

# FORENSIC SCIENCE OVERSIGHT BOARD

## Report on the Bristol County District Attorney's Office DNA Database



### Board Member Co-Authors:

Robin Cotton  
Lucy Davis  
Lisa Kavanaugh

### Legal research support:

Meg Foster

October 22, 2021

## Table of Contents

INTRODUCTION	1
EXECUTIVE SUMMARY	2
A. OVERVIEW OF INVESTIGATIVE STEPS	3
B. APPLICABLE LEGAL FRAMEWORK	5
C. FACTUAL FINDINGS RELATED TO BRISTOL DNA DATABASE	7
1. 2019 Bristol County District Attorney Request for Y-STR Data	7
2. January 2021 Grand Jury Subpoena	8
D. SCIENTIFIC & REGULATORY CONCERNS WITH DATABASE	9
1. Data Access and Security Measures	10
2. Data Quality Assurance	12
3. Handling of Searches and Profile Comparisons	14
4. Confidentiality and Data Sharing with Outside Entities	15
5. Relevant Features and Limitations of Y-STR DNA Data	19
CONCLUSION & RECOMMENDATIONS	21
EXHIBITS	22
A. District Attorneys' Letter to FSOB (1.27.21)	23
B. MACDL ACLUM Letter to FSOB (2.10.21)	26
C. FSOB Motion (2.10.21)	31
D. FSOB Letter to FSOB Chairperson (4.27.21)	32
E. FSOB Questions to Bristol DA (5.7.21)	36
F. FSOB Questions to MSPCL (5.7.21)	40

G. MSPCL Response to FSOB Questions (5.20.21)	.	.	.	43
H. FSOB Letter to DA Quinn (5.24.21)	.	.	.	45
I. Draft Data Use and Dissemination Agreement (1.25.21)	.	.	.	47

## INTRODUCTION

The Forensic Science Oversight Board (hereinafter “FSOB”) was established in 2018 to “have oversight authority over all commonwealth facilities engaged in forensic services in criminal investigations” and to “provide enhanced, objective, and independent auditing and oversight of forensic evidence used in criminal matters.” M.G.L. c. 6 sec. 184A. Subsection (d)(ii) authorizes the FSOB to “initiate an investigation into any forensic science, technique or analysis used in a criminal matter upon a determination by not less than 5 members of the commission...that an investigation of a forensic analysis would advance the integrity and reliability of forensic science in the commonwealth.”

On April 30, 2021, the FSOB voted to initiate an investigation under Subsection (d)(ii) into the integrity and reliability of an unregulated database of aggregated DNA records established in Bristol County (hereinafter the “Bristol Forensic DNA Database”). That vote came on the heels of the FSOB’s publication and dissemination of its March 24, 2021 Report on Familial DNA Searching,<sup>1</sup> which included a lengthy discussion of the perils of secondary, unregulated DNA databases “that threaten to sidestep the carefully crafted regulatory scheme for DNA testing in Massachusetts.”

Over the course of several public meetings, the FSOB invited the Massachusetts State Police Crime Lab (“Crime Lab”), Attorney General’s Office and Bristol County District Attorney’s Office (“Bristol District Attorney”) to provide information about the origin, nature and scope of the Bristol Forensic DNA Database. Crime Lab representatives attended every Board meeting; the Crime Lab also responded in writing to the FSOB’s questions. The Bristol District Attorney, in contrast, declined to respond in writing to any of the FSOB’s inquiries, and elected not to attend any of the public meetings at which the Bristol Forensic DNA Database was discussed.

This Report is organized as follows: **Part A** describes the steps taken by the FSOB to investigate the Bristol Forensic DNA Database. **Part B** identifies the applicable legal framework that should be used to analyze the Bristol Forensic DNA Database. **Part C** summarizes the FSOB’s factual findings with respect to the origin, nature and scope of the Bristol Forensic DNA Database. **Part D** describes the regulatory and scientific concerns identified by the FSOB in its evaluation of the Bristol Forensic DNA Database.

---

<sup>1</sup> Full Report Available online at <https://www.mass.gov/doc/forensic-science-oversight-board-familial-dna-searching-report-march-24-2021/download>

## **EXECUTIVE SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS**

**Based on available information and reasonable inferences drawn therefrom,** the FSOB concludes and recommends the following:

- The Bristol District Attorney has created an unregulated database of forensic DNA records that jeopardizes the integrity and reliability of forensic science in the Commonwealth of Massachusetts.
- The Bristol Forensic DNA Database consists of aggregated reports and data derived from DNA analysis conducted by the Crime Lab. It includes full DNA reports for all profiles, without any redaction of proper names or gender for known profiles. It includes profiles submitted by victims, family members and consensual sexual partners for exclusionary purposes; profiles from suspects and defendants who are not required by statute or regulation to provide a profile for inclusion in the state DNA database. It may also include profiles submitted by law enforcement, lab personnel and/or testing observers for exclusionary purposes. It also includes profiles that were developed from an entirely different biological sample than the one used to develop DNA profiles for inclusion in the state DNA database.
- In contrast with the highly regulated state DNA database that is overseen by the Crime Lab, it is unknown whether the Bristol District Attorney's Office has any protocols and procedures in place to safeguard the confidentiality and security of genetic information in the database; to ensure the accuracy and reliability of that genetic information; to require minimal training, education or demonstrated competency to access and administer the database; or to utilize scientifically trained personnel to interpret DNA data and comparisons of profiles.
- The absence of protocols and procedures for the Bristol Forensic DNA Database jeopardizes the privacy of all those whose information is included in the database, and its creation and administration may constitute a violation of the Fair Information Practices Act, G.L. c. 66A.
- The continued operation of the Bristol Forensic DNA Database jeopardizes the Crime Lab's accreditation status as well as its ongoing participation in NDIS, the national DNA database.
- The Legislature should amend G.L. c. 22E sec. 10 to explicitly prohibit the aggregation of DNA records for inclusion in an external, unregulated DNA record database.

## **A. OVERVIEW OF INVESTIGATIVE STEPS**

The FSOB's decision to initiate an investigation into the Bristol Forensic DNA Database was prompted by a series of events beginning on January 27, 2021, as the FSOB was finalizing its report on proposed revisions to M.G.L. c. 22E, the statute governing the Massachusetts statewide DNA database. On that date, the Executive Office of Public Safety and Security (EOPSS) provided the FSOB with a letter signed by six elected district attorneys which notified the FSOB of their intent to create an aggregated database of Y-STR records from the Massachusetts State Police Crime Laboratory (hereinafter "crime lab").<sup>2</sup> The letter referenced the "Commonwealth's District Attorneys' Offices" proposal to use Y-STR records to develop "investigative leads in unsolved homicides, rapes, and other serious crimes" and to create an "accurate list of every case where this (Y-STR) testing was used." It did not specify any details about the timing or scope of the request for DNA records. EOPSS also provided the FSOB with a draft Use and Dissemination Agreement prepared by the Crime Lab in response to the aforementioned request for production of DNA records, but no further information was provided about whether any requesting agencies had signed such an agreement.

At an emergency meeting on February 10, 2021, the FSOB learned that one of the signatories to the letter – the Bristol District Attorney – had already secured a grand jury subpoena to *compel* the crime lab to produce aggregated Y-STR records. EOPSS reported that the Attorney General had moved on behalf of the crime lab to quash the grand jury subpoena, and that the trial court judge presiding over the motion had denied the motion to quash. The FSOB discussed a letter submitted by the Massachusetts Association of Criminal Defense Lawyers ("MACDL") and the American Civil Liberties Union of Massachusetts ("ACLUM") that outlined numerous legal concerns with the Bristol District Attorney's planned database, including the risks that the planned database could violate both G.L. c.22E *and* G.L. c. 66A, the Fair Information Practices Act ("FIPA").<sup>3</sup>

At the conclusion of the February 10 emergency meeting, the FSOB passed a resolution that, in the view of FSOB members, production of the requested Y-STR records could jeopardize the Crime Lab's accreditation status and compliance with the National DNA Indexing System (NDIS) that manages the Combined DNA Indexing System (CODIS), and could also constitute a violation of the plain language of G.L. c.22E and G.L. c. 66A.<sup>4</sup> The FSOB urged the Attorney General, on behalf of the Crime Lab, to notify the trial court of the FSOB's position on these matters.

On March 24, 2021, the FSOB learned that the Attorney General, on behalf of the Crime Lab, had filed a motion to reconsider in which it provided the trial court with a copy of the FSOB's resolution and the stakeholder letters from the district attorneys, MACDL and the ACLUM. EOPSS reported that the trial court judge denied the Attorney General's motion to reconsider,

---

<sup>2</sup> Attached hereto as Exhibit A. The signatories to the letter are: Michael O'Keefe (Cape & Islands), Jonathan W. Blodgett (Essex), Timothy Cruz (Plymouth), Joseph D. Early (Worcester), Thomas M. Quinn (Bristol), David E. Sullivan (Northwestern).

<sup>3</sup> Attached hereto as Exhibit B.

<sup>4</sup> Attached hereto as Exhibit C.

but was unable to state whether the Attorney General intended to file an appeal on behalf of the Crime Lab.

On April 27, 2021, three FSOB members submitted a letter to the FSOB<sup>5</sup> articulating their view that the Bristol District Attorney's plan to aggregate and store Y-STR records in a searchable database clearly violates G.L. c. 66A because:

- The Y-STR records that the Bristol District Attorney requested are quintessential "personal data" as defined by G.L. c. 66A sec. 1 (personal data defined as "any information concerning an individual which, because of name, identifying number, mark or description can be readily associated with a particular individual");
- The Bristol District Attorney's Office meets the statutory definition of an "agency" under the meaning of G.L. c. 66A ("any agency of the executive branch of the government, including but not limited to any constitutional or other office, executive office, department, division, bureau, board, commission or committee thereof");
- The Bristol District Attorney is a "holder" of personal data as to the Bristol County Y-STR records that the Crime Lab provided to them pursuant to its earlier written request (holder defined as "an agency which collects, uses, maintains or disseminates personal data or any person or entity which contracts or has an arrangement with an agency whereby it holds personal data as part or as a result of performing a governmental or public function or purpose");
- The Bristol District Attorney has expressed a clear intent to become a "holder" of personal data from other counties as soon as the laboratory complies with the grand jury subpoena; and
- The January 27, 2021 letter, to which the Bristol District Attorney is a signatory, expressly states an intent to create an aggregated database of Y-STR records to enable counties across the state to "pool resources" to develop "investigative leads in unsolved homicides, rapes, and other serious violent crimes." This plan explicitly contemplates the sharing of data with outside agencies, in violation of G.L. c.66A sec 2(c).

On April 30, 2021, after voting to initiate an investigation into the Bristol District Attorney's planned database, the FSOB agreed to begin by eliciting responses from the Bristol District Attorney and the Crime Lab to written questions aimed at better understanding the nature and scope of the release of DNA data by the Crime Lab. On May 7, 2021, the FSOB finalized and disseminated two memoranda containing detailed questions, one directed at the Bristol District Attorney and another at the Crime Lab.<sup>6</sup> The FSOB invited both entities to provide written or oral responses to the FSOB's request for information, and to attend the next scheduled FSOB

---

<sup>5</sup> Attached hereto as Exhibit D.

<sup>6</sup> Attached hereto as Exhibits E and F.

meeting, on May 21, 2021. The Bristol District Attorney did not in any way acknowledge receipt of the FSOB's request, nor did he express an intent to respond or to attend the May 21, 2021, FSOB meeting. The Crime Lab responded in writing and attended the meeting.<sup>7</sup> The particulars of the Crime Lab's response are described below, in the "findings" section of this Report.

On May 21, 2021, the FSOB met to discuss the Crime Lab's responses. EOPSS informed the FSOB that it was unable to provide any of the pleadings or court orders relative to the grand jury investigation, even in redacted form. The Bristol District Attorney did not attend this meeting, nor did he send a representative on his behalf to answer the FSOB's questions. At the conclusion of the meeting, EOPSS agreed to send a second letter to the Bristol District Attorney, requesting his response on or before June 18, 2021. This letter<sup>8</sup> further informed the Bristol District Attorney that should it opt not to participate, the FSOB would move forward without that office's input, and report the results of its investigation and any resulting recommendations to the Executive Office of Public Safety and Security, the Joint Committee on Public Safety and Homeland Security, the Supreme Judicial Court, the Massachusetts District Attorney's Association, the Massachusetts Attorney General, the Committee for Public Counsel Services, the Massachusetts Association of Criminal Defense Lawyers, and the New England Innocence Project, Inc., as required by the FSOB's enabling statute. The FSOB also voted to prepare a written report summarizing its findings relative to the Bristol Forensic DNA Database, based on the information provided by the Crime Lab and any other relevant additional resources, including the January 27, 2021 letter.

To date, the Bristol District Attorney has not responded to the serious concerns raised by the FSOB in multiple public meetings.

## **B. APPLICABLE LEGAL FRAMEWORK**

By way of further background, the FSOB recognizes the following state and federal laws as framing our consideration of the legality of the Bristol District Attorney's unregulated DNA database:

### Mass. Gen. Laws c. 22E

- Establishes the state DNA index, enumerates the categories of persons required to submit a DNA sample, and mandates the Crime Lab laboratory director to promulgate regulations pertaining to collection, analysis, retention, and disclosure of DNA records.<sup>9</sup>

---

<sup>7</sup> Attached hereto as Exhibit G.

<sup>8</sup> Attached hereto as Exhibit H.

