IN THE COURT OF APPEALS OF THE STATE OF ALASKA

STEVEN HARRIS DOWNS, Appellant, v. STATE OF ALASKA, Appellee.	Court of Appeals No. A-14068

Trial Case No. 4FA-19-00504CR

APPEAL FROM THE SUPERIOR COURT
FOURTH JUDICIAL DISTRICT AT FAIRBANKS
HONORABLE THOMAS I. TEMPLE, JUDGE

OPENING BRIEF OF APPELLANT

ALASKA PUBLIC DEFENDER AGENCY

TERRENCE HAAS (0906030)
PUBLIC DEFENDER

EMILY JURA (0906031)
ASSISTANT PUBLIC DEFENDER
900 West 5th Avenue, Suite 101
Anchorage, Alaska 99501
Telephone: (907) 334-4400

Filed in the Court of Appeals
of the State of Alaska
_____, 2024

MEREDITH MONTGOMERY, CLERK
Appellate Courts

_____
Deputy Clerk

VRA AND APP. R. 513.5 CERTIFICATION

I certify that this document and its attachments do not contain (1) the name of a victim of a sexual offense listed in AS 12.61.140 or (2) a residence or business address or telephone number of a victim of or witness to any offense unless it is an address used to identify the place of the crime or it is an address or telephone number in a transcript of a court proceeding and disclosure of the information was ordered by the court. I further certify, pursuant to App. R. 513, that the font used in this document is Arial 12.5 point.

knowing S.S. or owning a .22 at the time of her murder. [Tr. 4400, 4454] He also said that he had been with Lee the night of S.S.'s murder and stated repeatedly that his DNA would not match the profile found on S.S. [Tr. 4430-32, 4434-35, 4471-72]

The state relied on circumstantial evidence as suggesting that a rape-murder had been committed by Downs, since Downs denied knowing S.S., S.S. had been found partially unclothed and with his semen in her vagina but not her underwear (suggesting a lack of movement after intercourse), and because she had injuries to her stomach and hips consistent with a knife being used to overcome resistance to sexual assault. [Tr. 4932-35] During deliberations, the jury listened to several playbacks and asked questions before ultimately convicting Downs on both counts. [R. 1730-31, 1734-39] Downs appeals.

ARGUMENT

I. Law Enforcement's Warrantless Search of a Genealogical Database, in Combination with Other Databases, Violated the Alaska and Federal Constitutions.

A. Standard of review

Constitutional questions relating to search and seizure issues are reviewed de novo; factual findings are reviewed for clear error.[4]

B. Factual background

1. The identification of Downs

In 2018, Alaska State Trooper Randy McPherron read about a cold case in Washington being solved through use of genetic genealogy and decided to pursue it

[4] *Sanders v. State,* 364 P.3d 412, 419-20 (Alaska 2015).

in S.S.'s case. [Tr. 18, 1357-58] McPherron reached out to Parabon Nanolabs and contracted with them to develop a single nucleotide polymorphism (SNP) (rather than a short tandem repeat (STR)) profile from the suspect DNA and upload it into GEDMatch's database in order to do a familial search. [Tr. 815, 1357-59] While STR profiles look at 'junk' markers that reveal little beyond identity, SNP profiles are used in genealogy because they have more "informational richness."[5]

GEDMatch is a public website where any individual can upload a DNA profile to search for potential relatives. [Tr. 1249] When there is a match, GEDmatch reveals the percentage of DNA that is shared, those segments of DNA that match (including the location of the shared DNA), and either the name or alias of the match along with the match's email. [Tr. 1250] GEDMatch does not test DNA; instead, DNA that has already been developed into a SNP profile data file can be uploaded for comparison purposes. [Tr. 1245] Parabon uses GEDmatch because it believes the terms of GEDmatch's privacy policy authorize Parabon to use GEDmatch for investigative purposes. [Tr. 1248-49] Here, after creating and uploading the suspect's SNP profile into GEDMatch, Parabon obtained a list of matches that included the same information that other consumers receive (i.e., the shared segments of DNA, percentage of shared DNA, and name/alias and email). [Tr. 1250] There were "two promising matches, three potentially promising matches and many more distant matches." [R. 3645]

---

[5] Erin Murphy, *Law and Policy Oversight of Familial Searches in Recreational Genealogy Databases,* FORENSIC SCIENCE INT'L 292, at e5-e6 (2018) [hereinafter *Recreational Genealogy Databases*].

