Filed
Washington State
Court of Appeals
Division Two

August 22, 2023

IN THE COURT OF APPEALS OF THE STATE OF WASHINGTON

DIVISION II

STATE OF WASHINGTON, Respondent, v. GARY CHARLES HARTMAN, Appellant.	No. 56801-2-II PUBLISHED OPINION

GLASGOW, C.J. — In 1986, MW, a 12-year-old girl, was raped and murdered in a Tacoma park. The killer left semen on MW's body, but his DNA did not match that of any suspects or anyone in police databases for the next 30 years.

In 2018, police enlisted Parabon Nanolabs, a DNA technology company, to analyze the killer's DNA and to upload it into GEDmatch, a consumer DNA database, looking for partial familial matches that would help identify the killer. Police did not secure a warrant to analyze the abandoned DNA or to compare it with DNA in the GEDmatch database.

Parabon learned that several of the killer's cousins had DNA in the GEDmatch database. Parabon used information from the database and public records to construct family trees. Parabon then directed police to try to obtain a DNA sample from Gary Charles Hartman. Police obtained a discarded napkin containing Hartman's DNA, and it matched the DNA from semen on MW's body. The State charged Hartman with first degree felony murder.

Before trial, Hartman moved to suppress the DNA evidence, arguing that Parabon's comparison of the DNA sample from the crime scene to the GEDmatch database was unconstitutional. He also asserted that the DNA later collected from the napkin directly linking him to the murder was inadmissible as fruit of the poisonous tree. Hartman did not argue below that he had any privacy interest in DNA left at the crime scene, nor did he challenge the collection and testing of DNA from the discarded napkin.

The trial court ruled that Hartman did not have standing to challenge the comparison of the DNA from the crime scene to DNA in the GEDmatch database because he did not have a privacy interest in his cousins' DNA in the database. In addition, Hartman's relatives had voluntarily uploaded their DNA into the GEDmatch database, and the DNA that Hartman left at the crime scene was abandoned and not private. The trial court denied the motion to suppress. After a bench trial on stipulated facts, the trial court convicted Hartman.

Hartman appeals his conviction. He argues that analyzing the DNA sample from the crime scene and comparing it with the GEDmatch database to look for his relatives' DNA disturbed his private affairs in violation of article I, section 7 of the Washington Constitution. Thus, he argues that he had standing to challenge the DNA comparison. In oral argument, he asserted for the first time that he has a privacy interest in the DNA from the semen abandoned at the crime scene.

We affirm. There is no privacy interest in commonly held DNA that a relative voluntarily uploads to a public database that openly allows law enforcement access. And there is no privacy interest in DNA that one abandons at a crime scene. Absent a privacy interest, Hartman did not have standing to challenge the comparison of the crime scene DNA with the GEDmatch database. But the legislature could adopt statutory restrictions and the companies that run consumer DNA

databases could adopt policies limiting law enforcement access to genetic information in those databases without a warrant. Indeed, GEDmatch did just that in 2019 after the investigation at issue in this case.

FACTS

I. BACKGROUND

A. Initial Investigation

In 1986, 12-year-old MW was playing with her sisters in a Tacoma park. MW left to get lunch and never returned to her sisters. That night, her body was found in a wooded gulch in the park. Someone had raped her and then killed her by slitting her throat and striking her in the head with a blunt object that caved in her skull.

The killer left semen and hair on MW's body. Over the next 30 years, DNA, blood type, and hair comparisons eliminated more than 100 possible suspects. The killer's DNA did not match anyone in the Combined DNA Index System (CODIS), the state and national police DNA databases.

In the mid-2010s, police began considering identifying MW's killer through a familial DNA analysis, which would involve looking for DNA profiles that were not exact matches but had enough DNA in common to be a relative of the killer. CP at 240. Congress has not expressly authorized checking for familial matches in CODIS at the national level, although a few states allow such analyses in their state police DNA databases. Shanni Davidowitz, *23andEveryone: Privacy Concerns with Law Enforcement's Use of Genealogy Databases to Implicate Relatives in*

Criminal Investigations, 85 BROOK. L. REV. 185, 199 (2019).[1] Currently, Washington State does not expressly allow analysis of a suspect DNA sample to check for familial matches in the police DNA databases. *See How We Can Help You: Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/how-we-can-help-you/dna-fingerprint-act-of-2005-expungement-policy/codis-and-ndis-fact-sheet [https://perma.cc/M3XT-HW2T].

B. Parabon and GEDmatch Investigation

In 2017, police sent the DNA of MW's killer to a genealogy consultant, Barbara Rae-Venter. Rae-Venter uploaded the killer's DNA profile into several nongovernment consumer DNA databases and began trying to identify family connections that could provide leads. Police also sent the DNA profile to a genetic genealogist at another company, Parabon, who compared the killer's DNA sample to the GEDmatch database. Through the consumer databases, Rae-Venter and Parabon both identified two of the killer's second cousins, one of whom lived in Washington.

GEDmatch's database contained a larger pool of people than most. While some consumer DNA databases like 23andMe and Ancestry "could only connect people through the samples in their own respective databases, GEDmatch allowed all [direct-to-consumer testing] customers to upload their test results *regardless of the testing company* and for free." Victoria Romine, *Crime, DNA, and Family: Protecting Genetic Privacy in the World of 23andMe*, 53 ARIZ. ST. L.J. 367, 372 (2021). In this way, GEDmatch "served as a gap filler, allowing people to connect with relatives who happened to use a different testing company." *Id*. And while police databases

[1] *See also Law Enforcement Resources: Combined DNA Index System (CODIS)*, FED. BUREAU INVESTIGATION ("Familial searching is not currently conducted at the national level."), https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis [https://perma.cc/PG5L-KYL7].

contained only about 20 identifying markers from a person's DNA, the analysis GEDmatch performed was extensive. It could "reveal information about a person's sex, physical appearance, medical conditions, genetic history, and ancestral origin." *Id.* at 379. Other consumer databases used in this case, FamilyTree DNA and MyHeritage, worked in a similar way. *Id.* at 372.