<sup>9</sup> Mass. Gen. Laws ch. 22E, § 8. See 515 Mass. Code Regs. 1.00, 2.00.



- Specifies that regulations must be compatible with the FBI's own procedural rules and quality assurance program with regard to the Combined DNA Index System (CODIS) and National DNA Index System (NDIS).<sup>10</sup>
- Legislative history suggests that 22E was never meant to permit creation of an unregulated DNA database, especially one containing non-22E-mandated DNA profiles.

Mass. Gen. Laws c. 66A, (Fair Information Practices Act)

- Section 2(l) prohibits the collection and maintenance of “more personal data than are reasonably necessary for the performance of the holder’s statutory functions.”
- The Bristol District Attorney’s request for Y-STR reports is akin to the “shadow database” maintained “outside the statutorily authorized State convicted offender database governed by G.L. c. 22E, and the FBI’s CODIS database” at issue in *Amato v. District Attorney for Cape and Islands*, 80 Mass. App. Ct. 230, 236 (2011). In *Amato*, the Appeals Court concluded that the plaintiff had sufficiently alleged a violation of FIPA where he, along with 200 other men, had voluntarily provided DNA for elimination purposes and was assured that such samples and associated records would be destroyed if it was determined that their DNA did not match crime scene evidence. Nine years later, the District Attorney nonetheless declined to destroy or return Amato’s record, despite completion of the statutory function of securing a conviction in the case.

G.L. c. 214, § 1B (Privacy Act)

- The *Amato* court also concluded that the creation of an alleged “shadow database” allowed for a Privacy Act claim: “The allegations that the defendants have retained Amato’s highly sensitive DNA records without his consent and made them available for nonconsensual use in other criminal investigations are sufficient to constitute an unreasonable, substantial, and serious interference with Amato’s privacy.”
- The court specifically noted its concern that the records at issue were “not subject to safeguards against disclosure, such as the criminal sanctions for unauthorized disclosure or acquisition of information in the State convicted offender database provided by G.L. c. 22E.”
- The Bristol District Attorney’s request to procure and retain Y-STR reports for a purpose beyond that for which they were lawfully obtained in the first place, if not a Fourth

---

<sup>10</sup> CODIS “is the generic term used to describe the FBI’s program of support for criminal justice DNA databases as well as the software used to run these databases.” *Frequently Asked Questions on CODIS and NDIS*, Fed. Bureau Investigation, <https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet>. NDIS is the national level of CODIS. *Id.* The Scientific and Regulatory section provides a more comprehensive description of CODIS and associated federal requirements relevant to the BCDA’s DNA database.

Amendment or Art. 14 violation, could at least constitute FIPA and Privacy Act violations.

**Health Insurance Portability and Accountability Act (HIPAA) and Genetic Information Nondiscrimination Act (GINA)**<sup>11</sup>

- While not directly applicable, HIPAA and GINA's specific restrictions on DNA information disclosure for law enforcement purposes caution against the indiscriminate disclosure requested by the Bristol District Attorney.

**C. FACTUAL FINDINGS RELATED TO THE BRISTOL DNA DATABASE**

The FSOB makes the following findings related to the process, content and scope of the establishment of a local, unregulated DNA database that is being run by the Bristol District Attorney.

1. September 2019 Bristol District Attorney Request for Y-STR Data

In September 2019, the Crime Lab received a written request from the Bristol District Attorney for **all Y-STR data**, in aggregate form, from **all counties** in the Commonwealth. The request sought "any/all investigative cases/DNA reports that produced a Y-STR profile in the possession of the Massachusetts State Police Crime Laboratory." It specified that "all Y-STR results tables include sample description, case numbers, item number and Y-STR results in data form..."

The Crime Lab had numerous scientific concerns with the Bristol District Attorney's request, including: (1) the prospective operation of a DNA database by non-forensic scientists; (2) the potential for release of data to/from other counties without express permission; and (3) the lack of safeguards to protect data and any information resulting from any potential forensic links resulting from that data. The Crime Lab discussed its concerns with EOPSS and the Attorney General's Office and communicated them to the Bristol District Attorney.

Notwithstanding these scientific concerns, the Crime Lab believed that it was required by law to provide Bristol District Attorney with its *own customer data* when requested. For purposes of the Crime Lab's accrediting body, ANSI National Accreditation Board (ANAB), the submitting agency and corresponding district attorney's office are considered the customer. The Crime Lab provided the Bristol District Attorney with all Y-STR reports originating from its own cases and requests, but declined to provide Bristol District Attorney with any Y-STR profiles that were developed for any other county outside of Bristol. The Crime Lab did receive two additional

---

<sup>11</sup> See 45 C.F.R. § 164.512(f) (outlining conditions to be met in order for personal health information disclosures to be made for law enforcement purposes under the HIPAA Privacy Rule); Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, § 206, 122 Stat. 881, 913-914 (outlining confidentiality requirements for employers in possession of employee genetic information).

requests, from the Worcester and Plymouth County District Attorneys, each of whom sought DNA records from their respective counties for inclusion in the Bristol Forensic DNA Database. However, neither district attorney signed the Crime Lab's draft Use and Dissemination Agreement, and the Crime Lab has not released any data to either county.

The Bristol County DNA data that the Crime Lab provided to the Bristol District Attorney in response to its September 2019 request included the following:

- Full DNA reports for all profiles provided, without any redaction, meaning that the reports contained proper names and gender for all known profiles;
- Y-STR and STR profiles;
- Profiles developed from *victims* as well as suspects;
- Profiles submitted by family members and consensual sexual partners for exclusionary purposes (although the Crime Lab noted that the exact relationship of an individual to a case is not always known);
- Profiles from individuals who are required by statute to be included in CODIS and the state DNA databases, but in circumstances where the profile provided to the DA's office would have been developed from an entirely different biological sample than the one used to develop the DNA profile for the state database; and
- Profiles from suspects/defendants who are *not* required by statute or regulation to provide a profile for inclusion in the CODIS or state DNA database.

The data provided to the Bristol District Attorney also potentially included profiles of law enforcement, laboratory personnel, and defense representative testing observers. The Crime Lab provided the Bristol District Attorney with a proposed Use and Dissemination Agreement, but the Bristol District Attorney declined to sign

## 2. January 2021 Grand Jury Subpoena

On January 9, 2021, after declining to provide the Bristol District Attorney with any DNA data from counties other than Bristol, the Crime Lab received a grand jury subpoena from Bristol County. After motion practice, the Crime Lab began complying with the subpoena by producing the requested data in PDF format.

Due to confidentiality restrictions with the grand jury process, the Crime Lab was unable to provide any details about the scope of the grand jury subpoena or its compliance therewith, and EOPSS has declined to provide the FSOB with redacted copies of the pleadings and/or trial

court order relative to this request. Nonetheless, the FSOB draws the following inferences from the materials provided:

- The Crime Lab already has released non-customer information to the Bristol District Attorney, including non-customer DNA data. It is reasonable to infer that the Crime Lab likely released the data in the same format and content as previous data provided to the Bristol District Attorney (unredacted PDF copies of DNA reports), thus it may also have included both Y-STR and autosomal DNA profiles.
- Additionally, recognizing that its compliance with the grand jury subpoena may jeopardize its accreditation status, the Crime Lab has notified the ANAB accreditation manager of the grand jury subpoena and of the fact that it has not yet determined whether it is legally permitted to notify the original submitting agencies (customers) of the release of their customer data to Bristol County.

#### **D. REGULATORY AND SCIENTIFIC CONCERNS**

Forensic DNA databases that public forensic laboratories develop and participate in are well regulated by state and federal legislation, as well as restrictive internal policies and procedures. These requirements are in place to ensure the validity of matches that may be identified when conducting a search. They also safeguard the privacy and constitutional rights of those individuals whose DNA may be in the database or who may be the subject of an investigation. None of these legislative and regulatory safeguards are binding upon the database created by the Bristol District Attorney. The Bristol Forensic DNA Database could affect the integrity and reliability of forensic science in the commonwealth because it is not operated in accordance with any defined policies and procedures to ensure the quality and security of the genetic information contained therein. Moreover, the method in which the database is being developed has grave implications for the Crime Lab, because the Bristol District Attorney is using the genetic analysis results that the Crime Lab released pursuant to its 2019 request and to the 2021 grand jury subpoena without any regulation or oversight.

As described above, the FSOB began its investigation into the Bristol District Attorney's planned DNA database by providing the Bristol District Attorney with a written list of questions aimed at better understanding how the BDCAO intended to manage the quality and security of the data it received and would continue to receive from the Crime Lab. The FSOB's inquiry included questions about the existence of any written protocols to address the establishment and oversight of the planned DNA database including: (1) data access/security; (2) data quality assurance; (3) handling of searches/profile comparisons; (4) confidentiality; (5) data sharing with outside entities; (6) notification & expungement; and (7) methodology/loci questions. The Bristol District Attorney has not provided any information in response to the FSOB's questions about these issues.

1. Data access/security concerns, based on the FSOB's general understanding of applicable CODIS rules

The forensic DNA databases that public forensic laboratories develop and participate in are part of a national database called the Combined DNA Indexing System (CODIS). There are three levels at which data is provided and accessed. The Local DNA Index System (LDIS) is data developed from criminal investigations by local forensic laboratories operated by local government agencies (such as the Boston Police Department Crime Laboratory). The State DNA Index System (SDIS) is a government laboratory appointed by the state to manage the state's CODIS system. SDIS databases will contain DNA profiles developed by the state laboratory from criminal investigations and profiles from persons defined by the state's legislation to submit DNA samples as offenders. The state database will also include data from the state's LDIS laboratories.

The Crime Lab is defined as the Massachusetts SDIS laboratory. Finally, the National DNA Index System (NDIS) is managed by the FBI laboratory and includes all states' DNA profiles (both criminal and offenders) as well as DNA profiles developed by federal laboratories. All participants in CODIS must follow federal requirements and must submit to regular audits to confirm they are meeting the NDIS Operational Procedures Manual<sup>12</sup> and any applicable legislative requirements.

The Crime Lab provided its DNA data to the Bristol District Attorney in hard copy (PDF) form. The data included personal identification information and genetic analysis of both autosomal STR and Y chromosome STR DNA profiles. The data included DNA profiles from crime scenes, profiles from suspects under investigation who are not required to provide DNA to the state database, elimination samples from other possible contributors not related to the criminal act, and family members or acquaintances of victims. Access to such information and data must be controlled to ensure that it is not seen or used by persons that may misuse it; consequently, CODIS does not allow these DNA profiles to be included in the database.

There are strict security requirements related to persons who may have access to the computers used for the CODIS database. A CODIS user must be an employee of a government laboratory, a qualified DNA analyst, meet all appropriate local and state employment requirements including background or security investigations, undergo an FBI security check, and maintain the appropriate security clearance while accessing the CODIS database. An IT employee who is permitted access to CODIS computer hardware/software and telecommunications for maintenance purposes must also meet these security requirements.

---

<sup>12</sup> National DNA Index system (NDIS) Operational Procedures Manual; version 9, revision 2; effective 2/1/2021

CODIS software network and data is managed by the FBI's Criminal Justice Information Services Division (CJIS), which protects the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The CJIS network is an encrypted, wide area network accessible to only criminal justice agencies approved by the FBI. Agencies with access to CODIS must meet the CJIS Security Policy.<sup>13</sup> This policy also has strict security requirements related to access to computers, servers, and all information included on the network.

The Crime Lab's CODIS/DNA Unit Manual<sup>14</sup> requires that SDIS users meet the NDIS background/security requirements. The Crime Lab's CODIS server is held in a secure, limited access room. Access to the room is granted by the Crime Lab's Director via an electronic key card or a controlled key. The CODIS server and workstations are password-protected and cannot be accessed without a valid user account and password. CODIS workstations are set to lock after a designated time period of non-use. A CODIS user may only log on to a CODIS workstation using his/her own user ID. A CODIS user must change his/her CODIS password at a defined frequency. CODIS database software is only installed on designated workstations that are used solely for the purpose of accessing CODIS.

In its May 7, 2021 memorandum, the FSOB asked the Bristol District Attorney to provide information regarding, among other things, who will have access to their database and if there are different levels of access of personnel who are authorized to view/edit/alter data. In particular, the FSOB asked the Bristol District Attorney to explain:

- Who can view the data?
- Who can edit the data?
- What requirements are there for authorization?
- What measures are in place to track who accesses/enters/views/edits data?
- What security measures exist to protect the data from being accessed or modified by unauthorized individuals (internal or external to their agency)?

To date, the Bristol District Attorney has not provided any information concerning these issues. However, other available information -- most notably a WCVB Channel 5 television interview of the Bristol County District Attorney -- support the inference that the Bristol District Attorney has *not* implemented adequate access and security measures. During the interview, the Bristol District Attorney displayed a computer located in a general area of the office and directed the camera to the computer's monitor, which contained a visible DNA profile:

---

<sup>13</sup> Criminal Justice Information Services (CJIS) Security Policy; version 5.9, 06/01/2020

<sup>14</sup> Crime Lab CODIS/DNA Unit Manual; ID: 2792, revision 4.