A genetic genealogist at Parabon, CeCe Moore, then used online social media accounts and public records databases to fill out the family tree for these matches and identify possible or likely sources for the suspect DNA. [Tr. 815, 1218-19; R. 3647-48] Moore calculates the likely relationship a match shares with the source DNA based on the percentage of overlap; i.e., 3 percent of shared DNA correlates with a second cousin relationship. [Tr. 1221] Here, the source DNA shared 23 percent of DNA with its closest match, which correlates with a half sibling or aunt/nephew relationship. [R. 3647] That means the amount of DNA disclosed to Parabon amounted to "hundreds of thousands" of shared genetic markers. [Tr. 1227, 1250; R. 3646]

The 23 percent match used an alias, which was disclosed to Parabon, but Moore was nonetheless able to ascertain the person's actual identity, M.H.[6] [R. 3427-28] Moore then used online public records databases to map out M.H.'s family tree and identify Downs as a potential or likely source of the DNA. [Tr. 1228] Downs is M.H.'s nephew, and Moore discovered that he attended UAF and stayed in the Bartlett dorm in 1993. [R. 3648] Moore described this as a straightforward instance of genealogical research, given the closeness of the match and limited number of qualifying relatives, but Moore nonetheless spent approximately ten hours researching M.H.'s family and the relationships between its members.[7] [Tr. 1241]

---

[6] This information was provided in Moore's grand jury testimony, which was submitted to and considered by the court in its ruling. [R. 1441, 3427-28, 3160; Tr. 1885]

[7] Genealogists may spend much more time engaged in such research depending on the remoteness of the match and complexity of the relevant family tree. For instance, in the Golden State Killer Case, it took a team of five individuals working for a total of four months to identify a common ancestor, from several remote third-cousin matches found on GEDmatch, and to then construct a family tree that produced a

Moore eventually generated a report, which included the chromosome locations for the 63 matching segments of DNA disclosed to Parabon. [R. 3646] Based on an analysis of this DNA, the report identified the subject/target of the search as likely being North European in ancestry, as having a Y-chromosome DNA haplogroup associated with Northern or Eastern Europe, and as likely having fair skin, hazel or brown eyes, brown hair, and some freckles. [R. 3645; Tr. 1241] Her report also included a summary of where Downs had lived throughout his life, who his family members were, and details regarding his deed and mortgage. [R. 3648-49]

Once McPherron learned of Downs as a possible suspect, he arranged for various forms of surveillance of Downs.[8] [Tr. 20-28, 34-41] These surveillance efforts continued for almost two months but were unsuccessful in obtaining Downs' DNA. [Tr. 20-21, 25] McPherron eventually obtained and executed a warrant. [Tr. 42]

2. GEDmatch's privacy policy

GEDmatch revised its privacy policy in May 2018, before Parabon conducted its search in this case. [Tr. 1342; R. 49-56, 3139-46]. This revised policy stated that: "GEDmatch respects your privacy and recognizes the importance of your personal information;" it also said it is "committed to protecting your information through our compliance with this Privacy Policy." [R. 49, 3139] And it informed users that "[r]aw

---

possible suspect based on his approximate age and residency. Michael Selvin, *A Too Permeating Police Surveillance: Consumer Genetic Genealogy and the Fourth Amendment After Carpenter*, 53 LOY. L.A. L. REV. 1015, 1015-17 (Summer 2020) [hereinafter *Permeating Police Surveillance*]

[8] These efforts included placing a pole camera in view of his home, having Maine detectives at times covertly follow him or his family members, having a Maine police officer concoct a reason to interact with him, and watching for Downs to put out his trash or otherwise discard an item that could contain his DNA. [Tr. 20-28, 34-41]

DNA data uploaded…remains the property of the person who uploaded it." [R. 52, 3142] The policy described GEDmatch's purpose as to share information with other researchers. [R. 50, 3140]

The policy includes law enforcement uploading DNA in order to identify a perpetrator of a violent crime as one of the authorized uses of its site. [R. 50, 3140] But another part of its policy stated:

> We may disclose your Raw Data, personal information, and/or Genealogy Data *if it is necessary to comply with a legal obligation such as a subpoena or warrant*. We will attempt to alert you to this disclosure of your Raw Data, personal information, and/or Genealogy Data, unless notification is prohibited under law.

