fourth Amendment issues should arguments like those raised in *Carbo* or *Hartman* proliferate.

Author Information

Peter G. Berris
Legislative Attorney

Disclaimer