DYS385 a/b	DYS393	DYS391	DYS439	DYS635	DYS392	YGATAH4	DYS437	DYS438	DYS448
(11), 14	13	11	(12)	(20)	(13)	(11)	14	(12)	(19)
12, 15	13	11	11	24	11	13	15	10	20
12, 15	13	11	(11)	(24)	(11)	(13)	(15)	(10)	NR
(12)	13	11	(11)	NR	NR	11	(15)	NR	NR
NR	13	11	NR	24	NR	(11)	15	(10)	(20)
11, 14	13	11	12	23	13	13	14	12	18
11 (14)	14	(10) 11	(12)	23	13	13	(14) 15	12	19
15 16 17	13	10 (11)	12	23	11 (12)	(11) 12	14	(12)	NR
11, 14	13	10	12	24	13	13	15	12	19
(16), (17)	(13)	10	NR	NR	NR	(11)	(14)	NR	NR
11, 15	13	10	13	23	13	12	15	12	19
11, 14	13	11	13	23	13	13	15	12	18
11 14 15	13	10 11	13	23	13	12 13	15	12	18
11, 15	13	10	13	23	13	12	15	12	19
11, 14	13	11	12	23	13	12	15	12	18
11 14 (15)	13	11	12	23	13	12	15	12	18
11, 15	13	10	12	23	14	10	14		

**Figure 1. Screenshot of WCVB broadcast interview with Bristol County DA Quinn**

DA Quinn’s conduct during the television interview,<sup>15</sup> and in particular the fact that he allowed a camera to capture a visible DNA profile on a computer screen, demonstrate the absence of any existing security measures and a lack of concern for the protection of the genetic data or any personal information contained within their database. The FSOB infers from available information, including the Bristol District Attorney’s unwillingness to sign a Use and Dissemination Agreement<sup>16</sup> with the Crime Lab or to respond to this FSOB’s requests for information, that the Bristol District Attorney has not implemented any measures to safeguard the privacy of the genetic information contained in their database.

## 2. Data Quality Assurance

To ensure the quality of the information being used to identify possible suspects of a criminal act, documented procedures are required, as is demonstrated compliance with those procedures. This is the foundation of any quality assurance program required by accreditation bodies. Although an organization is not required to be accredited, it is important to have a quality assurance program in place to ensure that inaccurate results are not reported. Quality issues related to developing, maintaining, and reporting database matches must be identified and minimized to provide reliable and accurate results.

The Federal DNA Identification Act of 1994<sup>17</sup> requires all laboratories accessing CODIS must meet or exceed the FBI Director’s *Quality Assurance Standards for Forensic DNA Testing and DNA Databasing Laboratories*.<sup>18</sup> The laboratory’s audit must be sent to the CODIS Unit, where the Chair of the NDIS Audit Review Panel performs a review of the documentation to ensure that the findings have been addressed and, if necessary, follow-up with the NDIS participating

<sup>15</sup> “State, DA in dispute over cutting-edge DNA database”, available at

<https://www.wcvb.com/article/massachusetts-state-da-dispute-over-cutting-edge-dna-database/35568421>

<sup>16</sup> A copy of the Draft Use and Dissemination Agreement is attached hereto as Exhibit I.

<sup>17</sup> Federal DNA Identification Act of 1994 [34 U.S.C. §12592(b)]

<sup>18</sup> FBI Director’s *Quality Assurance Standards for Forensic DNA Testing and DNA Databasing Laboratories*” available at <https://www.fbi.gov/file-repository/quality-assurance-standards-for-forensic-dna-testing-laboratories.pdf/view> and <https://www.fbi.gov/file-repository/quality-assurance-standards-for-dna-databasing-laboratories.pdf/view>



laboratory. Laboratories participating in NDIS are required to be accredited in DNA analysis by a nonprofit professional association of persons actively involved in forensic science which is nationally recognized within the forensic science community. Accreditation is gained through adherence to the international ISO/IEC 17025:2017 requirements, as well as supplemental requirements of the accreditation body related specifically to forensic laboratories. That body is also responsible for complying with the Federal DNA Act, the Privacy Impact Assessment National DNA Index System (NDIS) Notice, February 24, 2004,<sup>19</sup> the provisions of the NDIS Memorandum of Understanding (including the sub-license to use the CODIS software), and the NDIS Operational Procedures.

The ISO/IEC 17025 has over 200 requirements and the FBI Director's *Quality Assurance Standards for Forensic DNA Testing and DNA Databasing Laboratories* has over 500 requirements that must be met. The standards include requirements for management, facilities, equipment, personnel, security, technical analysis, reporting and reviewing results, corrective action procedures, internal audits, ongoing proficiency testing, continuing education, and software security. External qualified assessors inspect the laboratory to confirm compliance with all requirements, issue a report of their findings, and require documented correction of any identified non-compliance.

The primary concern related to the quality of the data within the Bristol Forensic DNA Database is the accuracy of the information within the database. Since the information provided to the Bristol District Attorney was in hard copy, that data had to be manually entered into their database software. Manual data entry may result in transcriptional errors of both the DNA profile and the personal identifying information. If the DNA profile entered is not accurate, potential matches may not occur or false matches may be made. When a profile is matched, if the identity of the profile is not correct it may result in the wrong person being investigated for a crime in which they were not involved. If a confirmation of the match does not occur prior to indictment or prosecution it is possible for that person to be wrongfully convicted. The data entered in the database must be stringently reviewed and confirmed by two or more scientifically qualified personnel, to ensure that the data transfer review has been verified to be accurate and that all other relevant quality assurance measures have been followed.

The FSOB did not receive a response to questions concerning what, if any, verification procedures are used to ensure the accuracy of data in the Bristol Forensic DNA Database and, if data is removed or new data integrated into the database, whether there are any verification procedures to ensure that the accuracy of the remaining/new data is impacted by those changes. These two steps are imperative to confirm the reliability of the information used to

---

<sup>19</sup> E-Government Act of 2002, P.L. 107-347, and the accompanying guidelines issued by the Office of Management and Budget (OMB) on September 26, 2003; <https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/ndis>



investigate a crime. The FSOB infers from the Bristol District Attorney's lack of response that the office has not implemented any such policies or procedures.

### 3. Handling of Searches and Profile Comparisons

Searches of a database can be conducted in multiple ways, including: (a) for a direct match of all alleles identified; (b) for a partial match that allows mismatches within the genetic loci; (c) for a partial match that allows mismatches between genetic loci; or (d) for mismatches both within and between genetic loci.

Each search parameter will lead to different levels of identification of the contributor. A direct match may identify the contributor of the profile; partial matches within the genetic loci may identify parents or children of the contributor; partial matches between loci may identify siblings of the contributor; and partial matches between and within loci may identify cousins, aunts, or uncles. To understand the significance of each search and match criteria, analysts must have knowledge of genetics and the heritance patterns of DNA.

Forensic DNA analysts who conduct DNA profile matches must have, at minimum, a bachelor's degree in biology, chemistry, or other related forensic science. The degree must include coursework in biochemistry, genetics, molecular biology, and statistics. Analysts must also participate in a minimum of 6 months training within a forensic laboratory, undergo competency testing prior to conducting casework, and undergo external proficiency testing twice a year. The person determining if two profiles match must understand the science and process to ensure that the results are correct within scientific limitations. There is no indication that the Bristol District Attorney is requiring any training, continuing education, or competency testing for persons determining matches generated by the database. The FSOB infers from available information that the Bristol District Attorney has not implemented any training, education or competency requirements for the administration of its database.

#### 4. Confidentiality and Data Sharing with Outside Entities

Confidentiality concerns relate to the multiple levels of access to the database, the information retained, and the sharing of data with others. The ISO/IEC 17025 Section 4.2 and the FBI Director's *Quality Assurance Standards for Forensic DNA Testing and DNA Databasing Laboratories* (QAS) Section 11 define specific requirements related to maintaining the confidentiality of genetic and personal information. The QAS requires that laboratories have procedures "for the release of personally identifiable information in accordance with applicable State and Federal law" and "to ensure the privacy of reports, case files, DNA records and databases." The Federal DNA Act provides that:

- the unauthorized disclosure of individually identifiable DNA information stored in the NDIS is punishable by a fine not to exceed \$100,000; and
- obtaining DNA samples or DNA information, without authorization, is punishable by a maximum fine of \$250,000 or imprisonment for not more than one year or both fine and imprisonment.<sup>20</sup>

The DNA profiles stored in CODIS are identified by a unique number, not by personal identifying information. If a match occurs within the CODIS software, the laboratory staff must then marry the DNA profile with the personal information of the contributor held outside the software database. This is to protect the personal and genetic information if there is unauthorized access of the database. If the database itself is compromised, only the DNA profiles are obtained and the identity of the person is not revealed. If sample records are compromised, the genetic information is also not revealed. If the identity of the person is the sample identification in the database it is possible that profiles included two different people with the same or similar names, therefore the reported match may result in confusion of the actual identity of the suspect.

Disclosure of personal and/or genetic information to those who don't have authorized access to the information may have significant repercussions. If the information is disseminated verbally, there is no documentation as to whether the information is accurate. If the information is disclosed to someone who does not have the appropriate confidentiality or security clearance, it may be further disseminated, again with no way to determine the source of the information or its accuracy. The information in the database also should never be used for non-law enforcement purposes. Strict requirements and documentation are required to ensure the privacy of those whose information is included in the database.

---

<sup>20</sup> Federal DNA Act of 1994 ,34 U.S.C. §12593(c)(1), (2).

Specific protocols or procedures must be established to protect the confidentiality of the DNA profiles and information contained in a database. A database should not include names or other identifying information about the sources of the profiles. Measures must be in place to ensure that personal identifying information is shielded from those without authorized access to the data. And if profiles are to be anonymized, then documentation should define who is authorized to learn the identity of a profile that is matched as a result of a search.

The absence of any protocols and procedures to govern the confidentiality of DNA profiles contained within the Bristol Forensic DNA Database has profound implications for the Crime Lab. That is because, unlike most databases developed by non-forensic laboratories, the Bristol Forensic DNA Database is based entirely on DNA information that was generated by the Crime Lab. The Crime Lab is subject to stringent requirements related to the development and maintenance of its own DNA data. Misuse or inaccurate associations of the Crime Lab's data by the Bristol District Attorney may be misappropriately attributed to Crime Lab staff when the issue was not their fault. Much of the data released to the Bristol District Attorney is maintained in the Crime Lab's CODIS database. Release of Crime Lab data currently in CODIS may have severe repercussions for its' accreditation status and continued participation in CODIS.

While this general discussion talks about Y-STR DNA profiles that are currently not uploaded to NDIS, data released by the Crime Lab also included autosomal STR DNA profiles that are uploaded to NDIS. Prior to receiving the CODIS software, the Designated State Official must sign the NDIS Memorandum of Understanding (MOU), and the Designated State Official must ensure the compliance of its laboratory with federal law and the NDIS Operational Procedures. The MOU provides, in relevant part:

- The generation of DNA data and/or a DNA database for dissemination beyond the purposes authorized by the Federal DNA Act [34 U.S.C. §12592(b)(3)] shall be considered an unauthorized use of the CODIS software. Similarly, the generation of DNA data and/or a DNA database consisting of such **DNA data for dissemination to individuals, entities, agencies, or laboratories other than NDIS Participating Laboratories shall be considered an unauthorized use of the CODIS software.**
- The NDIS Participating Laboratory agrees to comply with the limited access and disclosure provisions of the Federal DNA Act. The NDIS Participating Laboratories in states that may have more expansive provisions in their State laws relating to access and disclosure of DNA analysis and/or records **agree to abide by the more restrictive provisions in Federal law in order to participate in NDIS.** NDIS will not accept DNA analyses from any NDIS Participating Laboratories that fail to comply with these restrictions.

- The NDIS Participating Laboratory shall not provide access to or disclosure of DNA records that have been uploaded to NDIS to an entity or agency that is not a criminal justice agency nor authorized to access such DNA records under the Federal DNA Act. **If the NDIS Participating Laboratory disseminates, provides, or releases DNA records that have been uploaded to NDIS for purposes not authorized under the Federal DNA Act or to an entity or agency other than another NDIS Participating Laboratory or criminal justice agency, the NDIS Participating Laboratory shall notify the FBI and remove those DNA records from NDIS.**
- In accordance with the Federal DNA Act, disclosure of DNA records at NDIS is authorized for law enforcement identification purposes to the **Federal, State and Local criminal justice agencies who participate in NDIS.**

The National DNA Index System (NDIS) System of Records Notice<sup>21</sup> explains what disclosures of DNA records are authorized for laboratories participating in NDIS. **Specifically, direct disclosures of NDIS records are authorized to the Federal, State, and local criminal justice agencies who participate in NDIS.** These direct disclosures would include access to the DNA record contributed to NDIS if NDIS identifies a potential match. A secondary or indirect disclosure of a DNA record is permitted to law enforcement agencies for criminal identification purposes. The secondary or indirect disclosure generally encompasses the release of information to a law enforcement agency following the confirmation of a match.

It may be argued that since the Bristol District Attorney only publicly speaks about a Y-STR database, that concerns related to the Crime Lab's NDIS participation are not relevant but they are also in possession of autosomal STR DNA profiles. Given the lack of disclosure by the Bristol District Attorney concerning what they are doing with all of the data received, it is not clear if the Crime Lab is in violation of their NDIS MOU. Further investigation must be conducted to confirm if the release of the Crime Lab's DNA data to the Bristol District Attorney is an unauthorized use of the CODIS software which will result in the Crime Lab's DNA profiles currently at NDIS to be removed and/or the loss of Crime Lab's CODIS access. As an LDIS laboratory submitting DNA profiles to the Crime Lab's SDIS database, the Boston Police Department Crime Laboratory's DNA profiles may also be removed from NDIS. The Boston Police Department Crime Laboratory has responded to questions from the FSOB indicating that they have not received any requests from any Massachusetts agency to provide DNA profiles and have not provided any such profiles. NDIS contains over 14,541,796 offender profiles, 4,341,864 arrestee profiles and 1,103,683 forensic profiles as of April 2021. Table 1 is a summary of Massachusetts data currently residing at NDIS.