[R. 49, 3139 (emphasis added)] The policy also emphasized that the results "on this Site are intended solely for genealogical research" but that GEDmatch could not guarantee that "users will not find other uses" such as "familial searching by…law enforcement agencies to identify the perpetrator of a crime." [R. 53-54, 3143-44]

The policy allowed users to protect their privacy by providing an alias if they did not want to disclose their identity. [R. 50-51, 3140-41] But the policy warned that "matches may be able to learn identity despite the use of an alias" particularly if their name is otherwise linked to their data, and that individuals should not upload any information if they "require absolute privacy and security." [R. 50-51, 3140-41]

Prior to the revision of this policy in May 2018, GEDmatch had not anticipated law enforcement using its service. [Tr. 1343-44] The revision to the policy followed some high-profile instances of law enforcement using GEDmatch to identify suspects and was intended to alert consumers to this possibility. [Tr. 1343-44, 1352-55] No information was presented as to when M.H.'s genetic information was uploaded to

GEDmatch or whether she actually read this or any other privacy policy. [Tr. 1248]

3. Downs' motion to suppress

Downs filed a motion to suppress the evidence obtained as a result of the police agents' search of GEDmatch. [R. 279-86, 573-74] The state opposed, and the court denied Downs' motion to suppress. [R. 34-48, 1435-43] First, it held that Downs had no standing to assert any violation because it was not his DNA that was searched and because Downs lacked vicarious standing under the *Waring* test. [R. 1437-39] The court also rejected consideration of a broader vicarious standing test. [R. 1437-38]

The court alternatively found that law enforcement did not violate either Downs' or M.H.'s right to be free from unreasonable searches because it concluded that neither Downs nor M.H. had either a subjective or a reasonable expectation of privacy in this information. [R. 1440-42] Specifically, the court found that Downs failed to prove he had a subjective or objective expectation of privacy in his "Aunt's DNA profile." [R. 1440] And it found that M.H. had no subjective expectation of privacy, despite using an alias, because she had voluntarily shared her DNA with GEDmatch after being warned that her identity could not be protected. [R. 1440-42] The court also determined society would not recognize any expectation of privacy as reasonable under these circumstances. [R. 1442]

C. Law enforcement conducted an unreasonable search that violated the Alaska and federal constitutions.

As technological and surveillance capabilities for law enforcement increase in scope and intensity, these advances risk upsetting long-standing and well-established notions of privacy. Courts have responded to this risk by seeking "to

assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted" and, when necessary, have expanded existing fourth amendment protections and placed "obstacles in the way of a too permeating police surveillance."[9] Specifically, courts have done so by narrowing the search incident to arrest and third party doctrines,[10] and by broadening the concept of a search beyond what a "mechanical interpretation of the fourth amendment" would have recognized.[11] There has also been a resurgence of property-based theories of Fourth Amendment protection that protect one's property even when privacy-based theories of the Fourth Amendment may not.[12]

Warrantless searches of genetic genealogy databases threaten established notions of privacy by granting law enforcement access to information-rich areas of DNA, allowing them to uncover intimate biological details and familial associations. This technological advance is so new that vanishingly few appellate courts—and no Alaskan appellate court—have addressed this novel method of law enforcement investigation. As discussed further below, the search here violated both the *Katz* reasonable expectation of privacy test and a property-based theory of Fourth Amendment protections, as well as the more extensive protections of the Alaska

---

[9] *Carpenter v. United States,* 138 S.Ct. 2206, 2214 (2018).

[10] *Riley v. California,* 573 U.S. 373, 382-401 (2014) (modifying search incident to arrest exception so that phones cannot be included in such a search); *Carpenter,* 138 S.Ct. at 2214-2220 (modifying third party doctrine so that it does not apply with regards to cell site location data possessed by phone carriers).

[11] *Carpenter,* 138 S.Ct. at 2214 (referring to *Kyllo v. United States*, 533 U.S. 27 (2001)).

[12] *See Florida v. Jardines*, 569 U.S. 1, 10-12 (2013); *Jones v. State,* 565 U.S. 400 402-12 (2012).

Constitution's privacy and search and seizure clause.

1. Law enforcement's actions constituted a search.

a. The state interfered with M.H. and Downs' reasonable expectation of privacy.