GEDmatch could "consistently match relatives as distant as third cousins." Michael I. Selvin, *A Too Permeating Police Surveillance: Consumer Genetic Genealogy and the Fourth Amendment After Carpenter*, 53 LOY. L.A. L. REV. 1015, 1020 (2020). A database like GEDmatch needs to contain samples from approximately 2 percent of a population to provide a third-cousin match for almost every member of the population. Teneille R. Brown, *Why We Fear Genetic Informants: Using Genetic Genealogy to Catch Serial Killers*, 21 COLUM. SCI. & TECH. L. REV. 118, 137 (2019). In 2018, it was estimated that "60 percent of searches for individuals of European descent" in a database like GEDmatch would have produced a match to a third cousin. Hillary L. Kody, *Standing to Challenge Familial Searches of Commercial DNA Databases*, 61 WM. & MARY L. REV. 287, 294 (2019).

At the time of Parabon's analysis in 2017, GEDmatch allowed law enforcement to access its service in some circumstances. Specifically, GEDmatch's terms of service stated "that it accepted 'DNA obtained and authorized by law enforcement to either: (1) identify a perpetrator of a violent crime against another individual; or (2) identify remains of a deceased individual.' GEDmatch defined 'violent crime' as 'homicide or sexual assault.'" Selvin, *supra*, at 1023 (quoting *GEDMatch.Com Terms of Service and Privacy Policy*, GEDMATCH (footnote omitted), https://web.archive.org/web/20190506040926/https://www.gedmatch.com/tos.htm (version prior to May 18, 2019 update)).

The Parabon genealogist used information from GEDmatch and other publicly available sources to build family trees for the two second cousins found in the database. She found additional partial matches with two third cousins and one fourth cousin. The genealogist also relied on "census records, vital records, extensive newspaper archive searches, public 'people search' databases, and public social media data" to build the family trees. Clerk's Papers (CP) at 102. She did not contact any of the killer's cousins, although she did contact one of their daughters seeking information about the cousins' family tree. Through her research, the genealogist learned that the family tree contained at least one instance of misattributed paternity, meaning someone's biological father was not who they believed their biological father to be.

Rae-Venter had a different company analyze the DNA from the crime scene, and she learned from that analysis that the killer had alleles related to substance abuse, bipolar disorder, and baldness. And Parabon analyzed the killer's DNA sample to learn that the killer was roughly 9 percent Native American.

In 2018, based on her research, the Parabon genealogist suggested collecting DNA samples from Hartman and his brother, who both lived in Tacoma in 1986. Police surveilled both brothers to collect discarded items including used drinking straws and napkins. Hartman's brother's DNA excluded the brother as a possible source, while Hartman's DNA profile matched the DNA from the semen found on MW's body.

Police arrested Hartman, and they collected another sample of his DNA pursuant to a warrant. That sample of Hartman's DNA matched the DNA from the semen found on MW's body with a probability of error of 1 in 6 quadrillion. The State charged Hartman with first degree felony murder, with the rape of MW as the underlying felony.

Later, in 2019, after backlash to a forensic genealogy investigation in Utah, GEDmatch altered its privacy settings so that users had to opt into allowing law enforcement to access their DNA for forensic genealogy comparisons. Selvin, *supra*, at 1024. One year later, "only 185,000 of GEDmatch's 1.3 million users [had] chosen to opt-in." *Id.* As of mid-2022, Washington law enforcement had used forensic genealogy in only about two dozen cases, with the technology "reserved for unsolved cold cases of felony crimes with a sexual motivation" that had "no active leads and no CODIS matches." News Release, Wash. Att'y Gen., Multiple Cold Cases Solved with Assist from Attorney General's DNA Forensic Genetic Genealogy Program (July 11, 2022), https://www.atg.wa.gov/news/news-releases/multiple-cold-cases-solved-assist-attorney-general-s-dna-forensic-genetic [https://perma.cc/SPG2-FNZ8].

II. MOTION TO SUPPRESS AND DISMISS

Before trial, Hartman moved to suppress Parabon's analysis and DNA evidence later collected or analyzed as a result of the Parabon analysis, including the analysis of DNA from the napkin. He also moved to dismiss the case. Hartman concentrated on the information learned from GEDmatch in his motion to suppress. Below, he acknowledged that he had no privacy interest in the semen left at the crime scene, stating, "[W]e're not arguing that [there was a privacy interest in] anything left at the scene." 1 Verbatim Rep. of Proc. (Feb. 15, 2022) at 8. Hartman also stated, "I'm not arguing about the crime scene DNA search." *Id.*at 30. He did not challenge the direct analysis of the DNA from the semen left at the crime scene at all besides noting that the State *could* have learned private information such as predispositions for genetic diseases from that DNA. Instead, he emphasized that Parabon's comparison of that DNA against the GEDmatch database

"revealed [his] ethnic background" and uncovered misattributed paternity within his family tree. CP at 49.

