Electronically Filed
9/1/2023 3:25 PM
Second Judicial District, Latah County
Julie Fry, Clerk of the Court
By: Tamzen Reeves, Deputy Clerk

Anne C. Taylor, Public Defender
Kootenai County Public Defender
PO Box 9000
Coeur d'Alene, Idaho 83816
Phone: (208) 446-1700; Fax: (208) 446-1701
Bar Number: 5836
iCourt Email: pdfax@kcgov.us

Elisa G. Massoth, PLLC
Attorney at Law
P.O. Box 1003
Payette, Idaho 83661
Phone: 208-642-3797; Fax: 208-642-3799

Assigned Attorney:
Anne C. Taylor, Public Defender, Bar Number: 5836
Jay W. Logsdon, Chief Deputy Public Defender, Bar Number: 8759
Elisa G. Massoth, Attorney at Law, Bar Number: 5647

IN THE DISTRICT COURT OF THE SECOND JUDICIAL DISTRICT OF THE STATE OF IDAHO, IN AND FOR THE COUNTY OF LATAH

STATE OF IDAHO **Plaintiff,** **V.** **BRYAN C. KOHBERGER,** **Defendant.**	**CASE NUMBER CR29-22-2805** **RESPONSE TO STATE'S NOTICE OF INTENT NOT TO CROSS-EXAMINE DEFENSE WITNESSES, DISTRICT COURT DECISION, AND RECORDS TO EXPLAIN WITNESS CONTACT**

COMES NOW, Bryan C. Kohberger, by and through his attorneys of record, and hereby responds to the State's Notice of Intent Not to Cross-Examine Defense Witnesses, District Court Decision and Records to Explain Witness Contact.

PROCEURAL HISTORY

This Court conducted a hearing on August 18, 2023 on Mr. Kohberger's Third Motion to Compel. Four witnesses testified for the defense and the State reserved the right to cross-examine two witnesses. On August 30, 2023, the State filed notice that it does not intend to re-open the hearing and cross-examine the two witnesses.

RESPONSE

Referenced in the State's Notice of Intent Not to Cross-Examine Defense Witnesses, District Court Decision, and Records to Explain Witness Contact ("State's Notice") are a Third District Court Transcript from CR14-20-07840. Mr. Kohberger's defense team has reviewed the exhibit and provides the following response.

At first blush it appears the issue before Judge Whitney in *State v. Dalrymple* CR14-20-07840 was that the State was seeking a protective order relating to a database that produced information leading to Mr. Dalrymple's arrest. However, the decision Judge Whitney announced was on a different issue and was made without the benefit of expert testimony relating to the Forensic/Investigative Genetic Genealogy process. It is noteworthy that even without the benefit of that testimony Judge Whitney concluded that the State needed to turn over in discovery everything in its possession relating to Genetic Genealogy and the defense was welcome to bring further motion on the issue.

This Court's is asked to decide something different. The information sought by Mr. Kohberger, through his motion to compel, is the same information that the State seeks to protect with it motion for protective order: the SNP profile created on behalf of the State and the genetic genealogy process directly used by the State to identify Mr. Kohberger. Mr. Kohberger is not asking for a genetic genealogy *database,* rather the analysis and documentation utilized to

identify him. Mr. Kohberger has also asked for the SNP profile and the state has agreed to provide it.[1]

This Court is left to decide whether to shield the analysis and documentation developed and used to identify Mr. Kohberger or to order it be provided for his defense. This Court makes its decision with the benefit of expert Steve Mercer explaining the duties of attorneys to examine this evidence and the types of legal decisions that could be made based on this evidence. This court has the benefit of knowing, based on expert testimony, how SNP results are produced using bioinformatics. Further, expert testimony described how genetic genealogy tracing is conducted and the documents generated by a genetic genealogist showing the analysis and result. Further, this court has the benefit of expert testimony describing how SNP testing can be compared against STR testing for contaminants and mixtures as well as how the SNP and genealogical data can impact statistics. Lastly, this court has knowledge of the intricacies of prohibited law enforcement access to various DNA databases. The testimony the court received in the hearing relating to this loophole is not something Judge Whitney had the benefit knowing. It is important for the court to be aware that this same information has now been published on August 18, 2023 in the Intercept. This article details Forensic Genetic Genealogy and the loopholes utilized to obtain information in contradiction of authorization. (Attached as Exhibit A) The Intercept is an online journal that has existed since 2014. Open source information states this is an award winning news organization dedicated to exposing the powerful and holding them accountable.

[1] The State wrote, in its June 2023 Motion for Protective Order that it would provide the SNP profile. Again, during the August 18, 2023 hearing the State stated it would provide the SNP profile. At this time Mr. Kohberger has not been given this information.

The court in *State v. Dalrymple* also lacked the following documents that establish the relationship between the Idaho State Forensic Laboratory, local police departments, and prosecuting entities in the State of Idaho. This Court received such documentation attached to the Declaration of Anne C. Taylor in Support of Third Motion to Compel. The agreement is attached again herein as Exhibit B. This memorandum shows that Idaho utilizes Federal money to work with Othram laboratories to identify suspects in certain cases. This memorandum shows the intricate relationship between agencies for identifying which cases qualify for identification through genetic genealogy.

In Mr. Kohberger's case the Latah County Prosecutor, the Moscow Police Department, the Idaho State Police and the FBI worked together to investigate the case and identify a suspect. *At some point* Genetic Genealogy was utilized for identification. That information remains withheld from Mr. Kohberger. Mr. Kohberger does not even know when this began or when he was supposedly identified.

The memorandum contains a requirement that the Federal Department of Justice Policies (hereinafter "DOJ") must be adhered to and that agencies must sign a memorandum of agreement to follow such policies - the DOJ has a policy, regarding Forensic Genetic Genealogical DNA Analysis and Searching. (This policy was attached to Taylor Dec. in Support of Third Motion to Compel, and is again attached herein as Exhibit C.) That policy requires that the prosecutor and investigating agency collaborate (see p. 5-6). That policy also requires that investigative agencies only enter and search DNA data bases that permit law enforcement to use their services (see p. 6). That policy requires that all Forensic Genetic Genealogy "profiles, account information, and data shall be retained by the investigative agency for potential use

during prosecution and subsequent judicial proceedings." (see p.7) There is a relationship between local, state and the federal government to work together. DOJ policy requires retention of analysis and materials for use in judicial proceedings. This knowledge, in addition to the potential for misuse of information is something that is discoverable and necessary to Mr. Kohberger.

Idaho Rule of Criminal Procedure 16(a) reads:

> the prosecuting attorney's obligations under this paragraph extend to material and information in the possession or control of members of prosecuting attorney's staff and of any others who have participated in the investigation or evaluation of the case who either regularly report, or have reported in that case, to the office of the prosecuting attorney.

The duty of disclosure "is an obligation of not just the individual prosecutor assigned to the case, but of all the government agents having a significant role in investing and prosecution the offense." *State v. Garnder*, 126 Idaho 428, 433 (Ct. App. 1994). The FBI has been compelled to turn over its CAST report related to cellular data evidence and its investigation related to identification of the car. The investigation related to the car included hundreds of names of individuals owning white a white Elantra. The evidence held regarding DNA is no different. The court in *Dalrymple* incorrectly permitted the State to hide material from the defense by claiming they did not have it. That is not how discovery works when the State decides to work with outside agencies to take liberty from someone. This Court has thus far shown that the FBI does not exist outside the discovery rules. It should not grant them immunity now.

CONCLUSION

The transcript provided from the Judge Whitney does little to instruct this court about what should be decided. This court has a different question – Mr. Kohberger requests materials

and analysis not a database. These materials are required by the DOJ to be retained for use in judicial proceedings. This Court has the benefit of understanding the process and the materials that were created in this identification of Mr. Kohberber by the state and its agents. Mr. Kohberger respectfully requests the Court Order the state to disclose the materials. Mr. Kohberger is happy to comply with any limiting order the Court deems appropriate.

DATED this ___1____ day of September, 2023.