Because "the Fourth Amendment protects people not places," a search occurs whenever the government intrudes on some space or information that a person has manifested a subjective expectation of privacy in, so long as society recognizes that expectation as reasonable.[13] Because the federal constitution provides a floor but not a ceiling, if a search occurred under the federal constitution, then a search also occurred under the Alaska Constitution.

But because Alaska's constitution affords broader protections in this area, state action can constitute a search under the Alaska constitution even if no search occurred under the federal constitution.[14] That is, although Alaskan courts follow the same analytical framework for determining whether a reasonable expectation of privacy has been violated, Alaska law is more likely to recognize that an expectation of privacy is reasonable; and that is in large part because the Alaska Constitution "explicitly recognizes and protects the right to privacy."[15] Whether an expectation of privacy is reasonable under the Alaska Constitution turns on a "value judgment" rather than a factual question.[16] And the ultimate question is "whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional

---

[13] *Katz v. United States,* 389 U.S. 347, 351 (1967).
[14] *State v. McKelvey,* 544 P.3d 632, 640-41 (Alaska 2024).
[15] *Id.*
[16] *Id.*

restraints, the amount of privacy and freedom remaining to citizens would be diminished to a degree inconsistent with the aims of a free and open society."[17]

i. M.H. and Downs each had a subjective expectation of privacy.

The trial court found that neither M.H. nor Downs had a subjective expectation of privacy in their shared segments of DNA. [R. 1440-42] As to Downs, the court concluded that there was no evidence suggesting he had an "expectation of privacy in his aunt's DNA profile." [R. 1440] As to M.H., the court concluded that M.H. did not evince an expectation of privacy by uploading her DNA to be shared on GEDmatch—even though she used an alias—since GEDmatch's policy warned users that their DNA could be shared and that use of an alias was not foolproof. [R. 1441]

The court was wrong. As to Downs, the question was not whether he had a subjective expectation of privacy in his aunt's DNA profile; it is whether he had an expectation of privacy in the approximately 23 percent of his genetic code that he shares with M.H. and that was disclosed to police. [R. 1440] Through additional investigation, police inferred that this was also Downs' DNA; and their use of an inference does not insulate this from being considered part of their search.[18]

When evaluated in this framework, Downs had a subjective expectation of privacy in these shared segments of his own genetic code. Courts generally presume individuals have a subjective expectation of privacy in their own DNA, at least until

---

[17] *Id.* (internal citations omitted).

[18] *Carpenter*, 138 S.Ct. at 2218 ("[T]he court has already rejected the proposition that 'inference insulates a search[.]'"); *Kyllo,* 533 U.S. at 36-37 (holding that the use of technology to warrantlessly infer information that violated reasonable expectations of privacy constituted a search).

they voluntarily relinquish it to law enforcement.[19] This is consistent with the presumption that a subjective expectation of privacy exists with regards to private or sensitive information generally.[20] Downs never voluntarily revealed or shared his DNA with police or anyone else. As such, Downs retained a subjective expectation of privacy in his own shared segments of DNA.[21]

M.H. also had a subjective expectation of privacy in this portion of her genetic code. [R. 1441] While M.H. voluntarily uploaded her DNA to GEDmatch to share with potential relatives, there is no indication she intended to provide it to police. She also protected her identity and privacy by using an alias. [Tr. 3427-28] That was sufficient to establish a subjective expectation of privacy because it demonstrated an intent to keep this highly personal information anonymous, and therefore private.[22]

The trial court rejected M.H.'s use of an alias as demonstrating her intent to keep her DNA private because GEDmatch's privacy policy warned consumers that

---

[19] *United States v. Davis,* 657 F.Supp.2d 630, 645 (D.Md.2009) (noting that courts "seem to operate on the premise that individuals *always* have a *subjective* expectation of privacy in their DNA, unless…a DNA sample is taken from them, with their knowledge, for law enforcement purposes) (emphasis in original).

[20] See *Glass v. State*, 583 P.2d 872, 880 (Alaska 1978) (holding that a subjective expectation of privacy exists when an individual communicates "private matters to another").