Hartman argued that analyzing the consumer databases for "the DNA he shared with his close relatives" was a warrantless, suspicionless search by a state actor that disturbed his private affairs in violation of the state and federal constitutions. CP at 32. Thus, he reasoned that the trial court should suppress "all evidence obtained" because of Parabon's analysis, including the tests that directly matched his DNA to the killer's, as fruit of the poisonous tree. CP at 64. With no other evidence linking him to MW's murder, Hartman argued that the trial court should dismiss the charge if it suppressed the Parabon analysis and DNA evidence from the napkin.

A. Standing Arguments

Hartman asserted that he had standing to challenge the comparison of the DNA sample from the crime scene against the consumer DNA databases because Parabon was a state actor and the analysis revealed "medical and familial information" in which he had a reasonable expectation of privacy. CP at 45. He also argued that, "Americans are overwhelmingly opposed to sharing their private genetic information with law enforcement," pointing to the large proportion of GEDmatch users who refused to share their information with law enforcement when the site changed its policy in 2019. CP at 50-51. He thus asserted that he had standing to challenge the analysis of the DNA he held in common with his relatives because he "was subjected to a sweeping, warrantless search . . . that provided an 'intimate window' into his familial and sexual associations." CP at 49.

The State argued that Hartman lacked standing to challenge the investigation of the consumer databases because Hartman's argument was about his relatives' genetic information, not his own. In addition, "his relatives affirmatively volunteered" to upload their genetic information

to the databases, which anyone could access. CP at 119 (boldface omitted). The State explained that by "voluntarily providing their DNA to commercial DNA databases," Hartman's relatives "consented to the privacy policies as set by the companies" at the time. CP at 121. The State pointed out that at the time of Parabon's investigation in 2017 and 2018, GEDmatch allowed law enforcement to use its service without restriction.

B. Trial Court Ruling

The trial court noted that the standing question was an issue of first impression, so there was no controlling precedent to follow and no Washington statute restricted familial DNA comparisons in databases like GEDmatch. The trial court found that police used semen found on MW's body to construct a male DNA profile that did not match anyone in state or national police databases. It found that direct DNA comparisons eliminated 108 suspects before police resorted to the familial analysis. And the trial court concluded that Hartman had no standing to challenge the collection of DNA from the semen at the crime scene because he had abandoned that semen.

The trial court also concluded that Parabon and Rae-Venter were state actors. Thus, they were subject "to search and seizure restrictions and the restrictions on invasion of an individual's justifiable, reasonable, and legitimate expectations of privacy." CP at 251(Conclusion of Law (CL) 16). And "Hartman never supplied a DNA sample voluntarily to any source." CP at 247 (Finding of Fact (FF) 48).

The trial court found that Parabon compared the DNA sample to only public consumer databases, not police DNA databases. It also found that "[n]o medical information related to defendant Hartman was addressed in the Parabon analysis and report." CP at 242 (FF 25). And neither Parabon nor Rae-Venter "accessed the raw data DNA from 23andMe or Ancestry, which

are two databases . . . [that] have scope of use restrictions" for law enforcement. *Id*. (FF 26). "They did, however, access an open public website[,] GEDmatch, which had no access restrictions at the time of this search." *Id*.

The trial court ruled that Hartman had standing to challenge state actions "following the initiation of direct police surveillance." CP at 247 (CL 4). But he did not have standing to challenge the analysis of "his relative's DNA profile, which his relatives volunteered to have analyzed and posted on an open-source, unrestricted website." CP at 250 (CL 13). The court concluded that Hartman did not have "dominion or control over the item seized (his relative's raw data DNA) nor the public database where the DNA profiles were compared (GEDmatch)." CP at 252 (CL 18). Hartman had no authority to exclude others from accessing his relatives' DNA profiles on GEDmatch. Thus, state actors did not disturb Hartman's private affairs. And, like the DNA from the semen abandoned at the crime scene, Hartman could not challenge the analysis of the DNA from his discarded napkins because he had voluntarily abandoned the napkins.

The trial court concluded that Hartman failed to show that the State intruded on his private affairs because "[a]ny individual or entity could have directly accessed this voluntarily published and public information." CP at 247 (CL 2). Thus, Hartman had no standing to challenge the comparison with his relatives' DNA profiles in the GEDmatch database. As a result, the trial court ruled that the State "did not need a search warrant or a court order to access GEDmatch due to the public and unrestricted availability of the GEDmatch data." CP at 251 (CL 15).

Because Hartman lacked standing to suppress the evidence, the trial court concluded that the DNA evidence tying him to the rape and murder of MW was admissible. The trial court denied the motion to suppress and dismiss.

III. TRIAL AND SENTENCING

The case proceeded to a bench trial on stipulated facts. Hartman stipulated that the DNA collected from his used napkin matched DNA from the semen collected from MW's body. He also stipulated that his reference DNA sample collected pursuant to a warrant matched the semen from the crime scene. He agreed that "the estimated probability of selecting an unrelated individual at random from the U.S. population with a matching profile was calculated at 1 in 6.0 quadrillion." CP at 279.

The trial court convicted Hartman of first degree felony murder. It imposed a 320-month sentence at the top of the standard range. Hartman appeals his conviction and the order denying the motion to suppress and dismiss.

ANALYSIS

The Washington Constitution provides that "[n]o person shall be disturbed in his private affairs . . . without authority of law." CONST. art. I, § 7; *State v. Chacon Arreola*, 176 Wn.2d 284, 291, 291 P.3d 983 (2012). "It is well established that article I, section 7 is qualitatively different from the Fourth Amendment and provides greater protections." *State v. Hinton*, 179 Wn.2d 862, 868, 319 P.3d 9 (2014). Although Hartman also challenged the comparison of DNA in GEDmatch's database as a violation of the Fourth Amendment to the United States Constitution below, he asserts only a violation of article I, section 7 on appeal.