ANNE C. TAYLOR, PUBLIC DEFENDER
KOOTENAI COUNTY PUBLIC DEFENDER

BY: _____
ANNE TAYLOR
PUBLIC DEFENDER

CERTIFICATE OF DELIVERY

I hereby certify that a true and correct copy of the foregoing was personally served as indicated below on the ___1____ day of September, 2023 addressed to:

Latah County Prosecuting Attorney –via Email: paservice@latahcountyid.gov
Elisa Massoth – via Email: legalassistant@kmrs.net

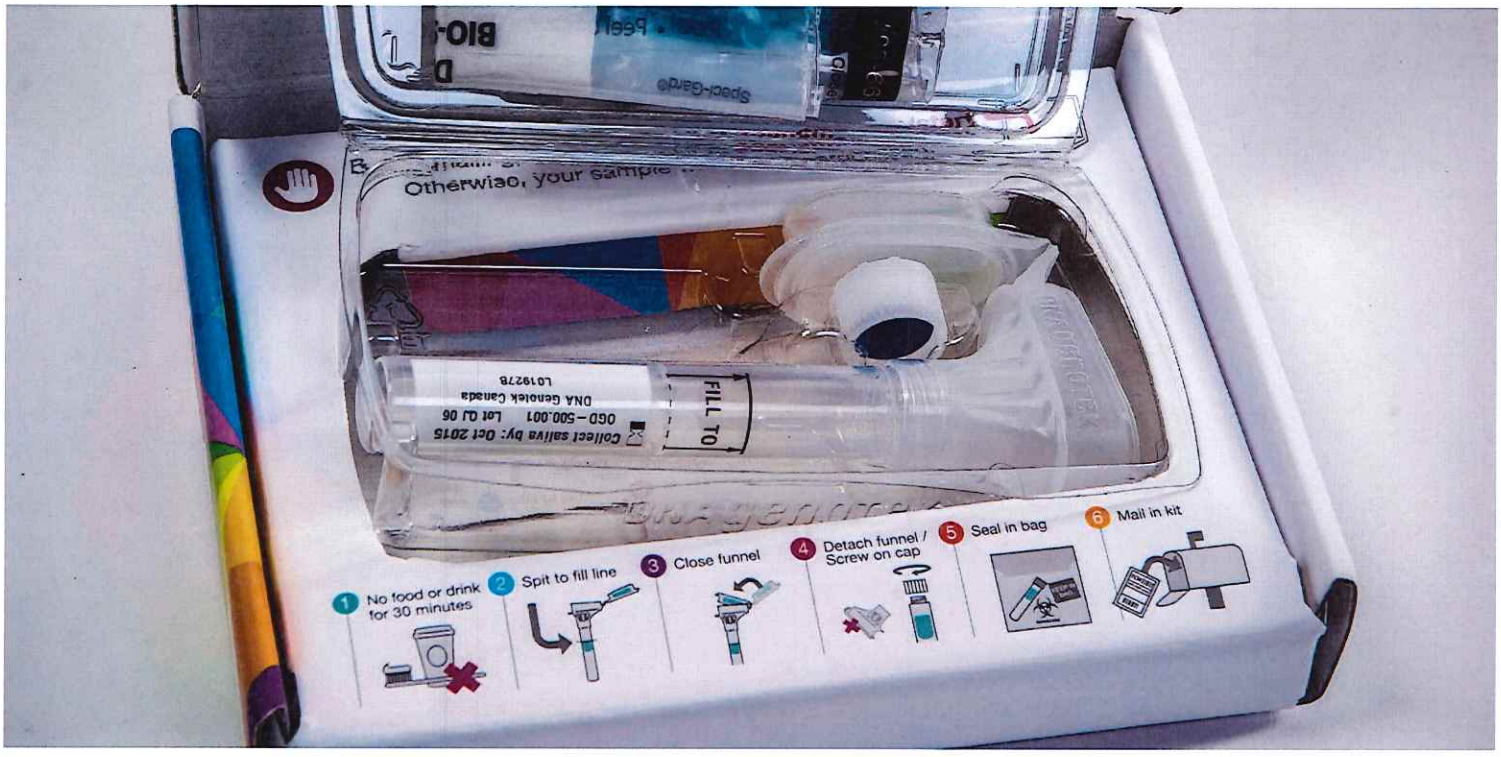
_____

POLICE ARE GETTING DNA DATA FROM PEOPLE WHO THINK THEY OPTED OUT

Forensic genetic genealogists skirted GEDmatch privacy rules by searching users who explicitly opted out of sharing DNA with law enforcement.

Jordan Smith

August 18 2023, 11:10 a.m.



The DNA kit genetic genealogist CeCe Moore used to help a woman find her biological mother on June 8, 2015.
Photo: MediaNews Group via Getty Images

CECE MOORE, AN actress and director-turned-genetic genealogist, stood behind a lectern at New Jersey's Ramapo College in late July. Propelled onto the national stage by the popular PBS show "Finding Your Roots," Moore was delivering the keynote address for the inaugural conference of forensic genetic genealogists at Ramapo, one of only two institutions of higher education in the U.S. that offer instruction in the field. It was a new era, Moore told the audience, a turning point for solving crime, and they were in on the ground floor. "We've created this tool that can accomplish so much," she said.

Genealogists like Moore hunt for relatives and build family trees just as traditional genealogists do, but with a twist: They work with law enforcement agencies and use commercial DNA databases to search for people who can help them identify unknown human remains or perpetrators who left DNA at a crime scene.

The field exploded in 2018 after the arrest of Joseph James DeAngelo as the notorious Golden State Killer, responsible for more than a dozen murders across California. DNA evidence collected from a 1980 double murder was analyzed and uploaded to a commercial database; a hit to a distant relative helped a genetic genealogist build an elaborate family tree that ultimately coalesced on DeAngelo. Since then, hundreds of cold cases have been solved using the technique. Moore, among the field's biggest evangelists, boasts of having personally helped close more than 200 cases.

The practice is not without controversy. It involves combing through the genetic information of hundreds of thousands of innocent people in search of a perpetrator. And its practitioners operate without meaningful guardrails, save for "interim" guidance published by the Department of Justice in 2019.

The last five years have been like the "Wild West," Moore acknowledged, but she was proud to be among the founding members

of the Investigative Genetic Genealogy Accreditation Board, which is developing professional standards for practitioners. "With this incredibly powerful tool comes immense responsibility," she solemnly told the audience. The practice relies on public trust to convince people not only to upload their private genetic information to commercial databases, but also to allow police to rifle through that information. If you're doing something you wouldn't want blasted on the front page of the New York Times, Moore said, you should probably rethink what you're doing. "If we lose public trust, we will lose this tool."

Despite those words of caution, Moore is one of several high-profile genetic genealogists who exploited a loophole in a commercial database called GEDmatch, allowing them to search the DNA of individuals who explicitly opted out of sharing their genetic information with police.

The loophole, which a source demonstrated for The Intercept, allows genealogists working with police to manipulate search fields within a DNA comparison tool to trick the system into showing opted-out profiles. In records of communications reviewed by The Intercept, Moore and two other forensic genetic genealogists discussed the loophole and how to trigger it. In a separate communication, one of the genealogists described hiding the fact that her organization had made an identification using an opted-out profile.

The communications are a disturbing example of how genetic genealogists and their law enforcement partners, in their zeal to close criminal cases, skirt privacy rules put in place by DNA database companies to protect their customers. How common these practices are remains unknown, in part because police and prosecutors have fought to keep details of genetic investigations from being turned over to criminal defendants. As commercial DNA databases grow, and the use of forensic genetic genealogy as a crime-fighting tool expands, experts say the genetic privacy of millions of Americans is in jeopardy.

Moore did not respond to The Intercept's requests for comment.

"If we can't trust these practitioners, we certainly cannot trust law enforcement."

To Tiffany Roy, a DNA expert and lawyer, the fact that genetic genealogists have accessed private profiles – while simultaneously preaching about ethics – is troubling. "If we can't trust these practitioners, we certainly cannot trust law enforcement," she said. "These investigations have serious consequences; they involve people who have never been suspected of a crime." At the very least, law enforcement actors should have a warrant to conduct a genetic genealogy search, she said. "Anything less is a serious violation of privacy."

