FACT SHEET ON FORENSIC DNA ANALYSIS
Addressing Privacy Concerns

A common concern raised during discussions of expansion of forensic DNA programs involves fears over risks to personal privacy, and especially genetic health information. Such concerns are understandable and are certainly an important matter to address. However, a significant body of laws and regulations (both state and federal) already exist to provide ample protection against illegal privacy intrusions. Moreover, forensic DNA analysis itself does not lend to genetic health testing procedures. The following fact sheet explains how existing scientific methods, as well as laws and regulations provide rigorous privacy protections.

FACT ONE: Forensic Analysis of DNA Samples Does Not Reveal Personal Information
- There are more than 3 billion base pairs in a DNA strand, and forensic DNA analysis uses just 13 of these pairs (or 26 individual sites). These 13 sites, or “loci”, were specifically selected by a scientific working group of DNA experts assembled by the FBI (with authority through an Act of Congress).
- The selected 13 sites were specifically selected because they reside on portions of the human genome that are non-coding and contain no useful genetic information. However they are uniquely individual to each person (with the exclusion of identical twins – thus far scientific research has discovered no genetic differences between identical twins).
- A convenient description was offered by a renowned forensic geneticist and former chair of the national DNA Advisory Board. The 13 core loci of forensic DNA analysis can be compared to the spaces in between songs on LP records – for the younger generation, liken this to the dead space in between songs on your iPod. The spaces in between songs (represented by the darker bands on the record below) contain no useful information about the song. One cannot listen to that space and determine how the songs on this record will sound. However, taken as a whole, the measure of these blank spaces between songs is unique to each album.

FACT TWO: Shared Forensic DNA Databases Do Not Include Personally Identifying Information
- The shared local, state and national forensic DNA databases (call CODIS – Combined DNA Index System) contains absolutely no personally identifying information about an included individual, other than a notation on whether the subject is male or female.
- The CODIS profile contains only the DNA profile (recorded as a series of numbers and letters), and additional data regarding the lab and analyst responsible for the profile. Consider the following sample CODIS profile – this is the only information shared in CODIS.

<table>
<thead>
<tr>
<th>Originating Laboratory Identifier</th>
<th>LabXYZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specimen ID #</td>
<td>0012152</td>
</tr>
<tr>
<td>13 Core Loci</td>
<td>06,09,11,12,10,10,22,24,9,3,10,8,9,14,15,17,17,22,25,12,12,9,10,9,13</td>
</tr>
<tr>
<td>Analyst Identifier</td>
<td>DHL</td>
</tr>
</tbody>
</table>

- After a CODIS match, the Originating Laboratory (which is the crime laboratory that “owns” the sample) uses the Specimen ID # (a consecutive number automatically generated upon database entry) to cross-reference an offline, state-owned secure database in which the identity belonging to that profile is kept. These identities are not shared with other laboratories (or criminal justice interests) absent a database match.
- CODIS profiles are not permitted to be shared with other types of databases and are not part of the criminal history record or otherwise accessed by third party criminal justice interests such as the Department of Homeland Security. DNA profiles are only searched against the CODIS index of unsolved crimes, and occasionally against the CODIS missing persons/unidentified remains index.
- CODIS data is protected by the FBI’s state of the art encryption and firewalls. The database has never been breached. However, if a hacker were to circumvent these protections and gain illegal access to the database, the only information this hacker would gain is the profile information provided in the sample above. There is no useful information to be gained by hacking CODIS.
While the profile generated by forensic DNA analysis does not contain private genetic information, arguments abound that the collected DNA sample could still be misused – either tested by the crime laboratory for alternate purposes or otherwise gained by 3rd parties for testing. The following points address the likelihood of this concern.

FACT THREE: Collected DNA Samples Are Retained For Quality Control and To Further Protect Privacy

In engaging in this discussion, it is first important to understand that crime laboratories, as a matter of regulation, do not destroy DNA samples after analysis. While destroying the samples could allay some privacy and misuse concerns, the actual result would be a loss of quality control and could result in unwarranted and avoidable privacy intrusions.

- Samples are retained so that laboratories may perform quality control checks. The following scenarios provide clarification of why retention of these samples is vital:
  1. After a match is made on the DNA database, the laboratory re-tests the original offender sample in order to confirm the match. This re-testing ensures that no mistakes were made – such as a mistake in data entry. This additional process to ensure accuracy also ensures that investigators are not wrongly given the name of an innocent person in connection with a serious crime investigation. This step protects the privacy of those on the database so that innocent people are not wrongly questioned.
  2. Through the process explained above, if a problem is identified with a DNA profile, then the laboratory would need to have access to all original samples in order to determine exactly when the mistake occurred, for how long the mistake was perpetuated, and whether it is a systemic problem or something localized to specific personnel. Without the ability to retest, the integrity of the entire database is compromised. It would also be impossible to recollect the majority of the samples, as many of the offenders will no longer be under supervision – recollecting samples from may not be legal, and would at the very least be an unnecessary invasion of privacy.

- CONSIDER: Many states currently require the retention of biological evidence for cases involving a serious criminal conviction. The biological evidence retained is not only that of just the offender, but also typically contains samples from the victim and from others who may have needed to be excluded as possible suspects– for example, in a rape case, spouses and other consensual sexual partners would have been asked to provide a DNA sample so that this DNA profile can be excluded if it is found in a rape exam.