Hartman argues that he had "a personal privacy interest" in the DNA he had in common with his family members and the information gleaned from the analysis of the consumer databases, rendering the analysis unconstitutional under article I, section 7. Br. of Appellant at 31. As a result, he asserts that he has standing to challenge Parabon's investigation involving the consumer DNA

databases because his private affairs were disturbed. Thus, he contends that the trial court abused its discretion by ruling that the DNA evidence secured as fruit of that investigation was admissible. Hartman also asserted in oral argument that before he was identified as MW's killer, he had a privacy interest protecting against analysis of the DNA that he abandoned at the crime scene because that analysis revealed information about the then-unidentified killer's race, a likelihood that the killer was bald, and a likelihood that he suffered from bipolar or substance abuse disorder. We disagree.

I. SCOPE OF ISSUES ON APPEAL

The issues before us are limited in scope. First, Hartman does not challenge any of the trial court's findings of fact, so they are verities on appeal, as are the stipulated facts from the bench trial. *State v. Bliss*, 153 Wn. App. 197, 203, 222 P.3d 107 (2009). Second, it is undisputed that Parabon and Rae-Venter were state actors and that there was no warrant for the analysis of the DNA found at the crime scene or its comparison with profiles in GEDmatch's database. Third, Hartman does not claim a privacy interest in any of the public records that Parabon used to build his family tree after identifying his cousins. Instead, he claims to have a reasonable expectation of privacy in the segments of his DNA that he had in common with relatives that those relatives voluntarily uploaded to GEDmatch.

Further, the State asserts that Hartman did not challenge the later warrant for a reference DNA sample that linked him to MW's murder, and that his challenge to the investigation that yielded the reference DNA is therefore waived. But without the GEDmatch analysis, there would not have been a later warrant for Hartman's DNA—just as there was not for the preceding three decades. It is undisputed that Hartman "never supplied a DNA sample voluntarily to any source."

CP at 247 (FF 48). Thus, if the trial court had concluded that the GEDmatch investigation was unconstitutional, it would have inevitably suppressed the other DNA evidence as the fruit of the poisonous tree. *State v. Maxwell*, 114 Wn.2d 761, 769, 791 P.2d 223 (1990) (holding that a court must suppress evidence obtained from a warrant if the warrant was based on illegally obtained information and the supporting affidavit does not contain "otherwise sufficient facts to establish probable cause independent of the illegally obtained information"). In sum, if Hartman is successful in his challenge to the GEDmatch comparison, the later DNA comparisons of Hartman's DNA to the crime scene DNA would also be excluded because they would not have occurred absent the alleged article I, section 7 violation. *Id*.

Finally, at oral argument, Harman focused on issues not raised below, not addressed in his opening brief to this court, and developed for the first time at oral argument. Hartman asserted for the first time that he has a privacy interest in the DNA from the semen abandoned at the crime scene. Specifically, Hartman now argues that the DNA extracted from semen abandoned at the crime scene is information that Hartman retained a privacy interest in, even though he abandoned the semen by leaving it on his victim. The State responded at oral argument that this court should decline to address this issue because it was not raised below, nor was it discussed in any detail in Hartman's briefing to this court. The State also fully responded to the merits of this new contention in oral argument. Thus, in the interest of preserving resources, we exercise our discretion under RAP 2.5(a) to resolve these contentions, as well as the arguments presented in Hartman's brief.

II. STANDING FOR HARTMAN'S ARTICLE I, SECTION 7 CHALLENGE

The central question raised in Hartman's brief—whether Hartman had a privacy interest in the segments of his DNA that he has in common with his relatives, giving him standing to challenge the analysis of the GEDmatch database—is an issue of first impression in Washington. To raise an article I, section 7 challenge, a defendant must have standing. Proving standing to challenge a search or seizure requires a defendant to show that a private affair is implicated under article I, section 7, meaning that they "possess a legitimate expectation of privacy in the place searched or the thing seized." *State v. Carter*, 127 Wn.2d 836, 841, 904 P.2d 290 (1995). Standing is a two-part inquiry into whether "the claimant manifest[ed] a subjective expectation of privacy in the object of the challenged search" and whether "society recognize[s] the expectation as reasonable." *State v. Link*, 136 Wn. App. 685, 692, 150 P.3d 610 (2007). In particular, a defendant has to show that the challenged action violated the defendant's own rights, rather than the rights of a third party. *Id*.; *Hinton*, 179 Wn.2d at 869 n.2 ("Generally, article I, section 7 rights may be enforced by exclusion of evidence only at the instance of one whose own privacy rights were infringed by government action.").

"A claimant who has a legitimate expectation of privacy in the invaded place has standing to claim a privacy violation." *Link*, 136 Wn. App. at 692. Thus, if the analysis of the GEDmatch database disturbed Hartman's privacy interest in the segments of his DNA that his relatives had in common with him, then Hartman had standing to challenge this aspect of the investigation because he had a subjective expectation of privacy that society recognizes as reasonable.

A. Whether Common DNA Between Relatives That Has Been Posted on the Internet is a Private Affair

To have standing to challenge the analysis of the GEDmatch database, Hartman must show that the genetic material he had in common with his relatives that they posted on the database was a private affair under article I, section 7. *Carter*, 127 Wn.2d at 841. Courts consider several factors when determining whether something is a private affair. We consider both "the nature and extent of the information that may be obtained as a result" of a governmental investigation and "what kind of protection has been historically afforded to the interest asserted." *State v. Reeder*, 184 Wn.2d 805, 814, 365 P.3d 1243 (2015).