CeCe Moore appears as a guest on "Megyn Kelly Today" on Aug. 14, 2018. Photo: Zach Pagano/NBCU Photo Bank/NBCUniversal via Getty Images

The Wild West

Forensic genetic genealogy evolved from the direct-to-consumer DNA testing craze that took hold roughly a decade ago. Companies like 23andMe and Ancestry offered DNA analysis and a database where results could be uploaded and searched against millions of other profiles, offering consumers a powerful new tool to dig into their heritage through genetics.

It wasn't long before entrepreneurial genealogists realized this information could also be used to solve criminal cases, especially those that had gone cold. While the arrest of the Golden State Killer captured

national attention, it was not the first case solved by forensic genetic genealogy. Two weeks earlier, genetic genealogists Margaret Press and Colleen Fitzpatrick joined officials in Ohio to announce that "groundbreaking work" had allowed authorities to identify a young woman whose body was found by the side of a road back in 1981. Formerly known as "Buckskin Girl" for the handmade pullover she wore, Marcia King was given her name back through genetic genealogy. "Everyone said it couldn't be done," Press said.

MOST READ

Georgia GOP Gears Up to Remove Atlanta Prosecutor Who Indicted Donald Trump

Akela Lacy

Biden Administration Adds Insulin to Drug Price Negotiation List in Major Blow to Big Pharma

Ryan Grim

NSA Orders Employees to Spy on the World "With Dignity an Respect"

Ken Klippenstein

The type of consumer DNA information used in forensic genetic genealogy is far different from that uploaded to the Combined DNA Index System, or CODIS, a decades-old network administered by the FBI. The DNA entered in CODIS comes from individuals convicted of or arrested for serious crimes and is often referred to as "junk" DNA: short pieces of unique genetic code that don't carry any individual health or trait information. "It's not telling us how the person looks. It's not telling us about their heritage or their phenotypic traits," Roy said. "It's a string of numbers, like a telephone number."

In contrast, the DNA testing offered by direct-to-consumer companies is "as sensitive as it gets," Roy said. "It tells you about your origins. It tells you about your relatives and your parentage, and it tells you about your disease propensity." And it has serious reach: While CODIS searches the

DNA of people already identified by the criminal justice system, the commercial databases have the potential to search through the DNA of everyone else.

Individuals can upload their test results to any number of databases; at present, there are five main commercial portals. Ancestry and 23andMe are the biggest players in the field, with databases containing roughly 23 million and 14 million profiles. Individuals must test with the companies to gain access to their databases; neither allow DNA results obtained from a different testing service. Both Ancestry and 23andMe forbid police, and the genetic genealogists who work with them, from accessing their data for crime-fighting purposes. "We do not allow law enforcement to use Ancestry's service to investigate crimes or to identify human remains" absent a valid court order, Ancestry's privacy policy notes. The two companies provide regular transparency reports documenting law enforcement requests for user information.

MyHeritage, home to some 7 million DNA profiles, similarly bars law enforcement searches, but it does allow individuals to upload DNA results obtained from other sources.

And then there are FamilyTreeDNA and GEDmatch, which grant police access but give users the choice of opting in or out. Both allow anyone to upload their DNA results and have upward of 1.8 million profiles. But neither company routinely publicizes the number of customers who have opted in, said Leah Larkin, a veteran genetic genealogist and privacy advocate from California. Larkin writes about issues in the field – including forensic genetic genealogy, which she does not practice – on her website the DNA Geek. Larkin estimates that roughly 700,000 GEDmatch profiles are opted in. She suspects that even more are opted in on FamilyTreeDNA; opting in is the default for the company's U.S. customers and "it's not obvious how to opt out."

But even opting out of law enforcement searches doesn't guarantee that a profile won't be accessed: A loophole in GEDmatch offers users working with law enforcement agencies a back door to accessing protected profiles. A source showed The Intercept how to exploit the loophole; it was not an obvious weakness or one that could be triggered mistakenly. Rather, it was a back door that required experience with the platform's various tools to open.

GEDmatch's parent company, Verogen, did not respond to a request for comment.

Law enforcement officials leave the home of accused serial killer Joseph James DeAngelo in Citrus Heights, Calif., on April 24, 2018. Photo: Justin Sullivan/Getty Images

An Open Secret

In forensic genetic genealogy circles, the GEDmatch loophole had long been an open secret, sources told The Intercept, one that finally surfaced publicly during the Ramapo College conference in late July.

Roy, the DNA expert, was giving a presentation titled "In the Hot Seat," a primer for genealogists on what to expect if called to testify in a criminal case. There was a clear and simple theme: "Do not lie," Roy said. "The minute you're caught in a lie is the minute that it's going to be difficult for people to use your work."

As part of the session, David Gurney, a professor of law and society at Ramapo and director of the college's nascent Investigative Genetic Genealogy Center, joined Roy for a mock questioning of Cairenn Binder, a genealogist who heads up the center's certificate program.

Gurney, simulating direct examination, walked Binder through a series of friendly questions. Did she have access to DNA evidence or genetic code during her investigations? No, she replied. Could she see everyone who'd uploaded DNA to the databases? No, she said, only those who'd opted in to law enforcement searches.

Roy, playing the part of opposing counsel, was pointed in her cross-examination: Was Binder aware of the GEDmatch loophole? And had she used it? Yes, Binder said. "How many times?" Roy asked.

"A handful," Binder replied. "Maybe up to a dozen."

Binder's answers quickly made their way into a private Facebook group for genetic genealogy enthusiasts, prompting a response from the DNA Doe Project, a volunteer-driven organization led by Press, one of the women who identified the Buckskin Girl. Before joining Ramapo College, Binder had worked for the DNA Doe Project.

In a statement posted to the Facebook group, Pam Lauritzen, the project's communications director, said the loophole was an artifact of

changes GEDmatch implemented in 2019, when it made opting out the default for all profiles. "While we knew that the intent of the change was to make opted-out users unavailable, some volunteers with the DNA Doe Project continued to use the reports that allowed access to profiles that were opted out," she wrote. That use was neither "encouraged nor discouraged," she continued. Still, she claimed the access was somehow "in compliance" with GEDmatch's terms of service – which at the time promised that DNA uploaded for law enforcement purposes would only be matched with customers who'd opted in – and that the loophole was closed "years ago."

It was a curious statement, particularly given that Press, the group's co-founder, was among the genealogists who discussed the GEDmatch loophole in communications reviewed by The Intercept. In 2020, she described the DNA Doe Project using an opted-out profile to make an identification – and devising a way to keep that quiet.

Press referred The Intercept's questions to the DNA Doe Project, which declined to comment.

In July 2020, GEDmatch was hacked, which resulted in all 1.45 million profiles then contained in the database to be briefly opted in to law enforcement matching; at the time, BuzzFeed News reported, just 280,000 profiles had opted in. GEDmatch was taken offline "until such time that we can be absolutely sure that user data is protected against potential attacks," Verogen wrote on Facebook.

In the wake of the hack, a genetic genealogist named Joan Hanlon was asked by Verogen to beta test a new version of the site. According to records of a conversation reviewed by The Intercept, Press and Moore, the featured speaker at the Ramapo conference, discussed with Hanlon their tricks to access opted-out profiles and whether the new website had plugged all backdoor access. It hadn't. It's unclear if anyone told Verogen; as of this month, the back door was still open.

Hanlon did not respond to The Intercept's requests for comment.

In January 2021, GEDmatch changed its terms of service to opt everyone in for searches involving unidentified human remains, making the back door irrelevant for genealogists who only worked on Doe cases, but not those working with authorities to identify perpetrators of violent crimes.

Undisclosed Methods

Exploitation of the GEDmatch loophole isn't the only example of genetic genealogists and their law enforcement partners playing fast and loose with the rules.

Law enforcement officers have used genetic genealogy to solve crimes that aren't eligible for genetic investigation per company terms of service and Justice Department guidelines, which say the practice should be reserved for violent crimes like rape and murder only when all other "reasonable" avenues of investigation have failed. In May, CNN reported on a U.S. marshal who used genetic genealogy to solve a decades-old prison break in Nebraska. There is no prison break exception to the eligibility rules, Larkin noted in a post on her website. "This case should never have used forensic genetic genealogy in the first place."

