

Memorandum

To: Scott Thorpe
Special Assistant Attorney General

Date: March 8, 2007

Telephone: CALNET (8)593-5892
(415) 703-5892

FACSIMILE: (415) 703-1234
E-Mail: michael.chamberlain@doj.ca.gov

From: Michael Chamberlain
Deputy Attorney General
DNA Legal Unit
Office of the Attorney General - San Francisco

Subject: Inquiry by Commission on Fair Administration of Justice - Access to DOJ Laboratories and DNA Data Bank Program

I. "ACCESS TO [DOJ] LABS FOR TESTING"

The Commission first inquires about Department of Justice ("DOJ") policy concerning the ability of criminal defendants to employ DOJ's DNA laboratories to conduct testing. While DOJ can conduct DNA testing that is requested by criminal defendants (Pen. Code, § 11050.5(b)) – ordinarily by way of a court order or passed along via the prosecution – this situation rarely arises for several reasons.

First, public funds are available for indigent defendants to spend on DNA testing by a private laboratory. (See, e.g., Pen. Code, § 987.9(a).) There is no indication, anecdotally or in case law, that indigent defendants in California have ever been denied the funds for scientific testing where the results would be probative of issues being litigated.

Second, there are a number of accredited and unaccredited private laboratories in California that regularly conduct defense DNA testing, the results of which are potentially admissible in court. Prominent private DNA laboratories include Forensic Analytical Specialties ("FASI"), Serological Research Institute ("SERI"), and Forensic Science Associates.

Third, criminal defendants ordinarily prefer that DNA testing done on their behalf be preformed by a non-law enforcement laboratory.

Fourth, criminal defendants ordinarily prefer that private labs conduct their DNA testing so that the results will not automatically be available to the prosecution and investigating law enforcement agency.

/////

/////

/////

II. ACCESS TO CALIFORNIA'S DNA DATABASE

The Commission next inquires about Department of Justice ("DOJ") policy concerning defense access to the State's offender DNA Database. California's DNA Data Bank Program was created, and continues to exist, as a law enforcement investigatory tool designed to match offender reference samples to DNA samples left at crime scenes by perpetrators. The limited scope of this function is set forth in comprehensive and controlling statutory authority, both state and federal. The Data Bank Program's limited parameters are also a significant factor in the ongoing constitutionality of the warrantless, suspicionless seizures of DNA samples from qualifying offenders mandated by DNA database legislation. The limited function and parameters of the Data Bank Program generally preclude use of the Database as an instrument for criminal defense investigation and discovery.

The following discussion of the law and policy defining the boundaries of the Data Bank Program applies with equal weight to questions concerning access to California's DNA Database by all varieties of defense counsel – including trial counsel, appellate counsel, habeas counsel, and Innocence Project counsel.

The Commission inquires specifically into DOJ's position regarding "access" to the State's DNA Database. As a threshold matter, "access" could mean any of the following:

- (1) The ability to submit DNA profiles developed by private laboratories, or of other non-law enforcement origin, directly to DOJ for upload and searching as forensic unknowns;
- (2) The ability to compel DOJ to upload and search crime scene DNA profiles developed by law enforcement that do not otherwise qualify as forensic unknowns;
- (3) The ability to compel DOJ to provide the DNA profiles for Database offenders other than the defendant in the hopes of identifying an alternative or third party perpetrator;
- (4) The ability to actually conduct searches using CODIS software;
- (5) The ability to acquire a copy of the entire state DNA database for research purposes or other use.

Fortunately, the same set of legal principles and policy considerations apply to each of the possible situations listed above and will be discussed as a whole.

//////

//////

//////

A. General Legal and Policy Considerations

California's DNA Data Bank Program is statutorily designated as an investigatory tool available exclusively to law enforcement. Penal Code Section 295(c) provides that "[t]he purpose of the DNA and Forensic Identification Database and Data Bank Program is to assist federal, state, and local criminal justice and law enforcement agencies within and outside California in the expeditious and accurate detection and prosecution of individuals responsible for sex offenses and other crimes [and] the exclusion of suspects who are being investigated for these crimes" (See also § 295(b)(3) [referring to the DNA Data Bank Program as a "law enforcement tool"].)

As this language makes clear, the overarching purpose of the Data Bank Program is to link one offender to one unknown perpetrator's DNA sample left at a crime scene. In doing so, all other offenders in the Database avoid needless interaction with, and attention from, investigators and other law enforcement representatives. (See, e.g., *People v. King* (2000) 82 Cal.App.4th 1363, 1375-1376 ["The ability to match DNA profiles derived from crime scene evidence to DNA profiles in an existing data bank can enable law enforcement personnel to solve crimes expeditiously and prevent needless interference with the privacy interests of innocent persons."] Therefore, the Database is designed to narrow a field of suspects, not broaden it. Various other components of state law emphasize that narrow and limited access to the Database is necessary to ensure its narrow and limited law enforcement function.