1. Nature of information sought and voluntary exposure

Hartman argues that the nature of the information Parabon learned from GEDmatch "was intensely private." Br. of Appellant at 35. He compares DNA to motel registries and cell site location information that police cannot access without a warrant, even though that information is shared with certain third parties. We disagree.

a. Cases addressing the nature of the information and voluntary exposure

When considering the nature of the information sought, we determine whether the information "reveals intimate or discrete details of a person's life." *State v. Jorden*, 160 Wn.2d 121, 126, 156 P.3d 893 (2007). Courts have considered "the purpose for which the information sought is kept, and by whom it is kept." *Id.* at 127; *see Reeder*, 184 Wn.2d at 815 (privacy interest in banking records); *In re Pers. Restraint of Maxfield*, 133 Wn.2d 332, 338-39, 945 P.2d 196 (1997) (privacy interest in electricity consumption records kept by a municipal corporation); *State v. Hathaway*, 161 Wn. App. 634, 643, 251 P.3d 253 (2011) (no privacy interest in Department of Licensing records kept to aid law enforcement).

"Voluntary exposure to the public is relevant to our inquiry and can negate an asserted privacy interest." *State v. Athan*, 160 Wn.2d 354, 366, 158 P.3d 27 (2007); *see Carpenter v. United States* ___ U.S. ___, 138 S. Ct. 2206, 2220, 201 L. Ed. 2d 507 (2018). But some information voluntarily revealed to certain other people or entities is still protected under article I, section 7 and the Fourth Amendment.

For example, in *Jorden*, police conducted a random, suspicionless check of a guest registry at a motel and learned that Jorden had an outstanding felony warrant after running the resulting list of names through a police computer. 160 Wn.2d at 124. The Washington Supreme Court concluded that the suspicionless check violated article I, section 7 even though guests voluntarily revealed their identities to hotel staff. The Supreme Court emphasized that "an individual's very presence in a motel or hotel may in itself be a sensitive piece of information" subject to protection from warrantless searches. *Id*. at 129. The list of law-abiding people who "may not wish to reveal [their] presence at a motel" included "business people engaged in confidential negotiations," domestic violence victims hiding from their abusers, and closeted same-sex couples or "couples engaging in extramarital affairs." *Id*. Further, the registry information "may also reveal co-guests in the room, divulging yet another person's personal or business associates." *Id*. Because of the depth of information provided, the Supreme Court held that searches of a guest registry revealed "'intimate details about a person's activities and associations'" constituting a private affair. *Id*. (quoting *State v. McKinney*, 148 Wn.2d 20, 30 n.2, 60 P.3d 46 (2002)). Government trespass on that information was therefore a search that required a warrant. *Id*. at 130.

Similarly, in *Carpenter*, the United States Supreme Court held that the Fourth Amendment required police to secure a warrant to access the location information automatically generated by

cell phones even though location information is exposed to a cell subscriber's wireless carrier. 138 S. Ct. at 2221. The *Carpenter* court held that cell phone location records have a "unique nature" because cell phones are a ubiquitous feature of modern life that constantly report their location and tend to be within a few feet of their owners at all times. *Id*. at 2217. Carpenter had a "reasonable expectation of privacy in the whole of his physical movements" which his phone logged "without any affirmative act on the part of the user beyond powering up." *Id*. at 2219-20. "Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data," so Carpenter had not voluntarily assumed the risk "of turning over a comprehensive dossier of his physical movements." *Id*. at 2220.

In short, even though Carpenter voluntarily exposed his location information to his wireless carrier, the extent and intimate nature of that information meant that he maintained a reasonable expectation of privacy in the information under the Fourth Amendment. Thus, police had to secure a warrant to access the cell site location information. *Id*. at 2221; *see also State v. Phillip*, 9 Wn. App. 2d 464, 479, 452 P.3d 553 (2019) (holding that there is a reasonable expectation of privacy in cell site location information under article I, section 7).

Washington courts have also recognized the private nature of other information available to certain third parties, such as text messages that are available to both the person receiving the message and the cell carrier. *Hinton*, 179 Wn.2d at 871. In *Hinton*, police arrested a man and seized his phone, then used the phone to set up a drug deal with Hinton by text. *Id*. at 865-66. "Despite the fact that a cell phone is carried on a person in public, text messages often contain sensitive personal information about an individual's associations, activities, and movements." *Id*. at 871. And "individuals closely associate with and identify themselves by their cell phone numbers," to

the point where users expect only a specific individual to possess a given phone. *Id*. Thus, sending a text message does not "extinguish a sender's privacy interest in its contents" even though the messages "remain susceptible to exposure because of a cell phone's mobility." *Id*. at 873. The Washington Supreme Court concluded that "incidental exposure of private information in the course of everyday life is distinct from other kinds of voluntary disclosure that extinguish privacy interests under article I, section 7." *Id*. at 875. "Forcing citizens to assume the risk that the government will confiscate and browse their associates' cell phones tips the balance too far in favor of law enforcement at the expense of the right to privacy." *Id*. at 877. As a result, the State disturbed Hinton's privacy interest when it searched the other person's cell phone. *Id*.

In contrast, the Washington Supreme Court has thus far declined to shield identifying information in discarded DNA. In *Athan*, detectives who suspected Athan of murder posed as a fictitious law firm inviting Athan to join a fictional class action lawsuit. 160 Wn.2d at 363. When Athan filled out and mailed back the class action authorization form, police obtained his DNA from saliva Athan used to seal the mailing envelope. *Id*. They then obtained a DNA profile that could be compared with DNA collected at a crime scene. *Id*.