[21] *Id.*

[22] LaFave, 1 SEARCH & SEIZURE 2.1(c) (6th ed. 2022) (surmising that a subjective expectation of privacy exists when one's conduct demonstrates an intent to keep some activity or information private); *see also Beltz v. State,* 221 P.3d 328, 333 & 335 (Alaska 2009) (presuming that a subjective expectation of privacy existed with regards to trash put out for collection and holding that this subjective expectation was objectively reasonable to a degree—even though the trash was intended for third-parties to find—because of "the highly personal information that is contained in trash," including the potential for collecting DNA evidence).

use of an alias did not guarantee anonymity. But an individual need not "ensure against all conceivable efforts at scrutiny" or take "extraordinary precautions" in order to demonstrate a subjective intent to keep information private.[23] The fact that M.H. erected a barrier to discovery of her identity is sufficient to demonstrate her intent to keep her personal information private.

ii. Society generally, and Alaskan society in particular, recognizes these expectations of privacy as reasonable.

In evaluating whether Downs and/or M.H.'s expectation of privacy is one that society is prepared to recognize as reasonable, the question is ultimately whether the government violated the privacy upon which an individual justifiably relied;[24] or intruded upon the privacy of the individual to a degree "that a reasonable person would not have anticipated,"[25] or that is "inconsistent with the aims of a free and open society."[26] That is, society—through courts—must sanction the privacy interest as being legitimate. Common experience, historical precedent, and social values and norms are all relevant to assessing whether an expectation of privacy is reasonable.[27]

---

[23] SEARCH & SEIZURE, at § 2.1(c)*; see also Cowles v. State,* 23 P.3d 1168, 1171 (Alaska 2001) (recognizing that the defendant had a subjective—though ultimately not reasonable—expectation of privacy in her conduct in an on office during the work day despite other people coming and going); *Glass*, 583 P.3d at 880 (recognizing a subjective expectation of privacy in the conversation the defendant had with another person).

[24] *Katz,* 389 U.S. at 351-53.

[25] *Jones,* 565 U.S. at 430 (Alito, J., concurring).

[26] *McKelvey,* 544 P.3d at 636.

[27] *Id*. at 430 (Alito, J., concurring) (resolving that long-term GPS monitoring of a car violated reasonable expectations of privacy in part by considering the absence of any historical analogue for such a search prior to advances in technology); *California v. Greenwood,* 486 U.S. 35, 51 n.3 (1988) (Brennan, J., dissenting) ("expectations of

And while a person often has no reasonable expectation of privacy in information that they willingly expose to others, this so-called "third-party doctrine" is not without limits—particularly where the information at issue is intimate, extensive and especially where it is involuntarily or unwittingly in the possession of a third party.[28]

Without further analysis, the trial court determined that Downs had no reasonable expectation of privacy in the shared portion of his genetic code that law enforcement examined because Downs did not cite to any evidence or caselaw directly holding or stating this. [R. 1440-41] And the appellate case to most directly address this issue, *State v. Hartman,* concluded that the defendant failed to establish a reasonable or legitimate expectation of privacy in the DNA he had in common with family members who used GEDMatch.[29] The Washington Court of Appeals concluded the defendant did not have a "valid privacy interest in the segments of his DNA that he had in common" with his relatives,[30] noting that there is no "historical protection for voluntarily shared genetic material" and relying on its determination that the DNA at issue had been voluntarily exposed by the relatives and that law enforcement

---

privacy are established by general social norms"); LaFave, 1 Search & Seizure 2.1(d) (noting that the *Katz* test reflects a value judgment from society).

[28] *See Carpenter,* 138 S.Ct. at 2216-20 (recognizing limits on application of the third-party doctrine with regards to cell site location data possessed by phone companies); *Katz,* 389 U.S. at 351-52 (stating that an individual may have a reasonable expectation of privacy in what he "seeks to preserve as private, even in an area accessible to the public"); *see also infra* Part. I.C.a.iii.

[29] 534 P.3d 423, 432-38. (Wash. App. 2023) Though resolved as a standing issue, the court's analysis considered whether the defendant possessed a "legitimate expectation of privacy in the place searched," a test functionally similar to the *Katz* test. *Id* at 432*; see Minnesota v. Carter,* 525 U.S. 83, 101 (1998) (Kennedy, J., concurring) (citing to the *Katz* test in resolving whether standing existed).

[30] *Id.* at 437.

conducted the search for the limited purpose of discovering a killer's identity and in compliance with GEDmatch's policy.[31]

But the court and *Hartman's* analysis undervalues the risk of widespread and indiscriminate access to DNA by the state—particularly in the form of SNP profiles. It also superficially and "mechanically" applies existing doctrine to a new technology—one that gives law enforcement unfettered access into areas of life previously kept private and inaccessible to government.[32] This court should reject the trial court and *Hartman*'s conclusion that a reasonable expectation of privacy does not exist here.