---

<sup>21</sup> Federal Register, Vol. 61, no. 139; July 18, 1996

Table 1. Massachusetts NDIS Information<sup>22</sup>

Samples included in NDIS database	Total
Offender Profiles	154,367
Arrestee	0
Forensic Profiles	14,107
NDIS Participating Laboratories - MA State Police Crime Laboratory (SDIS) - Boston Police Department Crime Laboratory (LDIS)	2

Massachusetts State Police Crime Laboratory is accredited to the ISO/IEC 17025:2017 and ANAB AR3125 standards by the ANSI National Accreditation Board (ANAB), certificate number FT-0331. Section 4.2 of the ISO/IEC 17025 addresses requirements related to confidentiality. This section includes the following requirements:

- 4.2.1 If the laboratory places a customer's<sup>23</sup> information in the public domain, it must inform the customer in advance.
- 4.2.2 If the laboratory is required by law to release confidential information, its customers\* must be notified, unless prohibited by law.
- 4.2.4 External bodies or individuals acting on the laboratory's behalf must keep confidential all information of laboratory activities, except as required by law.

In response to the FSOB questions to the crime lab concerning the release of information to the Bristol District Attorney on May 20, 2021, the laboratory was asked whether it had notified its accrediting body of Significant Changes, Events, and Nonconformities as required under the ANAB accreditation policies.<sup>24</sup> The laboratory responded:

"The laboratory notified the ANAB accreditation manager of the Grand Jury subpoena and advised ANAB that we are currently working to determine if we are legally permitted to notify our customers (e.g., original submitting agency) of the release of data without violating the terms of the Grand Jury. ANAB has acknowledged [the Crime Lab's disclosure and advised the Laboratory that **further communication will be needed only if [the Crime Lab] is ultimately unable to meet their accreditation requirements**

<sup>22</sup> See <https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics>

<sup>23</sup> ISO defines a "Customer" as a person or organization that receives a service that is intended for this person. Crime Lab "customers" are the individual law enforcement agencies that submit evidence to the crime lab for DNA testing. See ISO 9000:2015 Quality management systems – Fundamentals and vocabulary.

<sup>24</sup> ANAB MA 3033 Accreditation Manual for Forensic Service Providers, effective 2020/9/22

(e.g., notification of customer release of confidential information) due to grand jury restrictions.”

The accreditation body’s response indicates a concern that if the Crime Lab is not allowed to notify its customers that its information was provided to someone outside of the submitter’s agency, it may not be compliant with accreditation requirements.

#### 5. Y-STR Analysis Limitations

In order to fully understand the scientific implications of the present effort by the Bristol District Attorney to establish an unregulated database of Y-STR DNA records, it is important to understand the unique features of Y chromosome STR testing, and why a database of Y-STR profiles, in particular, poses a threat to the integrity of forensic science in the Commonwealth. Y chromosome STR testing was first developed to remedy the problem of being unable to amplify a small amount of male DNA in the presence of large amounts of female DNA. This problem most commonly arises when analyzing sexual assault evidence. Testing of typical sexual assault samples is successful because epithelial cell originating from a victim can be broken open, releasing their DNA, under chemical conditions which will not break open sperm cells. Once the female DNA is removed the DNA from sperm cells is recovered. In some circumstances the sperm breaks open too early in the procedure resulting in a DNA mixture. In this circumstance, the amount of female DNA may overwhelm the PCR reaction with little or no STR information being obtained from the male DNA.

PCR reactions designed to amplify STR loci found only on the Y chromosome produce detectable results even in the presence of large amounts of female DNA. Thus, amplification of Y-STR loci is the method of choice when analyzing forensic casework where a small amount of male DNA is present in a mixture with a large amount of female DNA. In these situations, useful data can be obtained using Y chromosome STR testing. The Y-STR testing kit used by the Crime Lab amplifies 17 loci.

However, there are important and significant differences between normal (autosomal) STR testing which now uses 27 loci including 3 Y-STR loci. These differences are related to the biology of genetic recombination which occurs prior to the production of sperm and eggs. STR loci are found on all human chromosomes. Alleles at each STR locus are randomly transmitted to offspring, with the exception of the alleles at STR loci on the X and Y chromosomes. This means that the alleles inherited at one STR locus are passed to a child independently of alleles at any other STR locus. In a sense, the parental alleles are “shuffled” during production of sperm and egg, so a child is not identical to either parent or other children of the same parents.

However, this “shuffle” or recombination does not occur for STR loci on the Y chromosome. The Y chromosome is inherited, in its entirety, from father to son. The STRs on the Y chromosome are inherited from father to son and are unchanged in the length of the DNA. Thus, in a given family, the Y chromosome is inherited “as is” from grandfather to father to son and the sons of sons without the recombination “shuffled of alleles”. While an autosomal STR test kit amplifying 27 STR loci can identify a specific person with an extremely high degree of certainty, testing with Y-STRs cannot. Using 17 Y-STR loci to test DNA from evidence will produce a Y-STR profile which can be matched to the male whose DNA is on the evidence. However, that “DNA match” between the Y-STR data obtained from evidence and a known person is not an “identification,” but instead, the “match” identifies a male individual and all the males in that lineage (family). That lineage is the line of males that carries that same Y chromosome and will identify grandfathers, fathers, uncles, brothers, and all sons in that male lineage.

Therefore, testing with Y chromosomal STRs can produce multiple false positive results to people in the same lineage as the true DNA contributor.<sup>25</sup> An additional problem is caused by the more complicated molecular nature of some of the Y chromosomal STR loci. Mutations at a locus can result in the appearance of multiple alleles at a locus or null (no alleles) at a locus. To assist laboratories, Y-STR interpretation guidelines have been published by the Scientific Working Group on DNA Analysis Methods (SWGDM) in 2014<sup>26</sup> and by the DNA Commission of the International Society of Forensic Genetics in 2020.<sup>27</sup>

The numeric allele designation data for Y-STR profiles held in a database do not contain the same level of information that is available from the Y-STR DNA profile electropherogram. Additionally, while the two commonly used current kits test either 27 or 23 Y STR loci, previous kits have tested fewer loci (17 or 12 loci) where evidence profile data could match to a greater number of profiles depending on the test kit used.

---

<sup>25</sup> The dangers of a false positive result are far from theoretical. In one recent case, a Rhode Island man was wrongfully accused and charged in connection with an unsolved 1988 murder of a ten-year-old Pawtucket girl, after investigators identified him as having a Y-STR profile that was “consistent” with the Y-STR profile developed from crime scene evidence. <https://www.providencejournal.com/news/20200204/charge-dismissed-against-man-accused-of-murdering-10-year-old-pawtucket-girl>

<sup>26</sup> SWGDM Interpretation Guidelines for Y-Chromosome STR Typing, available at [http://media.wix.com/ugd/4344b0\\_da25419ba2dd4363bc4e5e8fe7025882.pdf](http://media.wix.com/ugd/4344b0_da25419ba2dd4363bc4e5e8fe7025882.pdf)

<sup>27</sup> Roewer L., Andersen MM., Ballantyne J., Butler JM., Caliebe A., Corach D., D'amato ME., Gusmão L., Hou Y., De K., Parson W., Prinz M., Schneider PM., Taylor D., Vennemann M., Willuweit S. (2020), “DNA commission of the International Society of Forensic Genetics (ISFG): Recommendations on the interpretation of Y-STR results in forensic analysis,” *Forensic Sci. Int. Genet.* 48, 102308.

There are multiple reliable sources of population data for use in profile frequency calculation.<sup>28</sup> These databases - which have been developed over the last 20 years - contain also samples tested with differing numbers of Y-STR loci. There are several accepted calculation methods for estimation of the rarity of a Y-STR loci match. These methods are discussed in the guidelines mentioned above and require a thorough understanding for choice and use of method.

Expertise is needed related to the Y-STR test kit, known mutations, and the associated scientific literature to interpret Y-STR DNA profiles and associated comparisons. To understand the science of the Y-STR testing results, it is imperative for the interpretation of such matches be done by scientists who have training in genetics. However, there is no indication that the Bristol District Attorney's Office utilizes individuals who are scientifically qualified to review and interpret Y-STR data.

### **CONCLUSION & RECOMMENDATIONS**

- The Bristol Forensic DNA Database threatens the integrity and reliability of forensic science in the Commonwealth of Massachusetts.
- Since at the current time, this FSOB has no independent enforcement power, we believe that the Attorney General should take steps to enjoin the Bristol DA from unlawfully disseminating personal data.
- G.L. c. 22E sec. 10 should be amended to explicitly prohibit the aggregation of DNA records for inclusion in an external, unregulated DNA record database. The FSOB specifically notes that, although S1595 seeking to amend that statute does contain language that prohibits the aggregation of DNA data by entities outside of the Crime Lab, this prohibition is offered in the context of proposing the addition of a brand new subsection, G.L. c. 22E, sec. 10A, and does not also propose any modifications to the language of subsection 10.

---

<sup>28</sup> Y-Chromosome Haplotype Reference Database (YHRD) <https://yhrd.org/>  
Willuweit, Sascha & Roewer, Lutz. (2014). The New Y Chromosome Haplotype Reference Database. Forensic science international. Genetics. 15. 43-48. 10.1016/j.fsigen.2014.11.024.



## TABLE OF EXHIBITS

- A. District Attorneys' Letter to FSOB (1.27.21)
- B. MACDL ACLUM Letter to FSOB (2.10.21)
- C. FSOB Motion (2.10.21)
- D. FSOB Letter to FSOB Chairperson (4.27.21)
- E. FSOB Questions to Bristol DA (5.7.21)
- F. FSOB Questions to MSPCL (5.7.21)
- G. MSPCL Response to FSOB Questions (5.20.21)
- H. FSOB Letter to DA Quinn (5.24.21)
- I. Draft Data Use and Dissemination Agreement (1.25.21)



THE COMMONWEALTH OF MASSACHUSETTS

OFFICE OF THE  
DISTRICT ATTORNEY

CAPE & ISLANDS DISTRICT

MICHAEL D. O'KEEFE  
DISTRICT ATTORNEY

**Exhibit A**

3231 MAIN STREET  
P.O. BOX 455  
BARNSTABLE, MA 02630  
(508) 362-8113

January 27, 2021

Kerry A. Collins, Chair  
Forensic Science Oversight Board  
Undersecretary of Forensic Science and Technology  
Executive Office of Public Safety and Security  
1 Ashburton Place  
Boston, MA 02108

Dear Chair Collins and Board Members,

We understand that the Forensic Science Oversight Board's (FSOB) has been asked to weigh in on specific familial DNA legislation, and in the process, was discussing the use of Y-STR testing. Thank you for the opportunity to provide information relative this important investigative tool that helps bring justice to victims of unsolved violent crimes.

Since 2003, the Massachusetts State Police Crime Laboratory, (MSPCL), has been conducting Y-STR testing on thousands of biological samples submitted to the lab. This biological evidence is frequently recovered from a victim's body using a sexual assault collection kit and/or recovered from other evidence left at a crime scene. In many sexual assault cases, traditional STR testing is not effective because the samples produce a mixture of the victim's DNA and the perpetrator's DNA. In traditional STR analysis, the victim's DNA can overwhelm the male perpetrator's DNA and the perpetrator's STR profile cannot be determined. In those cases, Y-STR is used instead as it allows the analyst to extract the Y (male) DNA from the mixture and develop a profile for just the male perpetrator. This type of testing has been scientifically accepted and used in the courts across the country, including Massachusetts, for the last eighteen years. During this time, the MSPCL has provided, as required, a copy of Y-STR reports to the submitting police department and/or the District Attorney's Office. However, these Y-STR reports, which contain a series of sixteen numbers, are not useful to investigators attempting to identify an unknown/unidentified suspect. Until now, no effort has been made to attempt to use the information provided in these reports to compare it to the thousands of other unknown profiles from biological material where similar Y-STR testing was performed. The time is long overdue for our investigators to make use of these Y-STR reports for their intended purpose, i.e. to identify unknown perpetrators of violent crimes.

The Lab's obligation to furnish the reports to the District Attorney's Offices is clear. ("The director shall furnish records in his possession, including DNA records and analysis, to police departments in cities and towns, to the department, to the department of correction, to a sheriff's department, to the parole board or to prosecuting officers within the commonwealth upon request in writing or electronically.") The Commonwealth's District Attorneys' Offices are

criminal justice agencies seeking the Y-STR reports for legitimate law enforcement purposes. Specifically it is our goal to identify the perpetrators of sexual assaults in unsolved investigations in the Commonwealth.

The use of a spread sheet to compare Y-STR reports does not violate M.G. L. c. 22E. That statute pertains to the state maintained STR database which is made up of STR records. The District Attorneys have repeatedly indicated that the use of Y-STR information is for investigative leads in unsolved homicides, rapes, and other serious violent crimes. These Y-STR reports have been provided to the police and District Attorneys' Offices for years but the information has largely been unusable except when a suspect has been identified. As a result, Y-STR reports have not been effectively used to identify the unknown perpetrators responsible for the thousands of unsolved violent crimes. To date, the involved District Attorneys' Offices have made a request for all of their Y-STR reports to get an accurate list of every case where this testing was used. The District Attorneys are not asking the lab to do anything other than provide these readily available Y-STR reports. The District Attorneys have made it perfectly clear that their intent is to pool resources to use this, already tested and available information, to solve these crimes.