Athan and amicus argued that Athan had a privacy interest in his DNA because "DNA has the potential to reveal a vast amount of personal information, including medical conditions and familial relations." *Id*. at 367-68. The Supreme Court disagreed because "the State's use of Athan's DNA here was narrowly limited to identification purposes." *Id*. at 368. "What was done with the letter, including DNA testing for the limited purpose of identification, was not within the sender's control." *Id*. Thus, by voluntarily licking the envelope and placing it in the mail, Athan lost "any privacy interest" in his saliva or the DNA it contained. *Id*. at 367.

b. The nature of the information in this case

DNA inherently contains intimate and discrete details of a person's life, including information related to intimate family connections and the likelihood of experiencing medical conditions. *See id.* at 367-68. Because GEDmatch analyzes many more alleles than government databases, its database can be used to identify relationships between third cousins—people whose last common ancestors were their great-great grandparents. Selvin, *supra*, at 1020. Some legal commentators assert that people should have a reasonable expectation of privacy in their own DNA in consumer databases, based on the scope of health information contained therein and the fact that we constantly leave behind DNA everywhere we go. Kody, *supra*, at 306-11; Natalie Ram, *Genetic Privacy After Carpenter*, 105 Va. L. Rev. 1357, 1387-91 (2019).

Here, Parabon and Rae-Venter uncovered intimate personal information about Hartman and his family during their analyses of the GEDmatch database. These facts included his racial background and ancestry information that revealed a misattributed paternity. Hartman seems to argue that this information makes DNA analogous to cell site location information, even though the GEDmatch database is made up of DNA profiles that contributors have voluntarily shared with the public by uploading it onto an Internet site that is publicly available. Hartman asserts that a warrant is required to analyze those public profiles by comparing them with DNA left behind by an unidentified killer. But consumers frequently upload their DNA to consumer databases like GEDmatch for the very purpose of learning and *sharing with strangers* the exact private information—details about their ancestry and familial relations—at issue here.

Cell site location information is distinguishable from DNA. Both are deeply revealing and can be used to determine whether a person was at a particular crime scene. But identifying whether

the DNA sample from *this* crime scene had DNA in common with the genetic profiles Hartman's relatives loaded onto GEDmatch was a limited inquiry targeted only at identifying MW's killer. And although examination of the GEDmatch profiles revealed family information regarding a misattributed paternity, those family members voluntarily uploaded their DNA profiles and the comparison occurred at times when GEDmatch allowed sharing of information with law enforcement. Selvin, *supra*, at 1023. What was done with the relatives' DNA profiles—limited DNA comparison for the purposes of identification—was beyond the relatives' control once they uploaded the information to the public database under GEDmatch's policy at the time. *See Athan*, 160 Wn.2d at 368. And no relative of Hartman has challenged the analysis of their DNA.

Hartman claims a privacy interest in the segments of his DNA that his relatives had in common with him. But all that police learned from the GEDmatch analysis was the killer's familial relations, which brought them closer to learning the killer's identity. *See id*. And identifying unknown family members is the exact reason that users of consumer databases, like Hartman's relatives, post their genetic material on those databases.

The limited nature of the identification information learned from the GEDmatch analysis does not support concluding that Hartman had a privacy interest in the genetic information his relatives had in common with him. We next turn to the historical treatment of this information. *Reeder*, 184 Wn.2d at 814.

2. Historical treatment

Hartman asserts that Washington courts "have historically held DNA profile information safe from suspicionless government trespass." Br. of Appellant at 34. He argues that comparing the DNA from the crime scene to the consumer databases "opened every citizen, [including] those

who have submitted DNA to find family members and those who wish to remain unknown," to an unwarranted search. Br. of Appellant at 35. He contends that "even when information is held by a third party, law enforcement must have credible information providing them with individualized suspicion of a specific and previously identified defendant" to investigate a public database without a warrant. Br. of Appellant at 35. We disagree.

When assessing the historical treatment of the interest being asserted, we look to analogous case law, statutes, "and laws supporting the interest asserted." *Athan*, 160 Wn.2d at 366.

a. Cases and statutes regulating police Internet investigations and DNA

To begin, the Washington Supreme Court "has consistently expressed displeasure with random and suspicionless searches, reasoning that they amount to nothing more than an impermissible fishing expedition." *Jorden*, 160 Wn.2d at 127. For example, random urinalysis screens of probationers are permissible to monitor compliance with probation conditions, but cannot be used as "'a fishing expedition to discover evidence of other crimes, past or present.'" *State v. Olsen*, 189 Wn.2d 118, 134, 399 P.3d 1141 (2017) (quoting *State v. Combs*, 102 Wn. App. 949, 953, 10 P.3d 1101 (2000) (reaching the same conclusion about polygraph tests)); *see also State v. Cornwell*, 190 Wn.2d 296, 307, 412 P.3d 1265 (2018) (holding that a community custody officer's open-ended search of a defendant's vehicle was an impermissible fishing expedition). However, "particularized and individualized suspicion about the suspect that *preceded*" the intrusion can support a government trespass. *Jorden*, 160 Wn.2d at 127-28 (listing cases holding that police review of guest registries to confirm prior individualized suspicions is permissible).

Washington limits DNA collection for people not yet convicted of a crime. Police must have probable cause and a warrant to demand a DNA sample from a suspect. *State v. Garcia-*

Salgado, 170 Wn.2d 176, 184, 240 P.3d 153 (2010). However, a person who voluntarily "licks an envelope and places it in the mail" does not retain any privacy interest in the DNA contained in the "voluntarily discarded saliva." *Athan*, 160 Wn.2d at 367, 387.