A month later, Larkin wrote about another violation, this time in a California case. The FBI and the Riverside County Regional Cold Case Homicide Team had identified the victim of a

"This case should never have used forensic genetic

1996 homicide using the MyHeritage database — an explicit violation of the company's terms of service, which make clear that using the database for law enforcement purposes is "strictly prohibited" absent a court order.

genealogy in the first place."

"The case presents an example of 'noble cause bias,'" Larkin wrote, "in which the investigators seem to feel that their objective is so worthy that they can break the rules in place to protect others."

MyHeritage did not respond to a request for comment. The Riverside County Sheriff's Office referred questions to the Riverside district attorney's office, which declined to comment on an ongoing investigation. The FBI also declined to comment.

Violations have even come from inside the DNA testing companies. Back in 2019, GEDmatch co-founder Curtis Rogers unilaterally made an exception to the terms of service, without notifying the site's users, to allow police to search for someone suspected of assault in Utah. It was a tough call, Rogers told BuzzFeed News, but the case in question "was as close to a homicide as you can get."

It appears that violations have also spread to Ancestry, which prohibits the use of its DNA data for law enforcement purposes unless the company is legally compelled to provide access. Genetic genealogists told The Intercept that they are aware of examples in which genealogists working with police have provided AncestryDNA testing kits to the possible relatives of suspects — what's known as "target testing" — or asked customers for access to preexisting accounts as a way to unlock the off-limits data.

A spokesperson for Ancestry did not answer The Intercept's questions about efforts to unlock DNA data for law enforcement purposes via a

third party. Instead, in a statement, the company reiterated its commitment to maintaining the privacy of its users. "Protecting our customers' privacy and being good stewards of their data is Ancestry's highest priority," it read. The company did not respond to follow-up questions.

As it turns out, the genetic genealogy work in the Golden State Killer case was also questionable: The break that led to DeAngelo came after genealogist Barbara Rae-Venter uploaded DNA from the double murder to MyHeritage, according to the Los Angeles Times. Rae-Venter told the Times that she didn't notify the company about what she was doing but that her actions were approved by Steve Kramer, the FBI's Los Angeles division counsel at the time. "In his opinion, law enforcement is entitled to go where the public goes," Rae-Venter told the paper.

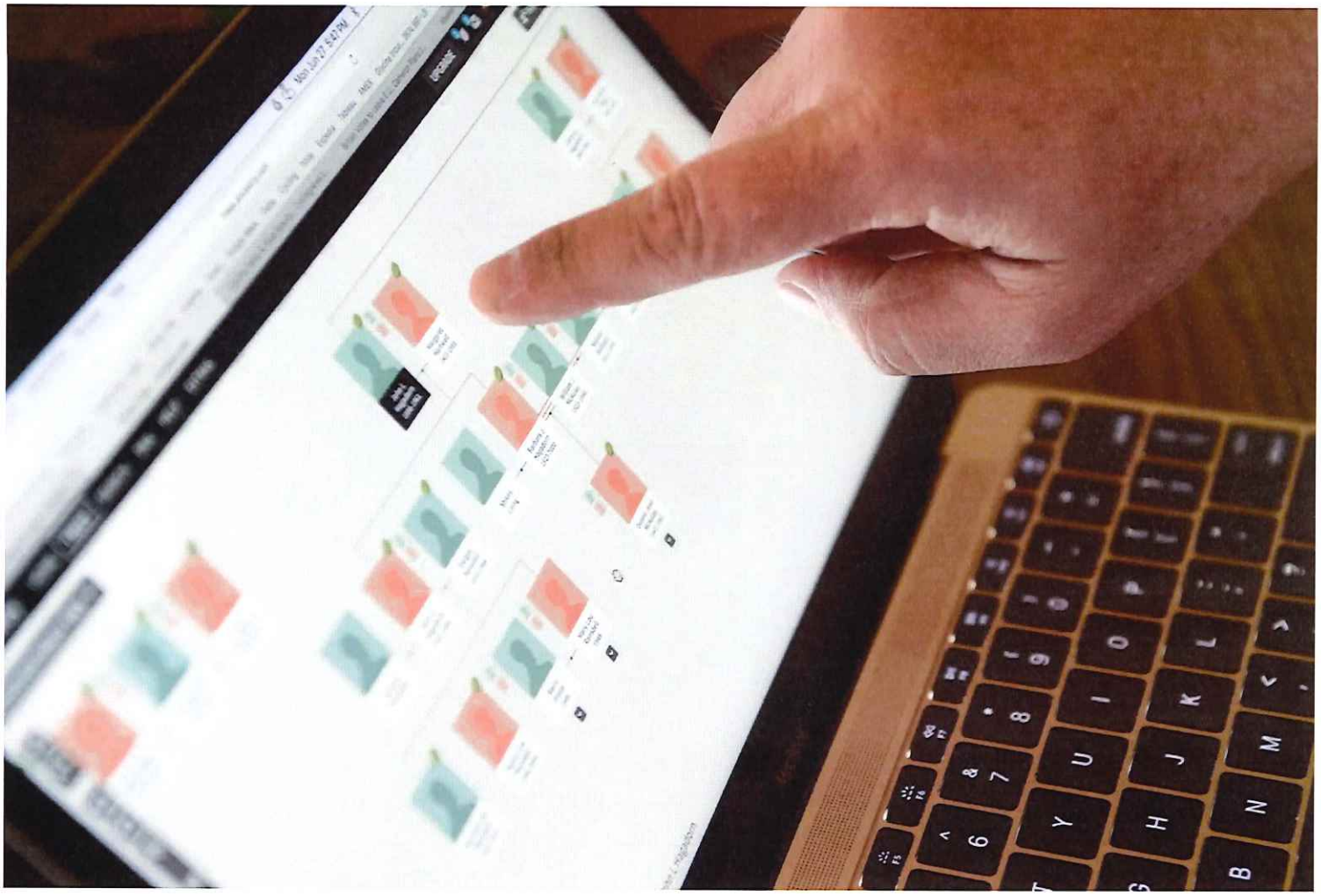
Just how prevalent these practices are may never fully be known, in part because police and prosecutors regularly seek to shield genetic investigations from being vetted in court. They argue that what they obtain from forensic genetic genealogy is merely a tip, like information provided by an informant, and is exempt from disclosure to criminal defendants.

That's exactly what's happening in Idaho, where Bryan Kohberger is awaiting trial for the 2022 murder of four university students. For months, the state failed to disclose that it had used forensic genetic genealogy to identify Kohberger as a suspect. A probable cause statement methodically laying out the evidence that led cops to his door conspicuously omitted any mention of genetic genealogy. Kohberger's defense team has asked to see documents related to the genealogy work as it prepares for an October trial, but the state has refused, saying the defense has no right to any information about the genetic genealogy it used to crack the case.

Prosecutors said it was the FBI that did the genetic genealogy work, and few records were created in the process, leaving little to turn over. But the state also argued that it couldn't turn over information because the family tree the FBI created was extensive – including "the names and personal information of … hundreds of innocent relatives" – and the privacy of those individuals needed to be maintained. According to the state, it shouldn't even have to say which genetic database – or databases – it used.

Kohberger's attorneys argue that the state's position is preposterous and keeps them from ensuring that the work undertaken to find Kohberger was above board. "It would appear that the state is acknowledging that the companies are providing personal information to the state and that those companies and the government would suffer if the public were to realize it," one of Kohberger's attorneys wrote. "The statement by the government implies that the databases searched may be ones that law enforcement is specifically barred from, which explains why they do not want to disclose their methods."

A hearing on the issue is scheduled for August 18.



An AncestryDNA user points to his family tree on Ancestry.com on June 24, 2016. Photo: RJ Sangosti/The Denver Post via Getty Images

"A Search of All of Us"

Natalie Ram, a law professor at the University of Maryland Carey School of Law and an expert in genetic privacy, believes forensic genetic genealogy is a giant fishing expedition that fails the particularity requirement of the Fourth Amendment: that law enforcement searches be targeted and based on individualized suspicion. Finding a match to crime scene DNA by searching through millions of genetic profiles is the opposite of targeted. Forensic genetic genealogy, according to Ram, "is fundamentally a search of all of us every time they do it."