B. Statutory Confidentiality Requirements

In particular, Penal Code section 299.5 sets forth comprehensive nondisclosure restrictions preventing the dissemination of DNA profiles or other information maintained in the Database. For example, section 299.5(a) states that "[a]ll DNA and forensic identification profiles and other identification information retained by the Department of Justice pursuant to this chapter are exempt from any law requiring disclosure of information to the public and shall be confidential except as otherwise provided in this chapter." Likewise, section 299.5(f) mandates that "DNA samples and DNA profiles and other forensic identification information shall be released only to law enforcement agencies" (See also § 299.5(g) & (h) [forbidding disclosure of DNA Database information other than the defendant's own DNA profile and associated information to defense counsel and defendants in criminal proceedings].)

By forbidding disclosure of DNA Database profiles, section 299.5(h) creates an absolute privilege of confidentiality for that official information within the meaning of Evidence Code Section 1040(b)(1).¹ (*Shepherd v. Superior Court* (1976) 17 Cal.3d 107, 123 [Section

¹ "A public entity has a privilege to refuse to disclose official information, and to prevent another from disclosing official information, if the privilege is claimed by a person authorized by the public entity to do so and: (1) Disclosure is forbidden by an act of the Congress of the United States or a statute of this state . . ." (Evid. Code, § 1040, subd. (b).)

1040(b)(1) confers upon its holder “an absolute privilege if disclosure is forbidden by a federal or state statute.”], overruled in part on other grounds by *People v. Holloway* (2004) 33 Cal.4th 96, 131; *Department of Motor Vehicles v. Superior Court* (2002) 100 Cal.App.4th 363, 375 [“A statute that ‘prohibits the disclosure of records’ would invoke the absolute privilege of Evidence Code sections 1040 and 1041.”]; *Marylander v. Superior Court* (2000) 81 Cal.App.4th 1119, 1126, fn. 1; *Rubin v. Superior Court* (1987) 190 Cal.App.3d 560, 584.)

Moreover, severe criminal and civil sanctions potentially result from failure to comply with statutory confidentiality restrictions. (Pen. Code, § 299.5(i).) It is the responsibility of the Attorney General to maintain the security of all criminal offender record information maintained by DOJ. (Pen. Code, § 295(g) [The Department of Justice . . . shall be responsible for the management and administration of the state’s DNA . . . Data Bank Program”]; § 11077 [“The Attorney General is responsible for the security of criminal offender record information”]; § 11075(a) [“‘[C]riminal offender record information’ means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders”].)

Because California uploads the contents of its offender DNA database into the National DNA Index System (“NDIS”), the State is subject to strict federal disclosure restrictions as well. Federal law provides as follows:

- The [National DNA Index System] shall include only information on DNA identification records and DNA analyses that are . . .
- (3) maintained by Federal, State, and local criminal justice agencies . . . pursuant to rules that allow disclosure of stored DNA samples and DNA analyses only--
- (A) to criminal justice agencies for law enforcement identification purposes;
 - (B) in judicial proceedings, if otherwise admissible pursuant to applicable statutes or rules;
 - (C) for criminal defense purposes, to a defendant, who shall have access to samples and analyses performed in connection with the case in which such defendant is charged; or
 - (D) if personally identifiable information is removed, for a population statistics database, for identification research and protocol development purposes, or for quality control purposes.

42 U.S.C. § 14132(b).) As subdivision (3)(C) makes clear, the *only* database records that may be provided to a criminal defendant “for criminal defense purposes” are those relating to the DNA analysis done in conjunction with that particular case. (See also Privacy Act of 1974; New System of Records, 61 Fed. Reg. 37496 (July 18, 1996).)

Federal law thus parallels California law with great precision. (See Pen. Code, § 299.5(g) [only a defendant’s DNA profile and associated information is available as discovery].) And, as section 14132 and its interpreting regulations demonstrate, only state

DNA information that is protected according to the confidentiality standards set forth is eligible for inclusion in the National DNA Index System.

The potential sanctions for violating these federal mandates are severe. They include expulsion from the national CODIS network: “*Access to the index established by this section is subject to cancellation if the quality control and privacy requirements described in subsection (b) [of Section 14132] are not met.*” (42 U.S.C. § 14132(c), italics added; see also Privacy Act of 1974; New System of Records, 61 Fed. Reg. 37497 (July 18, 1996) [“[C]riminal justice agencies with direct access to NDIS must agree to adhere to national quality assurance standards for DNA testing, undergo semi-annual external proficiency testing, and restrict access to DNA samples and data. The NDIS will not accept DNA analyses from those agencies and/or DNA personnel who fail to comply with these standards and restrictions; and the NDIS Custodian is authorized to restrict access to and delete any DNA records previously entered into the system.” (Italics added.)].)