Washington also imposes certain limits on DNA analysis. Police cannot use the information in the state police DNA database for any "purpose that is not related to a criminal investigation, to the identification of human remains or missing persons, or to improving the operation of the system." RCW 43.43.759. Washington has not addressed whether police can use the state CODIS database to look for familial matches in criminal investigations, and there is no evidence in the record that police databases are being used for familial comparisons in Washington.[2]

Next, information on the Internet is highly susceptible to police investigation. The Washington Supreme Court generally disfavors police review of information compilations, such as motel guest registries, when "there was no particularized and individualized suspicion of [the defendant] preceding review" of the compilation. *Jorden*, 160 Wn.2d at 128. But in *State v. Peppin*, Division Three held that a detective's scan of a "peer to peer network" to find child pornography files was not an intrusion into the defendant's private affairs because he "voluntarily offered" the files for "public access" by posting them on the network. 186 Wn. App. 901, 910-11, 347 P.3d 906 (2015). "[S]haring is inherent in these programs and a user must change the default setting if they desire not to share files." *Id*. at 906. Division Three held that Peppin had no privacy interest in the

[2] The legislature recently considered but failed to adopt a law that required either consent or "valid legal process" before law enforcement could access genetic information held in a consumer genetic database "without a consumer's express consent." H.B. 2485 § 2(1)(c), 66th Leg., Reg. Sess. (Wash. 2020).

files because his "use of peer to peer file sharing voluntarily opened this information to the public for anyone to access, including law enforcement." *Id*. at 910.

Hartman points to recent laws in other jurisdictions that restrict police investigations of consumer DNA databases. Few states have addressed familial DNA analyses, but the ones that have are divided about whether law enforcement may conduct warrantless familial comparisons in consumer DNA databases to identify criminal suspects. In particular, by statute, Maryland and Montana require a warrant to analyze consumer databases for individuals related to a DNA sample. MD. CODE ANN., CRIM. PROC. § 17-102(a)(1); MONT. CODE ANN. § 44-6-104(2). Both statutes went into effect in 2021. And in 2022, California began requiring consumer genetic testing companies to obtain a consumer's "separate and express consent" for, among other things, "[e]ach use of genetic data . . . beyond the primary purpose of the genetic testing or service" and "[e]ach transfer or disclosure of the consumer's genetic data . . . to a third party." CAL. CIV. CODE § 56.181(a)(2)(C)-(D). But ten states, including California, allow familial comparisons in their *police* DNA databases to identify suspects. *See How We Can Help You: Frequently Asked Questions on CODIS and NDIS*, *supra*.

In contrast, the State highlights a New York trial court's conclusion that a defendant lacked standing to challenge a familial DNA comparison. Police did a familial DNA analysis in the state CODIS database to solve a decades-old murder, learning that the killer's brother and nephew were in the database. *People v. Williams*, 77 Misc. 3d 782, 784, 178 N.Y.S.3d 420 (Sup. Ct. 2022). At that time, New York allowed familial DNA comparisons in CODIS. *Id*. at 783. But before Williams's trial, an appellate court overturned the regulation that allowed those analyses. *Id*. at 874; *Stevens v. N.Y. State Div. of Crim. Just. Servs.*, 206 A.D.3d 88, 107, 169 N.Y.S.3d 1 (N.Y.

2022). The trial court denied Williams's motion to suppress the evidence obtained through the familial comparison in the police database under the Fourth Amendment and New York Constitution because Williams did not "establish that *he* was the victim of an unlawful search." *Williams*, 77 Misc. at 785. The relevant provision of the New York Constitution is identical to the Fourth Amendment. N.Y. CONST. art. I, § 12.

b. Historical protection for genetic information in public consumer databases

Overall, there is no direct historical protection against the type of investigation conducted in this case. Generally, law enforcement can access information that is publicly available or voluntarily shared. *Athan*, 160 Wn.2d at 367; *Peppin*, 186 Wn. App. at 910. While it is undisputed that Hartman did not participate in uploading his relatives' DNA to the databases, his relatives nevertheless made the information available to the public on the Internet. They did so at a time that GEDmatch's terms of service expressly stated that it would let law enforcement use its service to identify perpetrators. Although Washington cases express a distaste for fishing expeditions, the DNA profiles uploaded into GEDmatch were expressly available for the public to analyze, unlike the motel registry list in *Jorden,* cell site location information in *Carpenter*, and the text messages in *Hinton*, all of which were revealed to specific businesses or individuals but were not posted on the Internet or made broadly available for public access. The historical treatment of information posted on the Internet does not support concluding that Hartman had a privacy interest in the genetic information his relatives had in common with him that those relatives posted online. And although other states have restricted familial genetic database analyses by statute, these are legislative, not constitutional, protections and they are not yet widespread, nor has a similar protection been adopted in Washington.

3. Whether family members like Hartman have a privacy interest in DNA on GEDmatch and similar websites

Users of consumer DNA databases share their genetic material with those companies mostly for the purpose of finding relatives—the exact thing that happened in this case. We decline to conclude that there is a privacy interest in common DNA that a relative has voluntarily uploaded to a public database.

First, the nature of the information—identifying genetic material held in common between relatives—does not favor finding a privacy interest when the genetic material was posted on a public Internet site that openly cooperated with law enforcement. Unlike staying at a motel or using a cell phone, the sole purpose of using a genealogy database is to let others search for and share intensely private information about the user's personal and family history. In light of the fact that customers share private information with genealogy companies with the express purpose of having the company and others consensually mine that data in order to develop familial connections, there can be no privacy interest in that shared information.