While proponents of forensic genetic genealogy say the individuals they're searching have willingly uploaded their genetic information and opted in to law enforcement access, Ram and others aren't so sure that's the case, even when practitioners adhere to terms of service. If the consent is truly informed and voluntary, "then I think that it would be ethical, lawful, permissible for law enforcement to use that DNA … to identify those individuals who did the volunteering," Ram said. But that's not who is being identified in these cases. Instead, it's relatives – and sometimes very distant relatives. "Our genetic associations are involuntary. They're profoundly involuntary. They're involuntary in a way that almost nothing else is. And they're also immutable," she said. "I can estrange myself from my family and my siblings and deprive them of information about what I'm doing in my life. And yet their DNA is informative on me."

Jennifer Lynch, general counsel at the Electronic Frontier Foundation, agrees. "We're putting other people's privacy on the line when we're trying to upload our own genetic information," she said. "You can't consent for another person. And there's just not an argument that you have consented for your genetic information to be in a database when it's your brother who's uploaded the information, or when it's somebody you don't even know who is related to you."

Related

Orange County Prosecutors Operate "Vast, Secretive" Genetic Surveillance Program

To date, efforts to rein in the practice as a violation of the Fourth Amendment have presented some problems. A person whose arrest was built on a foundation of genetic genealogy, for example, might have been harmed by the genealogical fishing expedition but lack standing

to bring a case; in the strictest sense, it wasn't their DNA that was searched. In contrast, a third cousin whose DNA was used to identify a suspect could have standing to bring a suit, but they might be hard-pressed to prove they were harmed by the search.

If police are getting hits to suspects by violating companies' terms of service — using databases that bar police searching — that "raises some serious Fourth Amendment questions" because no expectation of privacy has been waived, Ram said. Of course, ferreting out such violations would require that the information be disclosed in court, which isn't happening.

At present, the only real regulators of the practice are the database owners: private companies that can change hands or terms of service with little notice. GEDmatch, which has at least once bent its terms to accommodate police, was started by two genealogy hobbyists and then sold to the biotech company Verogen, which in turn was acquired last winter by another biotech company, Qiagen. Experts like Ram and Lynch worry about the implications of so much sensitive information held in for-profit hands — and readily exploited by police. The "platforms right now are the most powerful regulators we have for most Americans," Ram said. Police regulate "after a fashion, in a fashion, by what they do. They tell us what they're willing to do by what they actually do," she added. "But by the way, that's like law enforcement making rules for itself, so not exactly a diverse group of stakeholders."

For now, Ram said, the best way to regulate forensic genetic genealogy is by statute. In 2021, Maryland lawmakers passed a comprehensive law to restrain the practice. It requires police to obtain a warrant before conducting a genetic genealogy search — certifying that the case is an eligible violent felony and that all other reasonable avenues of investigation have failed — and notify the court before gathering DNA

evidence to confirm the suspect identified via genetic genealogy is, in fact, the likely perpetrator. Currently, police use surreptitious methods to collect DNA without judicial oversight: mining a person's garbage, for example, for items expected to contain biological evidence. In the Golden State Killer case, DeAngelo was implicated by DNA on a discarded tissue.

The Maryland law also requires police to obtain consent from any third party whose DNA might help solve a crime. In the Kohberger case, police searched his parents' garbage, collecting trash with DNA on it that the lab believed belonged to Kohberger's father. In a notorious Florida case, police lied to a suspect's parents to get a DNA sample from the mother, telling her they were trying to identify a person found dead whom they believed was her relative. Those methods are barred under the Maryland law.

Montana and Utah have also passed laws governing forensic genetic genealogy, though neither is as strict as Maryland's.

MyHeritage DNA kits are displayed at the RootsTech conference in Salt Lake City on Feb. 9, 2017. Photo: George Frey/Bloomberg via Getty Images

Solving Crime Before It Happens

The rise of direct-to-consumer DNA testing and forensic genetic genealogy raises another issue: the looming reality of a de facto national DNA database that can identify large swaths of the U.S. population, regardless of whether those individuals have uploaded their genetic information. In 2018, researchers led by the former chief science officer at MyHeritage predicted that a database of roughly 3 million people could identify nearly 100 percent of U.S. citizens of European descent. "Such a database scale is foreseeable for some third-party websites in the near future," they concluded.

"All of a sudden, we have a national DNA database," said Lynch, "and we didn't ever have any kind of debate about whether we wanted that in our society." A national database in "private hands," she added.

"All of a sudden, we have a national DNA database, and we didn't ever have any kind of debate about whether we wanted that in our society."

By the time people started worrying about this as a policy issue, it was "too late," Moore said during her address at the Ramapo conference. "By the time the vast majority of the public learned about genetic genealogy, we'd been quietly building this incredibly powerful tool for human identification behind the scenes," she said. "People sort of laughed, like, 'Oh, hobbyists … you do your genealogy, you do your adoption,' and we were allowed to build this tool without interference."

Moore advocated for involving forensic genetic genealogy earlier in the investigative process. Doing so, she argued, could focus police on guilty parties more quickly and save innocent people from needless law enforcement scrutiny. In fact, she told the audience, she believes that forensic genetic genealogy can help to eradicate crime. "We can stop criminals in their tracks," she said. "I really believe we can stop serial killers from existing, stop serial rapists from existing."

"We are an army. We can do this! So repeat after me," Moore said, before leading the audience in a chant. "No more serial killers!"

Update: August 18, 2023, 3:55 p.m. ET

After this article was published, Margaret Press, founder of the DNA Doe Project, released a statement in response to The Intercept's findings. Press acknowledged that between May 2019 and January 2021, the organization's leadership and volunteers made use of GEDmatch tools that provided access to DNA profiles that were opted out of law enforcement searches, which she described as "a bug in the software." Press stated:

> *We have always been committed to abide by the Terms of Service for the databases we used, and take our responsibility to our law enforcement and medical examiner partner agencies extremely seriously. In hindsight, it's clear we failed to consider the critically important need for the public to be able to trust that their DNA data will only be shared and used with their permission and under the restrictions they choose. We should have reported these bugs to GEDmatch and stopped using the affected reports until the bugs were fixed. Instead, on that first day when we found that all of the profiles were set to opt-out, I discouraged our team from reporting them at all. I now know I was wrong and I regret my words and actions.*

WAIT! BEFORE YOU GO on about your day, ask yourself: How likely is it that the story you just read would have been produced by a different news outlet if The Intercept hadn't done it?

Consider what the world of media would look like without The Intercept. Who would hold party elites accountable to the values they proclaim to have? How many covert wars, miscarriages of justice, and dystopian technologies would remain hidden if our reporters weren't on the beat?

The kind of reporting we do is essential to democracy, but it is not easy, cheap, or profitable. The Intercept is an independent nonprofit news outlet. We don't have ads, so we depend on our members to help us hold the powerful to account. Joining is simple and doesn't need to cost a lot: You can become a sustaining member for as little as $3 or $5 a month. That's all it takes to support the journalism you rely on.

We're independent of corporate interests. Will you help us?