These District Attorneys have a shared interest in identifying unknown perpetrators of violent crimes in their respective counties. The Y-STR reports have simply been placed in a searchable spreadsheet so that unknown individuals can now be identified or connected to other unsolved cases. There is nothing inappropriate with compiling this information in this manner to make it usable and efficient. The searchable Y-STR spreadsheet is needed so that Y-STR information can actually be used for its intended purpose, i.e. to assist in identifying the unknown perpetrators of these violent crimes. To date, only one unknown Y-STR profile from a different county was compared with the Bristol District Attorney's searchable spreadsheet. In that case, although the unknown perpetrator was linked through CODIS to multiple rapes and the homicides of two women, he was not identified. As a result, this case has remained unsolved for several years as there was no other way to identify him. However, within seconds of submitting the Y-STR profile of this individual to the Bristol County Y-STR spreadsheet, his profile was matched to a Bristol County rapist. This simple and undoubtedly proper comparison has now provided investigators with a significant investigative lead to pursue in that case.

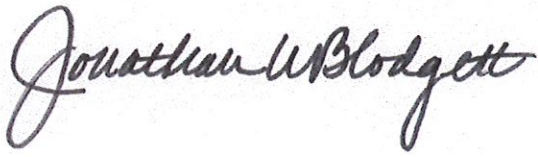
Sincerely,

A handwritten signature in black ink, appearing to read "Michael O'Keefe". The signature is fluid and cursive, with a large, stylized initial "M" and "O".

Michael O'Keefe

Cape and Islands District Attorney





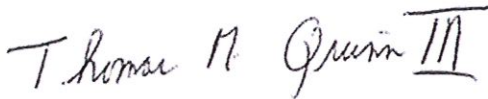
Jonathan W. Blodgett  
Essex District Attorney



Timothy Cruz  
Plymouth District Attorney



Joseph D. Early, Jr.  
Worcester District Attorney



Thomas M. Quinn III  
Bristol District Attorney



David E. Sullivan  
Northwestern District Attorney

February 10, 2021

Kerry A. Collins, Chair  
Forensic Science Oversight Board  
Undersecretary of Forensic Science and Technology  
Executive Office of Public Safety and Security  
1 Ashburton Place  
Boston, MA 02108

Dear Chair Collins and Board Members:

We write on behalf of the Massachusetts Association of Criminal Defense Lawyers (MACDL) and the American Civil Liberties Union of Massachusetts (ACLU) to express our alarm about the legal and policy implications of an effort by several district attorneys that, if successful, would effectuate an end run around the statutory framework that protects genetic data and privacy. We understand that the Forensic Science Oversight Board has scheduled an emergency meeting on February 10, 2021, to address a pending effort by six district attorneys to compel the Massachusetts State Police Crime Laboratory (MSP Lab) to produce multi-county, aggregated DNA/Y-STR profiles. The question for the Board, as we understand it, is whether granting this request would raise legal concerns under G.L. c. 22E, the State DNA Database statute, and G.L. c. 66A, the Fair Information Practices Act. It would.

MACDL and ACLU were involved in *Landry v. Attorney General*, 429 Mass. 336 (1999), which considered the constitutionality of G.L. c. 22E, and ACLU served as counsel for the plaintiff in *Amato v. District Attorney for Cape and Dist.*, 80 Mass. App. Ct. 230 (2011), which challenged the legality of the MSP lab's retention of an individual's DNA profile that was collected voluntarily (for elimination purposes) as part of a criminal investigation. As described below, neither case supports the district attorneys' position.

This Board has broad authority to provide enhanced, objective and independent auditing and oversight of forensic evidence and forensic services in criminal matters in the Commonwealth. G.L. c. 6, sec. 184(A)(a). For the reasons below, we urge the Board to exercise that authority to formally oppose the requested disclosure of aggregated Y-STR records.

## **1. The District Attorneys' reliance on G.L. c. 22E is misplaced.**

Chapter 22E of the Massachusetts General Laws, entitled "STATE DNA DATABASE," confers upon the Massachusetts State Police—and no other entity—the authority to maintain and implement rules regarding a state DNA database. Like its title, the Act's structure sets forth various rules governing the creation, maintenance, confidentiality, and security of the DNA database. Nevertheless, six district attorneys now argue that *one* phrase in *one* subsection of this Act has the effect of compelling the state's DNA database director to enable any law enforcement or prosecuting agency in Massachusetts to create their own database of genetic material, specifically Y-STR reports. This reading of Chapter 22E is at odds with the statute's structure and could undermine its constitutionality.

The six district attorneys focus on G.L. 22E, § 10(a), which states that the DNA database director “shall furnish records in his possession, including DNA records,” to law enforcement and prosecutors. The district attorneys state that they wish to “pool” thousands of Y-STR reports into a spreadsheet—this appears to be a way of saying “database of genetic material”—which they would then use to develop investigative leads.

However, in interpreting a subsection of a larger legislative act, courts “‘do[] not determine the plain meaning of a statute in isolation’ but rather in ‘consideration of the surrounding text, structure, and purpose of the Massachusetts act’ from which th[e] subsection is derived.” *New England Power Generators Ass’n, Inc. v. Dep’t of Env’tl. Prot.*, 480 Mass. 398, 410–11 (2018) (quoting *ENGIE Gas & LNG LLC v. Department of Pub. Utils.*, 475 Mass. 191, 199 (2016)). Thus, rather than interpret bits of text in isolation, the Supreme Judicial Court may seek guidance in its “surrounding text and structure.” *Id.* at 411.

These principles cut against the district attorneys’ proposed interpretation of Subsection 10(a). Nothing in the text, structure, and purpose of Chapter 22E as a whole suggests that, in empowering the MSP to maintain a state DNA database, the legislature also commanded the MSP to assist individual law enforcement and prosecuting agencies to create *altogether different* genetic databases of their choosing nor to release, *en masse*, the type of records the district attorneys now seek. None of the other subsections of Chapter 22E mention such a database or indiscriminate records release, let alone say what rules would govern it.

Thus, not surprisingly, the Supreme Judicial Court has already looked to the “surrounding text, structure, and purpose” of Chapter 22E when reviewing Subsection 10(a). In *Landry*, the Supreme Judicial Court held that the involuntary collection of blood samples of certain convicted offenders, pursuant to G.L. c. 22E, § 3, did not violate constitutional protections against unreasonable searches and seizures, “in light of [a convicted person’s] diminished privacy rights.” *Landry*, 429 Mass. at 347. In its opinion, the Court noted that Subsection 10(a) referenced the distribution of “records in [the director’s] possession, including DNA records and analysis.” *Id.* at 353 n.18. But the Court rejected an expansive reading of that phrase. Consistent with the surrounding, text, structure, and purpose of Chapter 22E, the Court “rest[ed] on the assumption that, because an analysis and record, by definition, may only consist of ‘numerical identification information,’ derived from a DNA sample, *a department’s request for any reason cannot reveal other private and protected information.*” *Id.* (emphasis added)

This language from *Landry* signals that, in light of Chapter 22E as a whole, the distribution command in Subsection 10(a) compels the director of the state DNA database to distribute records only if they are “derived from a DNA sample,” and only if they “cannot reveal other private and protected information.”

A contrary conclusion would put Chapter 22E's constitutionality in serious doubt. As the district attorneys appear to acknowledge, they seek Y-STR reports that are not limited to individuals who have been convicted of an offense enumerated in G.L. c. 22E, § 3, and whose expectations of privacy therefore have been deemed to be diminished under *Landry*. In fact, the district attorneys forthrightly say that Y-STR analysis is used at the *investigatory* stage of a case, and presumably would include the following classes of persons, *none of whom* are required to provide DNA for the database:

- *Suspects* who have not yet been convicted of a crime, including those who are ultimately *excluded* as the source of male DNA and/or acquitted of the underlying crime.
- Male *victims* who voluntarily provide elimination samples.
- Male *family members, co-habitants, and other individuals* who voluntarily provide elimination samples.
- Male EMTs, police, medical examiners, crime scene responders, and other individuals who are required to provide elimination samples due to possible contact with the crime scene evidence.

Moreover, Y-STR analysis necessarily implicates the privacy of a much larger group of people than autosomal STR testing, because all males from the same paternal lineage (brothers, fathers, sons, cousins) share the same Y-STR profile. Thus, obtaining Y-STR records could give the district attorneys the genetic information of many more people than just convicted offenders. Because the resultant ad hoc Y-STR would raise serious constitutional questions, the district attorney's preferred interpretation of Subsection 10(a) should be rejected if it is "fairly possible" to do so. *Commonwealth v. Jones*, 471 Mass. 138, 143 (2015) (quoting *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 69 (1994)).<sup>1</sup>

**2. The District Attorneys' request has serious privacy implications and threatens to create the very sort of "shadow database" at the heart of the controversy surrounding the *Amato* case.**

In *Amato*, the Appeals Court held that the plaintiff stated claims against the state defendants for "in essence, maintain[ing] a shadow DNA database outside the statutorily authorized State convicted offender database governed by G.L. c. 22E, and the FBI's CODIS database." 80 Mass. App. Ct. at 236. *Amato* was one of between 150 and 200 men who conditionally and voluntarily provided DNA samples as part of a criminal investigation. *Id.* at 232. After the perpetrator was identified, charged and convicted, *Amato* sought to have his DNA sample destroyed and his profile permanently removed from the MSP lab's

<sup>1</sup> We acknowledge that the lab may have separate obligations, *see, e.g.*, Mass. R. Crim. P. 14, to provide results of a Y-STR analysis as exculpatory evidence to prosecuting agencies and defendants in individual criminal cases. However, neither these obligations nor Chapter 22E would seem to authorize the wholesale release of aggregated Y-STR data nor the retention of those records in a separate, unregulated database.

records. *Id.* at 233. On appeal, the court concluded that the maintenance of Amato’s DNA sample raised concerns under the Fair Information Practices Act, G.L. c. 66A, § 2(l), and the Privacy Act, G.L. c. 214, § 1B. *Id.* at 236-41. In so doing, the Court noted the lack of safeguards against the disclosure of Amato’s DNA information, such as the criminal sanctions for the unauthorized disclosure, as provided by G.L. c. 22E, §§ 12-13. *Id.* at 241 n.21.

The district attorneys’ request for aggregated Y-STR records resembles the “shadow database” at issue in *Amato*. The district attorneys seek to create apparently unregulated databases of sensitive Y-STR records in order to conduct forensic searches for investigatory links to unsolved crimes. But, as in *Amato*, retaining “highly sensitive DNA records . . . for nonconsensual use in other criminal investigations” may give rise to claims for “an unreasonable, substantial, and serious interference” with privacy. *Id.* at 241.

And for good reason. The district attorneys describe the database as a spreadsheet that will contain the numerical data provided by the lab, but it is unclear what rules, in their view, would govern questions like the following:

- How will data be imported or entered into the spreadsheet?
- Who will have access to the spreadsheet?
- Will there be different levels of access, as there are at the lab, with only certain personnel who are authorized to edit/alter data in the spreadsheet?
- How will new information and data be integrated into the spreadsheet over time?
- How will information be removed from the spreadsheet? Is there a method for an individual to have their Y-Profile expunged?
- Will those with access to the spreadsheet be required to undergo training?
- What, if any, verification procedures will there be to ensure the accuracy of data?
- What measures are in place to ensure that personal identifying information is shielded from those with access to the data? (akin to CODIS, where the known profiles developed from offender profiles are assigned unique identifying numbers)
- If there is a database breach, will people in the database be notified?
- How will a defendant know if they became a suspect as a result of a search in this database? Would it be subject to discovery? If an adjudicated case hit to a known that does not match the defendant are they notified?
- What measures are in place to ensure that information in the database is not used for purposes other than investigation into unsolved crimes?

As in *Amato*, the records sought by the District Attorney are not “offender” records and are not part of the statewide CODIS database. Given *Amato*’s recognition of the privacy implications that flowed from the *lab*’s retention of non-database DNA records, it is unclear, especially based on the limited information presently available to MACDL and ACLUM, how



the district attorneys' proposed course of action will respect all potentially applicable privacy laws.

Respectfully submitted,

/s/ Victoria Kelleher  
MACDL President  
Law Office of Victoria Kelleher  
One Marina Park Drive  
Suite 1410  
Boston Ma 02210

/s/ Matthew R. Segal  
/s/ Jessica J. Lewis  
American Civil Liberties Union  
Foundation of Massachusetts, Inc.  
211 Congress Street  
Boston, MA 02110  
(617) 482-3170

/s/ John H. Cunha Jr.  
Former MACDL President  
Cunha & Holcomb, P.C.  
1 State Street, Suite 500  
Boston, MA 02109-3507  
(617) 523-4300

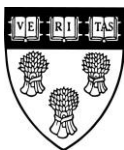
# Exhibit C

Forensic Science Oversight Board

February 10, 2021

Motion that the board takes a position against the lab providing the YSTR information requested because interpreting the statute to authorize or compel the release of YSTR records risks the MSPCL's loss of accreditation status and risks being out of compliance with NDIS and risks violation of the plain language of 22E and 66A and we urge the AGO to bring the FSOB's position before the court hearing the subpoena. The board is in the midst of studying these issues and the legal and scientific implications and attaches MACDL/ACLU and the DAO's letter.