- Destroying samples after analysis would also prohibit laboratories from changing to new, and possibly more accurate and efficient, DNA technologies. Such a change in technologies could require retesting of existing samples – this has already happened once since the DNA databases were established.

- Regulations established for participation in the national DNA database system by the Scientific Working Group on DNA Analysis Methods (SWGDAM) indicate a scientific preference for retaining offender DNA samples. Standard 7.2 of the Quality Assurance Standards for DNA Databasing Laboratories says that “where possible” laboratories should “retain the database sample for retesting for quality assurance and sample confirmation purposes”.

FACT FOUR: Collected DNA Samples Are Securely Stored and Amply Protected.

The Scientific Working Group on DNA Methods (SWGDM), which establishes Quality Assurance standards required by the FBI for participation in the national DNA database, has published the standards listed below relating to requirements for secure facilities (Quality Assurance Standards for DNA Databasing Laboratories, www.fbi.gov/about-us/lab/codis/qas_databaselabs). All DNA laboratories participating in the national DNA database system are further required to undergo an audit on an annual basis to ensure compliance with these standards.

**Standard 4.1.5** Specify and document the responsibility, authority, and interrelation of all personnel who manage, perform, or verify work affecting the validity of the DNA analysis

**Standard 6.1** The laboratory shall have a facility that is designed to ensure the integrity of the analyses and the samples.

**Standard 6.1.1** Access to the laboratory shall be controlled and limited in a manner to prevent access by unauthorized personnel. All exterior entrance/exit points require security control. The distribution of all keys, combinations, etc. shall be documented and limited to the personnel designated by laboratory management.

**Standard 7.1** The laboratory shall have and follow a documented sample inventory control system to ensure the integrity of database and known samples. This system shall ensure that:

**Standard 7.1.1** Database, known, and casework reference samples shall be marked with a unique identifier or the laboratory shall have and follow a method to distinguish each sample throughout the processing (such as plate or rack mapping) that may not require the assignment of unique identifiers.

**Standard 7.1.2** Documentation of sample identity, collection, receipt, storage, and disposition shall be maintained.
Standard 7.1.3 The laboratory shall have and follow documented procedures designed to minimize loss, contamination, and/or deleterious change of samples and work product in progress.
Standard 7.1.4 The laboratory shall have secure areas for sample storage including environmental control consistent with the form or nature of the sample.

- In sum, DNA samples must be stored in a secure, locked site which allows limited access to only those personnel named in the laboratory’s written policy manual. These national standards developed by SWGDM are a minimum standard, and are often superseded by more stringent state procedures.

**FACT FIVE: Federal and State Laws Penalize Misuse of Offender Profiles**

Federal law strictly prohibits the dissemination of information from the DNA database to unauthorized persons and for unauthorized reasons.
- Section 42 USC 14133(b) provides that results from DNA analysis may only be released to criminal justice agencies for law enforcement identification purposes; in judicial proceedings; and to criminal defendants for the case in which the person is involved.
- Section 42 US 14133(c) provides that any person who has access to information contained in the national DNA database and knowingly discloses such information in an unauthorized manner may be fined up to $100,000. Furthermore, any person who accesses such database information or samples without authorization may be fined up to $250,000 and sentenced to one year in prison.

**FACT SIX: Federal and State Laws Penalize Misuse of Private Genetic Information**

Under the federal Genetic Information and Non-discrimination Act (GINA) (PL 110-233):
- Insurance carriers are prohibited from discriminating among policy holders (current or prospective) based on information regarding genetic predisposition to disease.
- Employers may not request, require or purchase genetic information or samples from employees, and may not make hiring, firing, promotion, job placement or promotion decisions using genetic information.
- Thus, even if a rogue lab employee act in an illegal fashion to sell or otherwise misuse DNA collected for CODIS inclusion, there is little market for such information as the end user is prohibited from utilizing the data in any meaningful way and faces both criminal and civil prosecution.

**FACT SEVEN: Forensic DNA Analysts Do Not Have the Training or Resources to Misuse Samples**

Although misusing forensic DNA samples in violation of federal and state laws would mean a DNA analyst is willing to not only jeopardize his/her career but also risk criminal penalties in order to sell genetic information to a market that is prohibited by federal law from existing, occasionally there is still an argument that a “rogue” DNA analyst may attempt to do so for personal gain. However, this scenario is also extremely unlikely for the following reasons:
- As noted previously, the 13 loci tested for forensic purposes do not reveal any personal genetic health information. Thus, the original DNA sample would have to be accessed and re-tested.
- The laboratory personnel with access to both the storage facilities as well as the laboratory equipment is strictly regulated, so the number of personnel physically able to conduct such testing is very limited.
- Assuming the rogue employee has acquired the additional chemicals needed (which are highly proprietary and not commonly available), the next step would be to perform analysis on the genetic analysis machines. Many of these machines run automatically throughout the night and would need to be stopped and restarted in order to be adjusted for the supposed genetic health testing. Such actions would trigger activity logs showing the unauthorized activity.