CONTACT THE AUTHOR:

Jordan Smith

jordan.smith@theintercept.com

@chronic_jordan

RELATED

Orange County Prosecutors Operate "Vast, Secretive" Genetic Surveillance Program

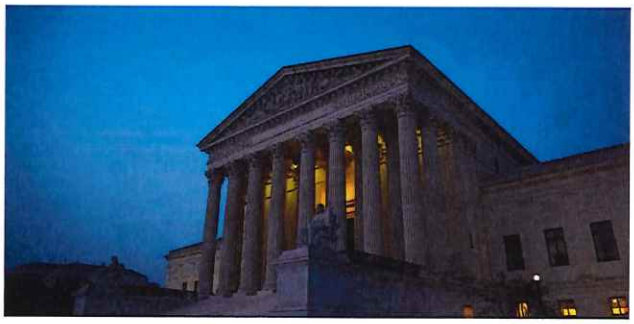
DHS Plans to Start Collecting Eye Scans and DNA — With the Help of Defense Contractors

LATEST STORIES

Meta Overhauls Controversial "Dangerous Organizations" Censorship Policy

Sam Biddle - 12:32 pm

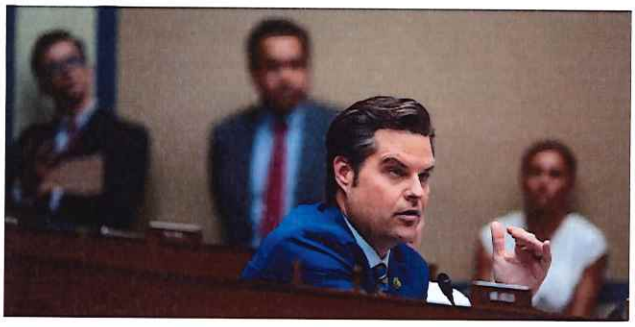
In an internal update obtained by The Intercept, Facebook and Instagram's parent company admits its rules stifled legitimate political speech.



Payday Lenders Gave Millions to Republican Group That Backed Supreme Court Suit to Annihilate CFPB

Akela Lacy - 7:47 am

The Republican Attorneys General Association fought to help a Supreme Court case against the Consumer Finance Protection Bureau.



Matt Gaetz Wants to Make the Pentagon Answer for Training Coup Leaders

Nick Turse - 7:00 am

By targeting the defense budget, Gaetz demands the military tell Congress about trainees who "broke bad."

Idaho State Police

Service Since 1939

Colonel Kedrick R. Wills
Director

Brad Little
Governor

To: Idaho Chiefs, Sheriffs, and Prosecutors
From: Matthew Gamette, ISP Forensic Services Laboratory System Director
Subject: **Cold Case Help—Molecular Genealogy Resources**
Date: July 28, 2021

The Idaho State Police Forensic Services Laboratory (ISPFS) is extremely excited to announce that we have secured a Bureau of Justice Assistance grant to fund genetic genealogy testing and searching of unsolved Idaho cases. The cases we are starting with are unsolved homicide, sexual assault, and missing person/unidentified remains cases. Idaho is the first state in the country to take the state-wide approach for this technology. Instead of each law enforcement (LE) agency having to negotiate their own contract, pricing, and quality control with a private lab and genealogist, ISPFS has done that at the state level through the Idaho Department of Purchasing. In addition, by ISPFS securing federal grant funding, we can offer these services to local, county, and state agencies at no cost to the local LE agency. In order to facilitate this, ISPFS has formed a State Genetic Genealogy Investigation team consisting of laboratory personnel, an Idaho State Police investigator/detective, and a representative from the Rocky Mountain Information Network (RMIN) to identify cases eligible for testing under this grant. Once a case is identified as eligible, the team is reaching out to the local law enforcement agency and prosecutor to bring them onto the team for that case. The state team is a resource for local LE. Idaho now has a formal contract with Othram Laboratories (a prominent leader in forensic genealogy) to conduct the genealogy testing and forensic genealogy searching. ISPFS is ensuring that Othram follows accepted laboratory processes and procedures, and complies with the United States DOJ interim policy on Forensic Genetic Genealogy DNA Analysis and Searching.

ISPFS has already searched our records for cases we know would be eligible under this program. We have started contacting individual Idaho law enforcement entities and prosecutors on approximately 15 of those cases. The law enforcement entity and prosecuting attorney are being asked to confirm certain case criteria and sign an MOU that they will investigate this case if the molecular genealogy technique generates investigative leads, that they will follow DOJ policy for investigating these cases, and that they will take all appropriate prosecution actions as an outcome of the investigation.

We want to be very clear that the local or county law enforcement agency will retain jurisdiction and responsibility for the case. The state team is in place to identify cases, coordinate with local entities, provide investigation resources (if requested), safeguard that the molecular genealogy technology and techniques are being appropriately used in Idaho, and ensure that all necessary resources are reliable and available at no cost to local LE for use of this technique. ISPFS is committed to ensuring that the lab science and genealogy work is robust, that the evidence is treated appropriately by the contract lab and in a way that allows for appropriate prosecution, and that the contract with the private lab and federal funding are spent appropriately. If more funding resources are needed to support this effort, ISPFS will obtain those resources in support of all Idaho law enforcement. ISPFS is also evaluating offering these services in Idaho if the need is demonstrated from this project.

We are accepting requests to work other cases that have not been identified by our team. If you have those cases, please reach out to our appointed project lead on this effort Ms. Rylene Nowlin. She can be reached at 208-884-7148 or Rylene.Nowlin@isp.idaho.gov All cases accepted into this program are subject to an MOU.

UNITED STATES DEPARTMENT OF JUSTICE
INTERIM POLICY
FORENSIC GENETIC GENEALOGICAL DNA ANALYSIS AND SEARCHING

I. Purpose and Scope[1]

The purpose of this interim policy is to promote the reasoned exercise of investigative, scientific, and prosecutorial discretion in cases that involve forensic genetic genealogical DNA analysis and searching ('FGGS').[2] It provides guidance to Department agencies when formulating a thoughtful and collaborative approach to important interdisciplinary decisions in cases that utilize this investigative technique. Collaboration between investigators, laboratory personnel, and prosecutors is important because the decision to pursue FGGS may affect privacy interests, the consumption of forensic samples, and law enforcement's ability to solve violent crime.

The Department must use FGGS in a manner consistent with the requirements and protections of the Constitution and other legal authorities. Moreover, the Department must handle information and data derived from FGGS in accordance with applicable laws, regulations, policies, and procedures. When using new technologies like FGGS, the Department is committed to developing practices that protect reasonable interests in privacy, while allowing law enforcement to make effective use of FGGS to help identify violent criminals, exonerate innocent suspects, and ensure the fair and impartial administration of justice to all Americans.

The Department will continue to assess its investigative tools and techniques to ensure that its policies and practices properly reflect its law enforcement mission and its commitment to respect individual privacy and civil liberties. This interim policy establishes general principles for the use of FGGS by Department components during criminal investigations and in other circumstances that involve Department resources, interests, and equities.

The scope of this interim policy is limited to the requirements set forth herein. It does not control investigative, scientific, or prosecutorial activities or decisions not specifically addressed. The Department's individual law enforcement components may issue additional guidance that is consistent with the provisions of this interim policy.

---

[1] This interim policy provides Department components with internal guidance. It is not intended to, does not, and may not be relied upon to create any substantive or procedural rights or benefits enforceable at law or in equity by any party against the United States or its departments, agencies, entities, officers, employees, agents, or any other person in any matter, civil or criminal. This interim policy does not impose any legal limitations on otherwise lawful investigative or prosecutorial activities or techniques utilized by the Department of Justice, or limit the prerogatives, choices, or decisions available to, or made by, the Department in its discretion.

[2] As used in this interim policy, the term 'forensic genetic genealogical DNA analysis and searching,' or 'FGGS,' means the forensic genetic genealogical DNA analysis of a forensic or reference sample of biological material by a vendor laboratory to develop an FGG profile and the subsequent search of that profile in a publicly-available open-data personal genomics database or a direct-to-consumer genetic genealogy service.

Approved: 09.02.2019

Effecti

II. Application

This interim policy applies to: 1) all criminal investigations in which an investigative agency in the Department of Justice ('investigative agency')[3] has exclusive or concurrent jurisdiction of the crime under investigation and the agency has lawful custody, control, or authority to use a forensic sample for FGG/FGGS; or 2) any criminal investigation in which the Department provides funding to a federal, state, local, or tribal agency to conduct FGG/FGGS; or 3) any criminal investigation in which Department employees or contractors conduct genealogical research on leads generated through the use of FGGS; or 4) any federal agency or any unit of state, local, or tribal government that receives grant award funding from the Department that is used to conduct FGG/FGGS.[4]

III. Background

a. STR DNA Typing and CODIS

Forensic DNA typing has historically been used to compare 13-20 STR DNA markers[5] between a forensic sample[6] and one or more reference samples.[7] When a suspect's identity is unknown, a participating crime laboratory may upload a forensic profile[8] into the FBI's Combined DNA Index System (CODIS). CODIS is a law enforcement database that compares DNA profiles derived from forensic samples to those of known offenders.