Motion was made by Judge Gertner. Lisa Kavanaugh seconds the motion. Two members abstained from voting. The remaining members voted in favor of the motion.



## HARVARD LAW SCHOOL

CAMBRIDGE · MASSACHUSETTS · 02138

**HON. NANCY GERTNER**

*Senior Lecturer of Law*

*United States District Court (Ret.)*

LANGDELL 328

TEL: 617-496-4099

FAX: 617-496-4863

E-MAIL: [ngertner@law.harvard.edu](mailto:ngertner@law.harvard.edu)

April 27, 2021

Kerry Collins

Undersecretary for Forensic Science

Commonwealth of Massachusetts Executive Office of

Public Safety and Security

Boston, Massachusetts 02108

Dear Kerry:

We are writing to request that our agenda this Friday include a discussion about our Board's institutional relationship to the Executive Office of Public Safety and Security (EOPSS) and the Massachusetts State Police Crime Laboratory (MSPCL).

As you know, the Working Group on Familial DNA spent a considerable amount of time researching and preparing our report on familial DNA and unregulated databases. We discussed our preliminary findings with the Board in December 2020, heard comments from the public and invited speakers at our January 27, 2021 meeting, and incorporated the oral and written feedback from Board members and stakeholders into the final version of our report, which we presented to the board on March 24, 2021. The Working Group was representative of the many stakeholders on this issue. Our recommendations with respect to familial DNA were adopted unanimously by the Board, and our recommendations with respect to unregulated databases was adopted with all members of the board voting in favor and one abstention.

But as we learned in January, there was already a parallel effort being made by a group of elected district attorneys, one that was working at cross purposes to the Working Group's efforts and in a manner fundamentally at odds with the Board's concerns about unregulated DNA databases. While we clearly do not know all the details, the following seems clear: By the time our Working Group commenced its work, the Bristol County DA's office had already secured a grand jury subpoena to compel the MSPCL to produce aggregated Y-STR records. We can only presume (because we have not been granted access to any of the relevant pleadings or rulings) that the Bristol DA ostensibly sought the subpoena to aid in the grand jury's investigation of the specific unsolved case that was the subject of the grand jury investigation. However, as the letter provided to the board on January 27, 2021 made clear, the Bristol County DA's purpose in seeking aggregated Y-STR records was actually far broader than the demands of that one grand jury investigation. In that letter, the signatories described a plan to establish what the FSOB report has since defined – and *condemned* – as an unregulated database. The DA's letter expressed an intent to use the information contained in the MSPCL records “to compare it to the thousands of other unknown profiles from biological material where similar Y-STR testing was

performed.” It referred to the “Commonwealth’s District Attorneys’ Offices” proposal to use Y-STR records to develop “investigative leads in unsolved homicides, rapes, and other serious violent crimes,” and to create an “accurate list of every case where this (Y-STR) testing was used.” The DA’s intent is unambiguous: “to pool resources to use this, already tested and available information, to solve these crimes.”

You indicated that there was no time to discuss the January 27 letter at our meeting. Accordingly, we called for an emergency meeting on February 10, 2021. During the meeting, we learned that the Attorney General’s Office (AGO) had moved on behalf of the MSPCL to quash the grand jury subpoena, and that a trial court judge had denied the motion to quash. We also discussed the concerns raised by MACDL and the ACLUM, including the risk that the planned database could violate G.L. c. 22E and also that it could violate G.L. c. 66A, the Fair Information Practices Act (FIPA). After learning of the motion to quash and discussing the concerns raised by Board members and external stakeholders, the Board passed the following resolution:

*Motion that the board takes a position against the lab providing the YSTR information requested because interpreting the statute to authorize or compel the release of YSTR records risks the MSPCL’s loss of accreditation status and risks being out of compliance with NDIS and risks violation of the plain language of 22E and 66A and we urge the AGO to bring the FSOB’s position before the court hearing the subpoena. The board is in the midst of studying these issues and the legal and scientific implications and attaches MACDL/ACLU and the DAO’s letter.*

In the six weeks leading up to the next Board meeting, the Working Group continued to work on and finalize its Report on familial DNA, which ultimately included a lengthy discussion of the perils of unregulated DNA databases such as that planned by the Bristol District Attorney. At the March 24 meeting, we learned that the AGO had filed a motion to reconsider in which it provided the Court with a copy of the board’s motion and the stakeholder letters. We also learned that the trial court judge had denied the motion to reconsider. EOPSS was unable to state whether the AGO intended to file an appeal.

In the intervening month since the board last met, I and others have independently urged the AGO to reconsider its decision and to file an appeal from the denial of the motion to quash. The AGO has declined to do so. We do not know the basis for that decision, nor do we know the breadth of the trial judge’s ruling because the grand jury proceedings were confidential. However, the net effect of the above proceedings is to undermine both the FSOB’s February motion, and the far more detailed recommendations and concerns embodied in the March 24, 2021 report.

An appeal here was critical, as it would have allowed the Appeals Court to reach the serious concerns raised by the FSOB and other stakeholders in a public forum, with grand jury information redacted. Notwithstanding the confidential nature of grand jury proceedings, the Appeals Court routinely reaches legal challenges to the procedure and substance of grand proceedings, as evidenced by the sheer number of reported appellate decisions that contain the heading “In Re Grand Jury Proceedings.”

On the merits, we believe that even putting aside the legality of the Bristol DA’s planned database under G.L. 22E, the plan to aggregate and store Y-STR records in a searchable database clearly violates G.L. c. 66A. Specifically:

- **The YSTR records that the Bristol DA’s office has requested (and already obtained, for their own county and possibly Plymouth) are quintessential “personal data” within the meaning of G.L. c. 66A §1.** (“any information concerning an individual which, because of name, identifying number, mark or description can be readily associated with a particular individual”);
- **The Bristol DA’s office meets the statutory definition of an “agency” under the meaning of G.L. c. 66A** (“any agency of the executive branch of the government, including but not limited to any constitutional or other office, executive office, department, division, bureau, board, commission or committee thereof”);
- **The Bristol DA has *already* become a “holder” of personal data as to YSTR records from Bristol County (because the lab has already provided them with YSTR records from Bristol), and it has expressed its intent to become a “holder” of personal data (YSTR records) from other counties, as soon as those records are produced by the lab** (“holder” defined as “an agency which collects, uses, maintains or disseminates personal data or any person or entity which contracts or has an arrangement with an agency whereby it holds personal data as part or as a result of performing a governmental or public function or purpose”);
- **The Bristol DA made clear, in his Jan. 27, 2021 to the FSOB, that he intends to aggregate the YSTR records he obtains from the lab into a searchable database to investigate unsolved crimes.** This plan explicitly contemplates sharing information with other counties and with police department. The planned sharing of data with these outside agencies clearly constitutes a violation of G.L. c. 66A §2(c), which states that a holder of personal data **shall not** “allow any other agency or individual not employed by the holder to have access to personal data unless such access is authorized by statute or regulations which are consistent with the purposes of this chapter require.”
- **G.L. c. 214 §3B provides for civil remedies, including injunctive relief, where any holder of personal data “violates or proposes to violate any of the provisions of chapter sixty-six A”**

It is abundantly clear that the Bristol DA’s plan to create an unregulated database of YSTR records for use in an untold number of criminal investigations in an untold number of counties across the state is actionable under G.L. 214. Consequently, we believe an original action should be brought under G.L. 214 §3B to enjoin the Bristol DA’s office from using or disseminating records already obtained. We further believe that the lab should be enjoined from releasing any additional records without a Use & Dissemination agreement that limits its use to the grand jury investigation for which the records were subpoenaed.

As far as this Board is concerned, and its independent obligations under the authorizing statute, we request that the following motions be presented to the Board for a vote:

- (1) Requesting that the AG’s office report to the Board regarding its decision not to appeal the denial of the motion to quash the grand jury subpoena, including any recommendations made to it by EOPPS and/or the MSPCL.

- (2) Resolving that the Bristol District Attorney's Office is a forensic service provider within the meaning of our enabling statute, as to the administration of its planned Y-STR database, and as such is subject to the Board's oversight authority.
- (3) Requesting that the MSPCL provide the Board with signed copies of any and all Use & Dissemination Agreements signed by the Bristol District Attorney's Office with respect to the Y-STR records it has already received.
- (4) Pursuant to M.G.L. c. 6 §184 A (d), requesting the initiation of an investigation into the establishment and use of the Bristol DA's YSTR database in order to advance the integrity and reliability of forensic science in the Commonwealth.

At the same time, for the sake of this Board and its continued efficacy, one thing needs to be clarified as soon as possible at our meeting.

**Did EOPSS and the MSPCL act in a manner that is consistent with the FSOB's recommendations, including by urging the AGO to appeal the denial of the motion to quash?**

In our view, if the answer is that they have *not* done so, this failure raises serious questions about the role of this Board and the considerable work it has done. In effect, the controversy over the Bristol DA's plan *as a new forensic provider* to establish a database of YSTR records wholly independent of the MSPCL's oversight represents an early and profoundly significant test of whether the FSOB can meaningfully oversee the forensic science areas under its jurisdiction, and whether EOPSS will prevent law enforcement agencies from doing an end run around the Board.

Sincerely,

/s/

Judge Nancy Gertner (Ret.)

Lisa Kavanaugh

Anne Goldbach

## MEMORANDUM

TO: Bristol County District Attorney

FROM: Forensic Science Oversight Board

DATE: May 7, 2021

RE: Topics to be discussed during May 21, 2021 FSOB meeting

---

What follows is a set of questions that we invite you to discuss with the Board at our May 21, 2021. You are welcome to provide the FSOB with written responses, to present orally, to present with a PowerPoint, or to respond in whatever manner you feel will be most appropriate. Our hope is to provide you with notice of the range of issues that the FSOB is interested in hearing about.

**For all questions, the terms “DNA data” and “DNA profiles” refer to both autosomal and Y-STR DNA profiles and any additional information related to those DNA profiles.**

1. If you are opting not to respond to any or all of the below questions, what is your rationale for not responding?
2. Are you in possession of any DNA data that you did not generate?
3. When and from whom have you received any DNA data?
4. What is the format of the DNA data you received (i.e., hard copy, computer file, .xlsx file, .cmf file)?
5. How is the DNA data being stored (e.g., hard copy, commercial software spreadsheets, commercial database programs)? Provide specific name and version of the software, if applicable.
6. What are you doing with the DNA data you have received?
7. What future plans do you have related to DNA databases/spreadsheets?
8. Were/are there any restrictions placed on your use of the DNA data you received? If so:
  - a. What are they?
  - b. How were they determined?
  - c. Who is responsible for overseeing compliance with any restrictions on data use?
  - d. How will you document your compliance with any such restrictions?

9. To what extent do you follow the guidance of any accreditation or licensing organizations with respect to DNA data access, security, quality assurance and control?
10. Does your agency plan to seek the appropriate accreditation, certification, or licensing to conduct forensic searches and DNA profile comparisons? If so, what accrediting, certifying, or licensing entity?
11. Have you developed any written protocols or guidance to address any or all of the issues enumerated below related to the establishment and oversight of your planned DNA database/spreadsheet? (Specifically: (a) data access/security; (b) data quality assurance; (c) handling of searches/profile comparisons; (d) confidentiality; (e) methodology/loci questions; (f) notification & expungement; (g) data sharing with outside entities).
12. If so, could you provide the FSOB with a copy of all such protocols?
13. Whether or not you have developed any *written* protocols or guidance regarding the enumerated issues, what are your plans with respect to the following:

**Data access/security**

- a. How will data be imported or entered into your database/spreadsheet?
- b. Who will have access to the database/spreadsheet?
- c. Are there different levels of access of personnel who are authorized to view/edit/alter data? If so:
  - i) Who can view the data?
  - ii) Who can edit the data?
  - iii) What requirements are there for authorization?
- d. How will new information and data be integrated into the database/spreadsheet over time?
- e. What measures do you have in place to track who accesses/enters/views/edits data?
- f. What security measures exist to protect the data from being accessed or modified by unauthorized individuals (internal or external to your agency)?
- g. How will information be removed from the database/spreadsheet?

**Data quality assurance:**

- h. Will those with access to the database/spreadsheet be required to undergo training?  
If so:
  - i) What are the specific training procedures?
  - ii) Who will be authorized and qualified to perform the training?
  - iii) What competency testing will be conducted to ensure successful completion of the training?
  - iv) How frequently will training be conducted?
- i. What verification procedures will there be to ensure the accuracy of data?



- j. As data is removed or new data integrated into your database/spreadsheet, are there any verification procedures to ensure that the accuracy of the remaining/new data is not impacted by those changes?

**Handling of searches/profile comparisons. Do you have written protocols for the following:**

- k. How searches will be performed?
- l. How comparisons of potential matches will be performed?
- m. Who is/will be authorized to initiate a search?
- n. Who is/will be authorized to make a comparison?
- o. What verification procedures are/will be required prior to releasing or acting upon a match generated using your database/spreadsheet?
- p. Whether you will require any specialized training for individuals who are authorized to conduct searches and to make comparisons? If so:
  - i) What are the specific training procedures?
  - ii) Who will be authorized and qualified to perform the training?
  - iii) What competency testing will be conducted to ensure successful completion of the training?
  - iv) How frequently will additional training or continuing education be required and conducted?
- q. Do you intend to perform searches in adjudicated cases? (for example, if requested by a defendant seeking to develop evidence of innocence) If so, will you notify a defendant if the search performed hits to a known profile that does not match the defendant's profile?