Therefore, the continuing ability of California to submit offender and forensic DNA profiles to the National DNA Index System for searches against other states’ data depends in part upon California’s strict observation of the federal confidentiality standards articulated above.

C. Constitutionality of the DNA Data Bank Program

The restricted access to the DNA profile and identification information contained in the database, as set forth in Penal Code Section 299.5 and applicable federal law, is a factor in assessing the Program’s constitutionality. The Fourth Amendment permits DOJ to store and utilize DNA information for law enforcement purposes because that use and access to the information is so tightly restricted. For example, in applying the Fourth Amendment balancing test to determine the constitutionality of warrantless, suspicionless seizures of DNA samples pursuant to California’s DNA Database Act, the court in *Alfaro v. Terhune* (2002) 98 Cal.App.4th 492, emphasized that the “Act exempts all DNA and forensic identification profiles and other identification information from any law requiring disclosure of information to the public, and it makes such information confidential. (§ 299.5, subds. (a), (b).) *These provisions are relevant in determining the extent of an intrusion upon privacy interests and in balancing the intrusion against the public interests to be served.*” (98 Cal.App.4th at p. 508, and fn. 6, emphasis added; see also *People v. King* (2000) 82 Cal.App.4th 1363, 1377 and 1375 [recognizing data bank’s use limitations as part of the constitutional balancing analysis; *United States v. Kincade* (9th Cir. 2004) 379 F.3d 813, 837, and fn. 33 [observing that statutory confidentiality protections counter defense claim that “soon, if not already, scientists will request access to what would serve as [a] preexisting goldmine of DNA data for their research.”].)

Accordingly, the strict confidentiality provisions that define the State’s DNA Database Act are not surplusage. Rather, they were carefully crafted by the Legislature in order to ensure the legality and constitutionality of this important public safety program. If not strictly

observed and enforced, a wholesale loss of DOJ control over highly sensitive information could result. One could imagine, for example, a public Internet site containing more than 800,000 offender DNA profiles that DOJ had been forced to reveal in the context of a criminal proceeding. Even stripped of offender names and other identifying information, those DNA profiles could be put to unscrupulous use, such as comparison by potential employers against DNA profiles surreptitiously collected from job applicants.

D. No Compelling Rationale Exists For Criminal Defense Access To CODIS

Where defense counsel – whether pre-trial or postconviction – believes that a crime scene DNA profile that has not been uploaded and searched in CODIS should be uploaded and searched in CODIS, there is no legal bar to the investigating law enforcement taking such action in appropriate cases. Conceptually, however, this situation will arise rarely because law enforcement should always utilize the DNA Database in appropriate cases. Thus, defense counsel's interest is coextensive with law enforcement's interest, making defense "access" to the DNA Database a moot point. The key issue is what constitutes "appropriate cases."

Several criteria must be met before a crime scene DNA profile may be submitted to the State's DNA Database for searching. Application of these prerequisites may preclude the submission of an uploadable DNA profile identified by defense counsel, and always precludes direct access to CODIS by a non-law enforcement crime laboratory. These criteria include the following:

(1) The profile to be uploaded contains a minimum number of identifiable alleles. At present, Cal-DNA regulations require a minimum of seven searchable loci (excluding amelogenin) for inclusion in the Database.

(2) The profile must have been developed by a laboratory that meets the statutory accreditation standards set forth in Penal Code section 297. In addition, if the profile was developed by a private laboratory, a properly accredited and inspected law enforcement crime laboratory must conduct a quality control review of the technical work prior to upload. (Pen. Code, § 297(b).) Finally, only DOJ is statutorily authorized to upload offender reference samples into the Database (§ 297(a)(3)), and only "public law enforcement crime laboratories" may upload forensic unknown samples into the Database (§ 297(b)).

(3) The profile must be attributable to the (or a) putative perpetrator of the crime. A profile that could just as easily be attributable to a non-perpetrator may not be searched. Thus, there would be no need for criminal defendants and their representatives to submit DNA profiles for upload into the State's DNA Database because those that qualify would have been uploaded already by law enforcement, or will be uploaded by law enforcement, given law enforcement's goal of identifying the perpetrator.

For example, a DNA sample obtained from a cigarette butt located near a public park homicide scene cannot be uploaded into the DNA Database absent evidence that it was smoked

by the killer. It could just as easily have been left at another time by a person unrelated to the crime. If that innocent person happens to be an offender in the State's DNA Database, however, he will by definition become a suspect, or at least receive undue police scrutiny, were the crime scene profile uploaded. Neither classification would be merited and would conflict with the Data Bank Program's purpose of identifying one offender as the perpetrator of a particular crime. As the California Court of Appeal observed,

The government also has an interest in ensuring that innocent persons are not needlessly investigated--to say nothing of convicted--of crimes they did not commit. DNA testing unquestionably furthers these interests. The ability to match DNA profiles derived from crime scene evidence to DNA profiles in an existing data bank can enable law enforcement personnel to solve crimes expeditiously and prevent needless interference with the privacy interests of innocent persons.