CODIS was created by the DNA Identification Act of 1994, Pub. L. No. 103-322 (1994), codified at 34 U.S.C. § 12592. This legislation authorized the FBI to create and maintain a national database comprised of designated DNA indices that are routinely searched against one another. If a CODIS search results in a confirmed match between a forensic profile and a known offender, a law enforcement lead is generated and the name of the matching offender is released. If the search does not result in a confirmed match, no lead is generated.

---

[3] As used in this interim policy, the term 'investigative agency' includes any federal, state, local, or tribal law enforcement agency that receives funding from the Department of Justice to conduct FGG/FGGS.

[4] The Department will implement this policy under its federal grant programs (as applicable) through the inclusion of a specific condition(s) in federal awards.

[5] STR DNA typing is a widely-used forensic DNA technology that examines 13-20 (or more) genetic locations on the non-sex chromosomes that contain 2 to 6 base-paired segments known as nucleotides, which tandemly repeat at each location. A 'marker' is a genetic locus, or location.

[6] A 'forensic sample' is biological material reasonably believed by investigators to have been deposited by a putative perpetrator and that was collected from a crime scene, a person, an item, or a location connected to the criminal event. For purposes of this interim policy, the term 'forensic sample' also includes the unidentified human remains of a suspected homicide victim.

[7] A 'reference sample' is biological material from a known source.

[8] As used in this interim policy, 'forensic profile' means an STR DNA typing result, and an STR and/or mitochondrial DNA typing result for unidentified human remains, derived from a forensic sample.

b. Forensic Genetic Genealogical DNA Analysis and Searching

Forensic genealogy is law enforcement's use of DNA analysis combined with traditional genealogy research to generate investigative leads for unsolved violent crimes. Forensic genetic genealogical DNA analysis ('FGG') differs from STR DNA typing in both the type of technology employed and the nature of the databases utilized.

FGG examines more than half a million single nucleotide polymorphisms[9] ('SNPs'), which replace the STR DNA markers analyzed in traditional forensic DNA typing. These SNPs span the entirety of the human genome. This allows scientists to identify shared blocks of DNA between a forensic sample and the sample donor's potential relatives. Recombination or reshuffling of the genome is expected as DNA from each generation is passed down, resulting in larger shared blocks of identical DNA between closer relatives and shorter blocks between more distant relatives. Due to predicted levels of recombination between generations, it is possible to analyze these blocks of genetic information and make inferences regarding potential familial relationships.

Department laboratories currently do not analyze SNPs during forensic DNA casework. Thus, in appropriate cases, it is necessary to outsource biological material to vendor laboratories that perform FGG.[10] After a forensic or reference sample is genotyped by a vendor laboratory, the resulting FGG profile[11] is entered into one or more publicly-available open-data personal genomics DNA databases or direct-to-consumer genetic genealogy services ('DTC service(s)')[12] (collectively referred to herein as 'GG service(s)'). The FGG profile is then compared by automation against the genetic profiles of individuals who have voluntarily submitted their biological samples or entered their genetic profiles into these GG services ('service users'). A computer algorithm is used to evaluate potential familial relationships between the (forensic or reference) sample donor and service users.

It is important to note that personal genetic information is not transferred, retrieved, downloaded, or retained by GG service users — including law enforcement — during the automated search and comparison process. In addition, the investigative use of FGGS involves different DNA technologies, genetic markers, algorithms, and databases from those used by

---

[9] 'Single nucleotide polymorphisms' are DNA sequence variations that occur when a single nucleotide (A, T, G, or C) in a genomic sequence is altered. These variations may be used to distinguish people for purposes of biological relationship testing.

[10] Contracts with vendor laboratories for FGG services should be reviewed by legal counsel to ensure that they contain appropriate language requiring maintenance of privacy and security controls for handling biological samples, FGG profiles, and other information and data both submitted to, and generated by, those vendor laboratories.

[11] The term 'FGG profile' means the SNP-based genetic profile generated from a forensic or reference sample by a vendor laboratory for the purpose of conducting FGGS.

[12] Direct-to-consumer genetic genealogy services are companies that offer a variety of DNA genomics tests and/or genetic genealogy services directly to the public (rather than through clinical health care providers), typically via customer access to secure online websites.

CODIS. Information and data derived from FGGS is not, and cannot be, uploaded, searched, or retained in any CODIS DNA Index.

IV. Limitations

If the search of an FGG profile results in one or more genetic associations,[13] the GG service typically generates and provides the service user with a list of genetically associated service usernames along with an estimated relationship and (in some cases) the amount of DNA shared by those individuals. A genetic association means that the donor of the (forensic or reference) sample may be related to a service user. However, information derived from genetic associations is used by law enforcement only as an investigative lead. Traditional genealogy research and other investigative work is needed to determine the true nature of any genetic association.

A suspect shall not be arrested based solely on a genetic association generated by a GG service. If a suspect is identified after a genetic association has occurred, STR DNA typing must be performed, and the suspect's STR DNA profile must be directly compared to the forensic profile previously uploaded to CODIS.[14] This comparison is necessary to confirm that the forensic sample could have originated from the suspect.

V. Case Criteria

Investigative agencies may initiate the process of considering the use of FGGS when a case involves an unsolved violent crime[15] and the candidate forensic sample[16] is from a putative perpetrator,[17] or when a case involves what is reasonably believed by investigators to be the unidentified remains of a suspected homicide victim ('unidentified human remains'). In addition, the prosecutor, as defined in footnote twenty of this interim policy, may authorize the investigative use of FGGS for violent crimes or attempts to commit violent crimes other than homicide or sexual offenses (while observing and complying with all requirements of this

[13] A 'genetic association' is determined by the amount of DNA shared between two individuals whose genetic profiles (including, in some cases, an FGG profile) have been entered into a GG service. This amount is measured and reported in centiMorgans. In general, the more DNA shared between two individuals, the higher the number of centiMorgans and the closer the genetic kinship relationship.

[14] Manual comparison is sufficient.

[15] As used in this interim policy, the term 'violent crime' means any homicide or sex crime, including a homicide investigation during which FGGS is used in an attempt to identify the remains of a suspected homicide victim. It also includes other serious crimes and criminal offenses designated by a GG service for which investigative use of its service by law enforcement has been authorized by that service.

[16] A 'candidate forensic sample' is: 1) the remaining portion of a forensic sample or extract being considered for FGGS, and from which a forensic profile was previously derived and uploaded to CODIS; or 2) one or more additional forensic samples or extracts from the same case that share the same forensic profile(s) as that derived from the forensic sample(s) uploaded to CODIS.

[17] A 'putative perpetrator' is one or more criminal actors reasonably believed by investigators to be the source of, or a contributor to, a forensic sample deposited during, or incident to, the commission of a crime.

interim policy) when the circumstances surrounding the criminal act(s) present a substantial and ongoing threat to public safety or national security. Before an investigative agency may attempt to use FGGS, the forensic profile derived from the candidate forensic sample must have been uploaded to CODIS, and subsequent CODIS searches must have failed to produce a probative and confirmed DNA match.

The investigative agency with jurisdiction of either the crime or the location where the unidentified human remains were discovered (if different) must have pursued reasonable investigative leads[18] to solve the case or to identify the unidentified human remains. Finally, when applicable, relevant case information must have been entered into the National Missing and Unidentified Persons System ('NamUs') and the Violent Criminal Apprehension Program ('ViCAP') national database.[19]

VI. Investigative Collaboration

If each of the criteria set forth in Section V has been satisfied, the investigative agency shall contact a designated official at the CODIS laboratory ('designated laboratory official' or 'DLO') that uploaded the forensic profile to CODIS. The DLO must determine if the candidate forensic sample is from a single source contributor or is a deduced mixture. The DLO will also assess the candidate forensic sample's suitability (e.g., quantity, quality, degradation, mixture status, etc.) for FGG and advise the investigative agency about the results of that evaluation. In addition, the DLO may advise the investigative agency of any reasonable scientific alternatives to FGGS, given the nature and condition of the candidate forensic sample, and the availability of other DNA technologies or techniques. The investigative agency shall document its consultation with the DLO.