**Confidentiality:**

- r. What protocols or procedures do you have to protect the confidentiality of the DNA profiles and the information contained in your database/spreadsheet?
- s. Does your database/spreadsheet include names or other identifying information about the sources of the profiles?
- t. What measures are in place to ensure that personal identifying information is shielded from those with and without authorized access to the data?
- u. If profiles have been or will be anonymized, who is authorized to learn the identity of a profile that is "matched" as a result of a search?

**Methodology/loci questions:**

- v. Which DNA loci are included in your database/spreadsheet?
- w. Have you identified a list of DNA profiling kits that have been validated for inclusion in your database/spreadsheet?
- x. If so, by what method have you determined the appropriateness of the DNA profiling kits to be included on that list?
- y. What searching and/or matching algorithms will be used to conduct and confirm DNA profile matches.

- z. Will a qualified DNA analyst review the matches? What parameters do you use to qualify persons to review and confirm matches?
- aa. What are the requirements to search mixed and partial DNA profiles?
- bb. Some Y-STRs are known to be rapidly mutating. Is there a procedure for how to handle profiles that match at all but one or two loci?
- cc. Have you determined the allele or haplotype frequency for a profile or multiple profiles in your database?
- dd. Have you checked for internal matches within the database, or do you have plans to do so?

**Notification & expungement:**

- ee. What measures are in place to notify individuals that their DNA profile is included in your database/spreadsheet?
  - i) Defendants?
  - ii) Witnesses/victims who provide elimination samples?
  - iii) Lab personnel/defense experts/ police who provide elimination samples?
- ff. If there is a database/spreadsheet breach will people in the database/spreadsheet be notified?
- gg. How will a defendant or other individual whose profile is included in the database/spreadsheet know if they became a suspect as a result of a search in this database/spreadsheet?
  - i) Would it be subject to discovery?
- hh. Have you defined any circumstances in which a profile that you initially include in your DNA database/spreadsheet can or should be removed? If so:
  - i) By what criteria would a DNA profile be removed?
  - ii) Is there a method for an individual to have their DNA profile expunged?
  - iii) If so, what is it?

**Data sharing with outside entities:**

- ii. What protocols and procedures are in place to prevent DNA data from being used for non-law enforcement purposes?
- jj. What protocols and procedures are in place to allow DNA data held in your database/spreadsheet to be given to other agencies, persons, or organizations?
- kk. If you have developed such protocols, please provide the FSOB with a copy of them.
- ll. Do you have an agreement with any outside entities, including other District Attorney offices:
  - i) To collaborate with or receive DNA data from?
  - ii) To provide DNA data from your database/spreadsheet
- mm. If so, would you provide the FSOB with copies of all such agreements?

## MEMORANDUM

TO: Massachusetts State Police Crime Laboratory

FROM: Forensic Science Oversight Board

DATE: May 7, 2021

RE: Topics to be discussed during May 21, 2021 FSOB meeting

---

What follows is a set of questions that we invite you to discuss with the Board at our May 21, 2021. You are welcome to provide the FSOB with written responses, to present orally, to present with a Powerpoint, or to respond in whatever manner you feel will be most appropriate. Our hope is to provide you with notice of the range of issues that the FSOB is interested in hearing about.

**For all questions, the terms “DNA data” and “DNA profiles” refer to both autosomal and Y-STR DNA profiles and any additional information related to those DNA profiles.**

1. When did the laboratory receive the Bristol County grand jury subpoena that is the subject of this inquiry?
2. Did the laboratory have any scientific concerns about complying with the Bristol County subpoena? If so:
  - a. What were the concerns?
  - b. To whom did they communicate those concerns?
3. Has the laboratory received any other requests for DNA data from any other counties, outside of Bristol County? If so:
  - a. When?
  - b. From which other counties?
  - c. Did the laboratory provide any DNA data in response to these requests?
4. Has the laboratory received any other grand jury subpoenas or court orders seeking DNA data, other than the one subpoena from Bristol County that has already been brought to the attention of the FSOB?
5. What records did the court order the laboratory to produce in response to the grand jury subpoena? What was the exact language of the court’s order?

6. Has the laboratory released DNA profile records pursuant to the Bristol County grand jury subpoena?
7. Is there a Use and Dissemination Agreement that has been executed by Bristol County and the laboratory regarding any records released?
  - a. If so, please provide the FSOB with a copy of the executed Use and Dissemination Agreement.
  - b. If not, why not?
8. When and to whom have you provided any DNA data developed and retained by the laboratory?
9. What is the format of the DNA data you provided (i.e., hard copy, computer file, .xlsx file, .cmf file)?
10. What information was included in the data provided (e.g., proper names, social security numbers, addresses, inmate number, gender, race, other confidential or identification information)?
11. Did the data provided include DNA data developed from customers in any of the following categories:
  - a. Suspects
  - b. Law enforcement or lab personnel
  - c. Victims
  - d. Family members or household members of victims
  - e. Consensual sexual partners of victims
  - f. Defense representatives/ testing observers
12. Were you able to and/or did you inform your customers in advance that the confidential information concerning samples submitted by them that you developed DNA profiles on may be given to another entity or placed in the public domain?
13. Did you receive agreement from said customers before providing the confidential information to another entity?
14. Were there any protections of the DNA data released from either intended or unintended alteration?
15. Were there any limitations placed on what DNA data you provided?
16. Have you complied with your accrediting body's requirements relating to disclosure of significant changes, events, and nonconformities?

17. Did the DNA profiles provided include people who under the authority of Massachusetts statute, regulation or other legal requirement allowed to be included in a DNA database?
18. Did the DNA profiles provided include people who do not meet the Massachusetts statute, regulation or other legal requirement to be included in a DNA database?
19. Did the DNA profiles provided include people who are currently held in your CODIS state database?
20. Did the DNA profiles provided include people who are not currently held in your CODIS state database?



# Exhibit G

## *The Commonwealth of Massachusetts* *Department of State Police*



### Crime Laboratory

124 Acton Street

Maynard, MA 01754

May 20, 2021

CHARLES D. BAKER  
GOVERNOR

KARYN E. POLITO  
LIEUTENANT GOVERNOR

THOMAS A. TURCO, III  
SECRETARY

CHRISTOPHER S. MASON  
COLONEL/SUPERINTENDENT

R. SCOTT WARMINGTON  
DEPUTY SUPERINTENDENT

To: Undersecretary Kerry A. Collins, Chair, Forensic Science Oversight Board

From: Director Kristen L. Sullivan, Chief Science Officer, MSP Crime Laboratory

Subject: Y-STR Data Provision

Dear Chair Collins and Forensic Science Oversight Board Members,

The Massachusetts State Police Crime Laboratory (MSPCL) is in receipt of the Forensic Science Oversight Board's (FSOB) request dated May 21, 2021 for information related to the release of DNA data. The MSPCL has determined that this is the most appropriate way to answer the FSOB's questions. In the event, the FSOB wishes to submit additional questions to the MSPCL, it would be happy to provide further answers in a similar format.

### **Background**

In September of 2019, the Bristol County District Attorney's Office (BCDAO) asked the Massachusetts State Police Crime Lab (MSPCL) to provide all Y-STR data, in aggregate form, from all counties in the Commonwealth. The specific request was "for any/all investigative cases/DNA reports that produced a Y-STR profile in the possession of the Massachusetts State Crime Lab . . . [A]ll Y-STR results tables include sample description, case numbers, item numbers and Y-STR results in data form . . ."

MSPCL had scientific concerns about the operation of a DNA database by non-forensic scientists that is not regulated, release of data from other counties without expressed permission, and safeguards that would be employed to protect data and any information resulting from any potential forensic links resulting from that data. These concerns were discussed among the Executive Office of Public Safety and Security (EOPSS) agencies as well as with the Attorney General's office (AGO). Additionally, the MSPCL has communicated these concerns to the Bristol County District Attorney's Office (BCDAO). As a result, in response to this initial request, Bristol was not provided with Y-STR profiles developed for other counties.

### **Customer Data Provided to Bristol**

Per ANAB accreditation, a customer is considered the submitting agency and District Attorney's Office. Recognizing the BCDAO was requesting Y-STR data in which it was the customer and that it had previously received the data from the MSPCL when the Y-STR results were originally reported to their office and that the majority of the reports were available to BCDAO through their access in LIMS; BCDAO was provided with all Y-STR reports originating from its cases and requests only.

### **Profiles Included**

The data provided to Bristol in response to this request included the full DNA report, without redaction. Information contained in these reports may include proper names, gender, Y-STR profiles, and STR profiles. The material provided

included data developed from suspects and victims. Although the exact relationship of an individual to a case is not always known, profiles submitted for exclusionary purposes, e.g., family members and consensual sexual partners, were provided.

The reports provided are very unlikely to contain profiles of law enforcement, lab personnel or defense representatives or testing observers. However, these data included profiles from individuals who are required, by statute, to be included in both the CODIS and state DNA databases. In instances, such as these, however, the profile provided to the DA's office would have been developed from an entirely different biological sample than the one used to develop the DNA profile for the state database. The reports also included profiles of persons who do not meet the Massachusetts statute, regulation or other legal requirement to be included in either the CODIS or the State DNA databases.

**Other Requests: profiles not provided**

On August 3, 2020, the MSPCL received a request from the Worcester County District Attorney's Office (WCDAO) to provide "*all YSTR reports of testing on cases in Worcester County (Middle District) from 2015 to the present day.*" It was communicated to the laboratory that the intent was to provide this to BCDAO for inclusion in a database.

In response, EOPSS and the MSPCL drafted a Use and Dissemination agreement in an effort to ensure proper use and safeguarding of the information when released to the requesting district attorney's office (DAO). To date, neither EOPSS nor the MSPCL has received a signed copy of the agreement from any DAO. The data requested by the WCDAO has not been released.

On December 11, 2020, the MSPCL received a request from the Plymouth County District Attorney's Office (PCDAO) requesting that their Y-STR reports be provided to Bristol County. The PCDAO was provided with the Use and Dissemination agreement for review and signature and MSPCL declined to provide the data until the Use and Dissemination agreement was signed. To date, neither EOPSS nor the MSPCL has received a signed copy of the agreement from PCDAO. Records were not turned over to PCDAO in response to this request.

**Grand Jury Subpoena**

On January 9, 2021, the MSPCL received a subpoena from the Bristol County. After motion practice, the MSPCL began complying with the subpoena by producing the requested data in PDF format. The MSPCL is unable to provide any further information at this time due to the secrecy of the Grand Jury.

**Accrediting Body Notification**

The laboratory notified the ANAB accreditation manager of the Grand Jury subpoena and advised ANAB that we are currently working to determine if we are legally permitted to notify our customers (e.g., original submitting agency) of the release of data without violating the terms of the Grand Jury. ANAB has acknowledged MSPCL's disclosure and advised the Laboratory that further communication will be needed only if MSPCL is ultimately unable to meet their accreditation requirements (e.g., notification of customer of release of confidential information) due to grand jury restrictions.

Respectfully submitted,

Kristen L. Sullivan  
Chief Science Officer



The Commonwealth of Massachusetts  
Executive Office of Public Safety and Security  
One Ashburton Place, Room 2133  
Boston, Massachusetts 02108

Tel: (617) 727-7775  
TTY Tel: (617) 727-6618  
Fax: (617) 727-4764  
[www.mass.gov/eopss](http://www.mass.gov/eopss)

CHARLES D. BAKER  
Governor

KARYN E. POLITO  
Lt. Governor

THOMAS TURCO, III  
Secretary

**Exhibit H**

District Attorney Thomas M. Quinn, III  
Bristol District Attorney's Office  
888 Purchase Street, 5<sup>th</sup> Floor  
New Bedford, MA 02740  
VIA ELECTRONIC MAIL AND FIRST CLASS MAIL

May 24, 2021

Dear District Attorney Quinn,

The Forensic Science Oversight Board (FSOB) has requested that I, as FSOB Chairperson, renew its prior request to discuss matters related to the Bristol County YSTR DNA database and your office's use, storage, handling, and sharing of DNA data and profiles. This request was made pursuant to M.G.L. c. 6, § 184A(d)(ii), which requires the FSOB to "initiate an investigation into any forensic science, technique or analysis used in a criminal matter" in the event of a vote that such an investigation "would advance the integrity and reliability of forensic science in the commonwealth."

On behalf of the FSOB, Board advisor Lisbeth Pimentel on May 5 invited you via email to attend the FSOB's May 21 meeting. This invitation was followed by a May 11 email containing a set of questions posed by the FSOB for purposes of this discussion. Because you did not attend the May 21 meeting, the Board has asked me to relay its significant concerns with your lack of response. The next scheduled FSOB meeting will be held on June 24, at which time they will further discuss their investigation and would again ask you to discuss these same matters. The Board has further asked that you respond to their request by the close of business on June 17.

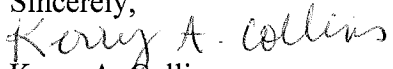
The FSOB was established to have oversight authority over all commonwealth facilities engaged in forensic services in criminal investigations, and to provide enhanced, objective, and independent auditing and oversight of forensic evidence used in criminal matters, and of the analysis, including the integrity of such forensic analysis, performed in state and municipal laboratories. As such, the FSOB welcomes your contributions and hopes you will attend its next meeting. You are free to address the Board's questions in written form, to present orally or with a PowerPoint, or to respond in whatever manner you feel will be most appropriate. Should you opt not to participate, the FSOB will move forward without your input and, as required by statute, report the results of its investigation and any resulting recommendations to the Executive Office of Public Safety and Security, the Joint Committee on Public Safety and Homeland Security, the Supreme Judicial Court, the Massachusetts District Attorneys Association, the Massachusetts Attorney General, the Committee for Public



Counsel Services, the Massachusetts Association of Criminal Defense Lawyers, Inc. and the New England Innocence Project, Inc.