Although we disfavor fishing expeditions, there is no historical protection for voluntarily shared genetic material or for information posted on websites intended for public access. Further, although the technology of forensic genealogy is advancing quickly, this was not a "random and suspicionless" fishing expedition in the sense that the investigation lacked a specific target. *Jorden*, 160 Wn.2d at 127. Direct DNA comparisons eliminated more than 100 possible suspects in MW's murder, and there were no matches in the state or national police DNA databases before Parabon's analysis. Parabon's investigation sought to identify people who were related to the specific suspect who left DNA behind in a 30-year-old murder case that had repeatedly run out of leads. The

information gleaned from the public database (that several people bore certain degrees of familial relation to a suspect DNA profile) then allowed law enforcement to narrow the field of suspects.

We hold that Hartman did not have a valid privacy interest in the segments of his DNA that he had in common with his cousins when his cousins voluntarily posted the genetic information on a public website. Thus, Parabon's investigation of GEDmatch's database did not violate article I, section 7 because it did not disturb Hartman's private affairs. Because there was no intrusion on Hartman's private affairs, he had no standing to challenge the DNA comparison of DNA collected at the crime scene with the GEDmatch database.[3] *Link*, 136 Wn. App. at 692.

B. Abandonment of DNA in the Course of a Crime

At oral argument, Hartman argued that the DNA extracted from semen he left behind on his victim is information that Hartman retained a privacy interest in. He reasons that, although it was permissible for police to look for a direct match to the DNA profile in the police DNA database, any additional analysis, including the discovery that the killer had alleles for baldness and certain mental health disorders, required a warrant. In short, Hartman asks us to abandon the well-established rule that analysis of evidence left behind at a crime scene does not require a

[3] This does not mean that law enforcement will necessarily have unfettered access to commercial DNA databases. The companies running consumer databases have begun restricting police access to users' genetic information without the users' consent or a warrant. *See* Selvin, *supra*, at 1023-24 (GEDmatch users must now opt in before law enforcement may access their genetic material). As discussed above, legislation has emerged in some states, and legal commentators have encouraged state legislatures and Congress to "properly balance state and private interests and delineate acceptable parameters for this method of criminal investigation." *Id*. at 1061-62. *See also* Romine, *supra*, at 394-96 (arguing that state legislatures should create a privacy right in genetic information); Davidowitz, *supra*, at 212-14 (arguing that Congress should regulate when police can conduct forensic genealogy analyses).

warrant where the abandoned evidence contains DNA, even though DNA contains a wealth of personal information. We decline to do so.

Abandonment is an exception to the warrant requirement. *State v. Garner*, ___ Wn. App. 2d ___, 529 P.3d 1053, 1058 (2023). The doctrine provides that "law enforcement officers may retrieve and search voluntarily abandoned property without implicating an individual's rights under the Fourth Amendment or under article I, section 7." *State v. Reynolds*, 144 Wn.2d 282, 287, 27 P.3d 200 (2001).

In general, police may not obtain urine or saliva samples directly from a person through "invasive or involuntary procedure[s]" without the person's consent, except for in certain circumstances authorized by statute. *Athan*, 160 Wn.2d at 367; *see Olsen*, 189 Wn.2d at 124 ("[T]he nonconsensual removal of bodily fluids implicates privacy interests."); *Robinson v. City of Seattle*, 102 Wn. App. 795, 812-13, 10 P.3d 452 (2000) (city's mandatory pre-employment urinalysis testing constituted a search that implicated article I, section 7). But a person who licks an envelope and mails it, "spit[s] on the sidewalk[,] or leav[es] a cigarette butt in an ashtray" loses "any privacy interest" in the bodily fluid left behind. *Athan*, 160 Wn.2d at 367; *see also State v. Bass*, 18 Wn. App. 2d 760, 780 n.5, 491 P.3d 988 (2021) (defendant had no privacy interest in the saliva he left on a discarded cup and soda can), *review denied*, 198 Wn.2d 1034, 501 P.3d 148 (2022).

Hartman argues that DNA contains so much private information, that abandoning DNA does not waive an individual's privacy interest in the DNA for any analysis besides looking for a *direct* match in *police* DNA databases. He relies on *Athan*'s acknowledgement that "DNA has the potential to reveal a vast amount of personal information, including medical conditions and

familial relations." 160 Wn.2d at 367-68. But *Athan* expressly dismissed the assertion that there is an automatic privacy interest in DNA that persists after abandonment of a bodily fluid, when the government's use of the abandoned DNA is "narrowly limited to identification purposes." *Id*. at 368.

Here also, the purpose of the entire investigation was to determine the killer's identity and nothing more. To the extent that Hartman argues *Athan* and other cases limit law enforcement to analyzing abandoned DNA for only identification purposes, all of the steps that police took in this case were for the purposes of identifying MW's killer, including narrowing the suspect pool by learning the killer's identifying characteristics. We thus reject this novel argument as contrary to the controlling caselaw on abandonment of bodily fluids. *Id.* at 367-68. By ejaculating on MW's body, Hartman lost "any privacy interest" in the semen he left behind or the DNA it contained. *Id*. at 367. Hartman's attempt to challenge any DNA analysis of the semen he left behind on MW's body fails.

CONCLUSION

We affirm. Hartman did not have a privacy interest in the DNA that his relatives had in common with him and voluntarily posted in a public database, so he did not have standing to challenge the investigation of that database. And there is no privacy interest in DNA that one abandons at a crime scene.

Glasgow, C.J.

We concur:

Maxa, J.

Cruser, A.C.J.