After consulting with the DLO, the investigative agency shall contact the prosecutor.[20] The investigative agency shall advise the prosecutor of the nature and status of the investigation, the results of the DLO's evaluation of the candidate forensic sample, and any reasonable scientific alternatives to FGGS provided by the DLO.[21] After discussing these issues, and based on the information provided, the prosecutor and the investigative agency must agree that the

---

[18] 'Reasonable investigative leads' are credible, case-specific facts, information, or circumstances that would lead a reasonably cautious investigator to believe that their pursuit would have a fair probability of identifying a suspect.

[19] This latter requirement only applies if the case meets relevant ViCAP case entry criteria.

[20] As used in this interim policy, the term 'prosecutor' refers, as applicable, to the Assistant Attorney General, United States Attorney, state or local prosecuting attorney, or state attorney general (or his or her designee), with jurisdiction of either the crime under investigation or the location where the unidentified human remains were discovered (if different). When the Department of Justice and one or more state or local prosecuting authorities have concurrent jurisdiction of the crime(s) under investigation, the 'prosecutor' means the Assistant Attorney General, United States Attorney, or the state or local prosecuting official whose office will prosecute the case in the event that charges are filed.

[21] If circumstances permit, it is best practice to have the DLO join (telephonically or otherwise) this meeting. The DLO's participation can help ensure provision of the most complete and detailed information possible regarding sample status, testing options, and possible alternatives to FGGS. This information can, in turn, help optimize subsequent investigative decisions.

candidate forensic sample is suitable for FGG, and that FGGS is a necessary and appropriate step at that stage of the investigation to develop investigative leads or to identify the unidentified human remains. If agreement is reached on these points, FGGS may proceed.

VII. Investigative Caution

Investigative agencies shall identify themselves as law enforcement to GG services and enter and search FGG profiles only in those GG services that provide explicit notice to their service users and the public that law enforcement may use their service sites[22] to investigate crimes or to identify unidentified human remains. The investigative agency shall, if possible, configure service site user settings that control access to FGG profile data and associated account information in a manner that will prevent it from being viewed by other service users.

In certain cases, the genetic association of an FGG profile with a GG service user, in conjunction with subsequent genealogy research, may identify one or more third parties[23] who may have a closer kinship relationship to the donor of the forensic sample than the associated GG service user. In such cases, the acquisition of reference samples from these third parties for the purpose of conducting FGGS may help the investigative agency identify the donor of the forensic sample.

An investigative agency must seek informed consent from third parties before collecting reference samples that will be used for FGGS, unless it concludes that case-specific circumstances provide reasonable grounds to believe that this request would compromise the integrity of the investigation. If that determination is made, the investigative agency shall consult with, and receive approval from, the prosecutor[24] before covertly collecting any reference samples that will be used for FGGS. The investigative agency shall also consult with the DLO, who may provide guidance to investigators about the type and nature of biological samples that may prove most conducive to FGG analysis. Covert collection shall be conducted in a lawful manner. In addition, a search warrant shall be obtained by the investigative agency before a vendor laboratory conducts FGG analysis on any covertly-collected reference sample.

Investigative agencies shall use biological samples and FGG profiles only for law enforcement identification purposes and shall take all reasonable and necessary steps and precautions to ensure that same limited use by others who have authorized access to those samples and profiles. Biological samples and FGG profiles shall not be used by investigative

---

[22] The term 'service site' means the online web page and content of a GG service.

[23] As used in this interim policy, the term 'third party' means a person who is not a suspect in the investigation.

[24] Before authorization is granted, the prosecutor should notify and consult with the prosecutor in the jurisdiction where the sample will be covertly collected (if different) to ensure that all applicable legal authorities and local procedures relevant to sample acquisition are followed. When the Department of Justice and one or more state or local prosecuting authorities have concurrent jurisdiction of the crime(s) under investigation, the 'prosecutor' means the Assistant Attorney General, United States Attorney, or the state or local prosecuting official whose office will prosecute the case in the event that charges are filed.

agencies, vendor laboratories, GG services, or others to determine the sample donor's genetic predisposition for disease or any other medical condition or psychological trait.

FGGS is a law enforcement technique used to generate investigative leads. Investigative agencies shall not arrest a suspect based solely on a genetic association generated by a GG service. Traditional genealogy research and other investigative work is required to determine the true nature of any genetic association.

VIII. Sample and Data Control and Disposition

All FGG profiles and GG service account information and data shall be treated as confidential government information consistent with any applicable laws, regulations, policies, and procedures. These materials are subject to transfer and disclosure by Department employees and contractors only during the discharge of their official duties and only for authorized purposes.

If a suspect is arrested and charged with a criminal offense while FGG is in progress, the investigative agency shall promptly contact the relevant vendor laboratory or DTC service and direct that all testing cease at a point in time when the (forensic or reference) sample can be preserved. The investigative agency shall also request that the sample, extract,[25] and amplicon[26] be returned directly to the submitting law enforcement agency or custodial CODIS laboratory, as applicable. The investigative agency shall document its request and compliance by the vendor laboratory or DTC service.

If a suspect is arrested and charged with a criminal offense after an FGG profile has been entered into one or more DTC services, the investigative agency shall make a prompt formal request that all FGG profiles and associated account information and data held by any such service be removed from its records and provided directly to the investigative agency.[27] The investigative agency shall document its request and compliance by the DTC service(s). All FGG profiles, account information, and data shall be retained by the investigative agency for potential use during prosecution and subsequent judicial proceedings.

If a suspect is arrested and charged with a criminal offense after an FGG profile has been entered into an open-data personal genomics DNA database, the investigative agency shall promptly remove the FGG profile and all associated account information and data from the database.[28] The investigative agency shall document the removal of this information and data. It

[25] 'Extract' is the total amount of cellular DNA isolated from a biological sample.
[26] 'Amplicon' is the total amount of the targeted DNA segment or sequence generated by the PCR amplification process.
[27] These requests should be made only after the suspect's known STR DNA profile has been manually compared to the forensic profile previously uploaded to CODIS and it has been determined that the profiles match.
[28] The profile, information, and data should be removed only after the suspect's STR DNA profile has been manually compared to the forensic profile previously uploaded to CODIS and it has been determined that the profiles match.

shall be retained by the investigative agency for potential use during prosecution and subsequent judicial proceedings.

Subject to applicable law, in all cases that result in a criminal prosecution, reference samples obtained from third parties for FGGS (including all extracts and amplicon), all derivative FGG profiles, and all GG service account information and data shall be destroyed by the investigative agency only after the entry of an appropriate judicial order. The investigative agency shall document the authorized destruction of these samples, profiles, information, and data.

Subject to applicable government information retention schedules, if FGGS does not result in an arrest and the filing of criminal charges, the investigative agency shall promptly destroy all third-party reference samples (including all extracts and amplicon), all derivative FGG profiles, and all GG service account information and data after their investigative use is complete. The investigative agency shall document the destruction of these samples, profiles, information, and data.

IX. Collection of FGGS Metrics

Each Department component that either uses or funds another agency to use FGG/FGGS for criminal investigative purposes, or that provides any unit of federal, state, local, or tribal government with grant award funding that is used by a grantee to conduct FGG/FGGS for criminal investigative purposes, shall collect and retain the following information on an annual basis: 1) the type of crime investigated; 2) whether FGG/FGGS was conducted on a forensic sample or a reference sample; 3) the type of forensic sample subjected to FGG, and a description of the total amount, condition, and concentration of that sample (e.g., single source, mixed profile, degradation status, etc.); 4) whether FGG analysis resulted in a searchable profile; 5) the identity of the vendor laboratory used to conduct FGG and the GG service(s) used to search the FGG profile; 6) whether the investigation resulted in an arrest that was based, in part, on the use of FGGS; and 7) the total amount of federal funding used to conduct FGG/FGGS in each case.