(*People v. Travis* (2006) 139 Cal.App.4th 1271, 1285; see also *Rise v. Oregon* (9th Cir. 1995) 59 F.3d 1556, 1561 ["The creation of a DNA data bank also advances the overwhelming public interest in prosecuting crimes *accurately* - DNA evidence can exculpate an accused just as effectively as it can inculcate him."].) Uploading DNA samples not identifiable as left by the perpetrator defeats the twin goals of accurate prosecution and exoneration of non-matching offenders, which, as discussed in *Travis* and *Rise, supra*, are factors contributing to the constitutionality of DNA database programs generally.

Similarly, if an evidence item that may contain the perpetrator's DNA is also likely to contain the DNA of non-perpetrators, then the value of uploading any DNA profile from that object may be minimal or nonexistent. This is because a match in the Database will not necessarily identify the perpetrator, and the function of the Database is to identify perpetrators -- not to identify all persons who may have handled physical evidence at some point in time or may have been present at the crime scene at some point in time. Using the Data Bank Program to develop a list of names that may or may not be associated with the crime in some capacity would represent a fundamental and unjustified broadening of the Program's limited function, and implicate privacy interests of offenders who are in the Database but did not commit the particular crime in question.

Finally, a DNA profile uploaded into CODIS as a forensic unknown must be of verifiable origin. In other words, a clear chain of custody must exist originating with the crime scene. Were this not so, the evidentiary value of the sample would be negligible. In most cases, this precludes the uploading of any "crime scene profile" not collected by the investigating law enforcement agency.

//////

//////

E. There Is No Compelling Need For Defense Access To The DNA Database In Order To Search For Alternative Perpetrators

If a criminal defendant seeks to compare a third party's DNA profile to a DNA profile left at the crime scene, there is no need to compromise California's statutory confidentiality provisions and employ the DNA Database for that purpose. Instead, it is well-established that a trial court may order that a biological sample be collected from a third party at the defendant's request upon a showing of "probable cause" to believe the intrusion will uncover material evidence [The trial court] must then weigh 'the degree of intrusion against the likelihood and importance of recovering the evidence.'" (*People v. Earp* (1999) 20 Cal.4th 826, 882, quoting *People v. Melton* (1988) 44 Cal.3d 713, 738.) The *Earp* court further noted that the existence of probable cause is evaluated "by considering the totality of circumstances." (*Id* at p. 883; see also *People v. Browning* (1980) 108 Cal.App.3d 117, 124-125 [trial court may issue warrant subjecting person other than defendant to bodily intrusion].) In fact, one appellate court opined that there is "no valid reason why courts . . . may not require of any person within their jurisdiction the furnishing of a few drops of blood for test purposes when, in the opinion of the court, so to do will or may materially assist in administering justice in a pending matter." (*People v. Bynon* (1956) 146 Cal.App.2d 7, 12.)

A defendant's burden of demonstrating probable cause is far from onerous. Probable cause is a "particularized suspicion." (*Texas v. Brown* (1983) 460 U.S. 730, 742.) It is "facts that would lead a man of ordinary caution . . . to entertain . . . a strong suspicion that the object of the search is in the particular place to be searched." (*Wimberly v. Superior Court* (1976) 16 Cal.3d 557, 564.) "[P]robable cause requires only a . . . substantial chance." (*Illinois v. Gates* (1983) 462 U.S. 213, 243, fn. 13.) In sum, probable cause "is less than proof beyond a reasonable doubt . . . ; less than a preponderance of the evidence . . . ; and less than a prima facie showing . . ." (*People v. Tuadles* (1992) 7 Cal. App. 4th 1777, 1783.)

If a defendant cannot demonstrate the probable cause necessary to obtain reference samples from third parties via warrant, then he certainly lacks any compelling reason to access the State's confidential and privileged offender DNA Database for the same purpose. Conversely, if a defendant can demonstrate probable cause for third party reference samples, he can obtain them by warrant and need not access DOJ's confidential DNA Database.

F. Research

Penal Code section 299.5(m) permits DOJ, an agent of DOJ, or a "local public laboratory" to use DNA database records for training, research, statistical analysis, or quality control purposes. It does not contemplate or authorize disclosure of DNA profiles to any other recipient, let alone to any other recipient for criminal defense purposes. In any event, the entire analysis presented above applies with equal force to defense requests to access the State's DNA Database for "research" purposes.