To facilitate the discussion on this matter, I have attached the questions posed by the FSOB and previously provided to you on May 11. Please let me know if you have any questions.

Sincerely,

A handwritten signature in cursive script that reads "Kerry A. Collins".

Kerry A. Collins

Chairperson, Forensic Science Oversight Board

Cc: Forensic Science Oversight Board

# Exhibit I

## DATA USE AND DISSIMINATION AGREEMENT

This Data Use Agreement (Agreement) is made by and between the Massachusetts State Police Crime Laboratory (MSPCL) and the Office of the \_\_\_\_\_ County District Attorney (DAO), including any of its agents and contractors.

**WHEREAS**, the DAO office has requested all DNA records containing results of Y-STR testing on cases in \_\_\_\_\_ County from 2015 to the present day.

**WHEREAS**, the DAO has previously received these records in connection with specific investigations and cases.

**WHEREAS**, the DAO is asking MSPCL to release these reports to the DAO in the aggregate.

**WHEREAS**, the MSPCL has been informed that the DAO office seeks to use this information for: [TO BE FILLED IN BY THE DAO; including who will hold the data, for what purpose and who will have access to the data]

**WHEREAS**, Y-STR reports are DNA records that may provide information of patrilineal relationships and therefore may include data on more than one individual.

**WHEREAS**, The DNA records requested by the DAO include records of suspects, victims, witnesses and elimination profiles.

**WHEREAS**, M.G.L. Chapter 22E, Section 2 authorizes the director of the MSPCL to manage and administer the state DNA database.

**WHEREAS**, M.G.L. Chapter 22E, Section 10 requires the director of the MSPCL, to furnish records in its possession, including DNA records and analysis, to prosecuting officers within the Commonwealth upon request in writing or electronically for “identification purposes in order to further official criminal investigations or prosecutions”.

**WHEREAS**, M.G.L. Chapter 22E, Section 9 states, “All DNA records collected pursuant to this chapter shall be confidential and shall not be disclosed to any person or any agency unless such disclosure shall be authorized by this chapter”.

**WHEREAS**, 515 C.M.R. 2:07 regulates data provided by MSPCL and provides for a Use and Dissemination Agreement.

**WHEREAS**, DNA records constitute personal data as defined by the Fair Information Practices Act, M.G.L. chapter 66A, (FIPA).

**WHEREAS**, FIPA applies to government agencies maintaining records of personal data and requires agencies to “not collect or maintain more personal data than are reasonably necessary for the performance of the holder’s statutory functions”.

**WHEREAS**, M.G.L. Chapter 30 Section 63 requires holders of personal data to file notice with the Secretary of State.

**WHEREAS**, M.G.L. Chapter 214, Section 1B states “A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.”

**WHEREAS**, M.G.L. Chapter 214 Section 3B subjects an agency in violation of Chapter 66A to an action for injunction, declaratory judgment, or mandamus.

**WHEREAS**, lab protocols for search parameters of DNA records and databases held by the MSCPL are set in compliance with Federal regulations and FBI restrictions and meet the standards necessary for lab accreditation.

**WHEREAS**, MSPCL requires that the DAO execute this written Agreement to ensure that DNA records and data obtained from the MSPCL will be received, stored and used in compliance with M.G.L. c. 22E, M.G.L. c. 66A, 34 U.S.C. 12592, and all other applicable state and federal laws and regulations. The DAO acknowledges that failure to comply with the DNA Identification Act of 1994 privacy requirements could result in loss of access to CODIS for the Commonwealth.

**NOW THEREFORE**, in consideration of the foregoing recitals (which are hereby incorporated and made an integral part of this Agreement), as well as the duties and obligations set forth in this Agreement, it is agreed by and between the parties as follows:

#### **TERMS AND CONDITIONS**

1. Permitted Use: The DAO hereby certifies that the DAO is permitted to request DNA records as it is a prosecuting officer and that DNA records and data received pursuant to this request will only be used in a way that is permitted by law. The DAO further certifies that it will receive, store and use such DNA records in compliance with M.G.L. c. 66A, 42 U.S.C. 14132(b) (DNA Identification Act of 1994) and all other applicable state and federal laws and regulations. The DAO acknowledges that failure to comply with the DNA Identification Act of 1994 privacy requirements could result in loss of access to CODIS for the Commonwealth.
2. Access To and Use of Personal Data: The DAO certifies that it will use DNA records and data solely for purposes consistent with Paragraph 1 of this Agreement. Furthermore, the DAO shall not use any personal information obtained, pursuant to this Agreement, for any purpose that is not permitted under Massachusetts or Federal laws, rules or regulations and the DAO agrees it will comply with all applicable laws and regulations respecting access to and use of personal information including, but not limited to, the Massachusetts Fair Information Practices Act (FIPA) M.G.L. c. 66A, the Massachusetts Identity Theft Act, M.G.L. c. 93H, M.G.L. c. 214, Section 1B, the DNA Identification Act of 1994, the Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.00, and Executive Order 504. The DAO further agrees that it will comply with all state and federal laws and orders, state or federal, regarding access to and the use of DNA records and personal data. The DAO further agrees that information accessed, pursuant to this Agreement, shall not be used to create or aggregate the data for any purpose, except as specifically provided for by federal or state law.
3. Additional Testing
  - a. If additional testing is requested by the DAO with respect to any of the YSTR profiles that are being provided pursuant to this Agreement, MSPCL reserves the right to require submission of a new standard for comparison

- b. Standards submitted for comparison for a particular case or investigation shall not be used by MSPCL for comparison to another case unless exigent circumstances are present. Comparison without the submission of a new standard requires the explicit permission of the Laboratory Director.
  - c. Prior to submission, the DAO shall notify MSPCL that any additional requests for testing or comparison are made on the basis of a link in a non-CODIS database.
  - d. Any subsequent testing shall comply with the statute and federal laws and regulations and accreditation guidelines and standards. If the DAO requests that MSPCL conduct testing which does not comport with state of federal law or regulation, or accreditation guidelines, MSPCL shall not conduct the testing.
  - e. The DAO agrees not to permit the use of any reference standard profiles for any database search.
- 4. Access To and Use of Personal Data: The DAO certifies that it will use DNA records and data solely for purposes consistent with Paragraph 1 of this Agreement. Furthermore, the DAO shall not use any personal information obtained, pursuant to this Agreement, for any purpose that is not permitted under Massachusetts or Federal laws, rules or regulations and the DAO agrees it will comply with all applicable laws and regulations respecting access to and use of personal information including, but not limited to, the Massachusetts Fair Information Practices Act (FIPA) M.G.L. c. 66A, the Massachusetts Identity Theft Act, M.G.L. c. 93H, M.G.L. c. 214, Section 1B, the DNA Identification Act of 1994, the Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.00, and Executive Order 504. The DAO further agrees that it will comply with all state and federal laws and orders, state or federal, regarding access to and the use of DNA records and personal data. The DAO further agrees that information accessed, pursuant to this Agreement, shall not be used to create or aggregate the data for any purpose, except as specifically provided for by federal or state law.
- 5. The DAO agrees to implement any and all administrative, physical and technological safeguards necessary to ensure the confidentiality and integrity of the DNA records and data being provided pursuant to this agreement.
  - a. Electronic Security Requirements
    - i. Ensure the use and maintenance of a log indicating the name and position of any individual who was granted electronic access to DNA records, pursuant to this agreement, as well as the date and time said records were viewed and a brief description of the specific records that were accessed and what purpose they were accessed for.
    - ii. Written password policies and procedures, including the deactivation of passwords that follow current industry standards.
  - b. Administrative Security Requirements
    - i. Written procedures that ensure the electronic safety, physical security and confidentiality of the DNA records.
    - ii. Written procedures that ensure DNA records are accessed only for permitted uses, consistent with M.G.L. c. 22E, FIPA and all other applicable state and federal laws and regulations.

- iii. Written procedures that ensure the DNA records subject to this agreement shall never be disseminated unless such dissemination is required or permitted by law.
- iv. Ensure the use and maintenance of a log indicating the name and position of any individual who disseminated any DNA records or data, subject to this agreement, as well as the date said records were disseminated, the name and address of any individuals said records were disseminated to and a brief description of the specific records that were disseminated and what purpose they were disseminated for. Written procedures that ensure the DNA records provided subject to this agreement shall never be used in furtherance of an illegal act, including a violation of criminal or civil laws.
- v. Written or electronic records will be kept to document that DAO has familiarized all personnel and adhered to all regulations governing the receipt, storage and use of all information covered in this Agreement.
- vi. Written or electronic records shall be maintained by DAO that support and justify inquiries and requests for DNA Database searches.
- vii. Disclosure by the DAO of any information obtained from the DNA Database to any unauthorized agency or person is prohibited. The DAO will make reasonable efforts to prevent disclosure to an unauthorized agency or person.
- viii. Unauthorized use of the DNA information provided to the DAO pursuant to this Agreement can result in suspension of access, cancellation of access, and/or fines for any violations of the terms and conditions of the use and dissemination agreement by a user agency, its employees or agents, and a policy for reinstating access by the Department only after the Department is satisfied that the causes of all violations have been eliminated.

c. Physical Security Requirements

- i. Ensure that DNA records obtained pursuant to this Agreement are stored in a secure location that is not visible or accessible to unauthorized individuals;
- ii. Ensure that DNA records obtained pursuant to this Agreement that are in printed or in paper form are stored in locked filing cabinets when not in use and that said records are shredded or deposited into a locked shredder container when no longer needed;
- iii. Ensure the use and maintenance of a log indicating the name and position of any individual who was granted physical access to DNA records provided pursuant to this agreement, as well as the date and time said records were viewed and a brief description of the specific records that were accessed and what purpose they were accessed for.

6. Reporting of Disclosures or Security Incidents. The DAO agrees that it will promptly notify the necessary parties or agencies following discovery or notice of any use or disclosure of DNA records not allowed by the Agreement or law, or any Security Incident involving the DNA records received pursuant to this Agreement. The notification may be made verbally, and notification will also be made in writing, to the contacts designated by the Parties below, within ten (10) calendar days of the verbal notification.

7. Duty to Mitigate and to Inform. The DAO will mitigate, to the extent practicable, any harmful effect that is known to the DAO resulting from any use or disclosure of DNA records provided pursuant to this Agreement in violation of the Agreement, including but not limited to, retrieving, when possible, such records. The DAO shall take such further actions as deemed appropriate by the parties to mitigate, to the extent practicable, any harmful effects of a use or disclosure in violation of this Agreement. In addition, the provisions of M.G.L. c. 93H, M.G.L. c. 66A or other legal authority may require notice to be provided to individuals of a wrongful use or disclosure the DNA records. The DAO shall consult with the MSPCL regarding any notice required to be made.
8. Individual Rights. The DAO agrees to take such action as may be reasonably requested by the MSPCL in order for the agency to meet its obligations under M.G.L. c. 66A or other legal authority with respect to any DNA records provided to the DAO under this Agreement.
9. Agents or Contractors: If the DAO engages an agent or contractor, the DAO will ensure that the agent or contractor agrees, in writing, to comply with the same or greater restriction and conditions that apply to the DAO under this agreement.
10. Indemnification and Liability: The DAO agrees to indemnify and hold harmless MSPCL from and against any and all damages (including, without limitation, reasonable attorneys' fees, charges and disbursements) incurred as a result of any unauthorized use or dissemination of the information that MSPCL provides to the DAO pursuant to this Agreement.
11. Expungement: If the DAO seeks to use this information in a non-CODIS database, it shall have a procedure for expungement of the DNA record from the non-CODIS database.
12. Conflict of Interest Disclosure: The DAO will assure that any of its vendors, contractors or agents that have access to the DNA records are in compliance with the state conflict of interest laws and have filed all necessary written disclosures pursuant to M.G.L. c. 268A, section 6A.
13. Single Transaction Clause: The provision of information contemplated by this Agreement will be a single transaction. The DAO agrees that the information requested is for the date range from 2015 to the date of this Agreement. MSPCL is not obligated by this Agreement to provide data generated after the date of execution of this Agreement.

## CONTACTS

Notices and other communications as to any matter hereunder will be sufficient if given in writing or by e-mail to the contact person(s) identified below.

DAO:

MSPCL:

Darina Griffin  
Legal Counsel  
Massachusetts State Police Crime Lab  
124 Acton Street  
Maynard, MA  
978-451-3553  
[darina.griffin@pol.state.ma.us](mailto:darina.griffin@pol.state.ma.us)

### **MISCELLANEOUS**

**Ambiguity.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that allows a Party to comply with M.G.L. c. 22E, M.G.L. c. 66A, and M.G.L. c. 93H & I or any other applicable privacy or security law, rule or regulation.

**Amendment.** This Agreement may be amended by the Parties at any time; provided, that any amendment must be agreed upon and reduced to writing and must be signed by each Party.

**Effective:** This Agreement shall take effect only after officials of the MSPCL and the DAO having both the administrative and legal authority to bind the parties to the terms and conditions of the agreement have signed the use and dissemination agreement.

**IN WITNESS WHEREOF,** the Parties have caused their duly authorized representatives to execute this Data Use Agreement, as follows:

Office of the District Attorney

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

State Police Crime Laboratory

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_