To begin with, DNA testing and analysis, even when limited to testing of the junk regions in STR profiles, is (at least absent a diminished expectation of privacy) appropriately considered a search.[33] That is because a person retains a "legitimate expectation of privacy in the information obtained from the testing,"[34] i.e. their identity, which can be used to connect a person to a location, activity, or intimate association.

This expectation of privacy is much stronger when the DNA profile at issue is a SNP profile. While STR profiles are typically used in the criminal realm because they reveal little personal or medical information beyond identity,[35] SNP profiles are used

---

[31] *Hartman,* 534 P.3d at 434-35.

[32] *Carpenter*, 138 S.Ct. at 2019; *see also McKelvey,* 544 P.3d at 645 (rejecting a mechanical extension of open view doctrine to aerial surveillance).

[33] *See United States v. Davis,* 690 F.3d 226, 243-45 (4th Cir. 2012) (holding that the defendant had a reasonable expectation of privacy in the testing of DNA to determine identity), *cert denied*, 571 U.S. 829 (2013).

[34] *Id.* at 243-45.

[35] *See Maryland v. King,* 569 U.S. 435, 442-43 (2013) (identifying the DNA testing at issue in Maryland's DNA collection statute as being limited to analysis of 'junk DNA' or a portion of the noncoding region that is limited to determining a person's identity without revealing "more farreaching and complex characteristics like genetic traits").

in the genealogy context precisely because they have "informational richness" that reveals much more information about a person,[36] including their "sex, physical appearance, medical conditions, genetic history, and ancestral origin."[37] Such information "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."[38] Thus, much more intimate information and associations are implicated with SNP profiles.[39]

Genetic genealogy searches, particularly in combination with a search of other public records and resources, are used by law enforcement in ways that implicate these broader privacy concerns. First, law enforcement uses the information learned from these searches to construct a family tree delineating an individual's familial associations. This can reveal a variety of intimate associations, including "abandoned parental bonds, adoptee relationships, children conceived through technology, even family secrets about paternal identity."[40] In *State v. Carbo,* a case involving a related challenge to law enforcement's use of SNP technology, investigators learned than an individual was "fathered by someone other than that [person's] father of record."[41]

---

[36] *Recreational Genealogy Databases*, *supra* note 5, at e5.

[37] *See Hartman,* 534 P.3d at 428 (internal citations omitted).

[38] *Id.* at 434.

[39] *See State v. Carbo,* ___N.W.3d___, 2024 WL 2035660 at *11 (Minn. May 8, 2024) (Procaccini, J., concurring in part) (recognizing that the "sensitive genetic information revealed by a SNP analysis is *quintessentially personal*" and comparable to other things courts have modified existing precedent to protect such as cellphones and long-term movements; and also that SNP profiles diminish the privacy of relatives as well) (emphasis in original).

[40] *Permeating Police Surveillance*, *supra* note 7, at 1049 (internal citations omitted).

[41] 2024 WL 2035660 at *11 (Procaccini, J., concurring in part).

Second, this investigative method can also be used by law enforcement to reveal an individual's biological information, such as their disease proclivities or other "biological characteristics."[42] It can reveal information about a person's "physical appearance, medical conditions, genetic history, and ancestral origin."[43] These searches thus reveal information that society has long recognized as highly confidential and protected.[44]

Moreover, the reach of this form of surveillance is almost limitless. At this point in time, "[l]ong range familial searches could return a match to virtually anyone" of European descent.[45] This amounts to a *de facto* universal DNA database being accessible to law enforcement without any regulation or oversight.[46]

As such, the breadth and depth of this investigative technique reveals "private aspects of identity [that are] susceptible to abuse [by law enforcement]," similar to other methods of investigation that have triggered Fourth Amendment protections due to their composite breadth and depth, such as long-term GPS tracking.[47]

---

[42] *Id.* at 1040; *see also* Victoria Romine, *Crime, DNA, and Family: Protecting Genetic Privacy in the World of 23and me*, 53 ARIZ. ST. L.J. 367, 379 (Spring 2021) (stating that such searches can "reveal information about a person's sex, physical appearance, medical conditions, genetic history, and ancestral origin").

[43] *Hartman,* 534 P.3d at 428.

[44] *See McKelvey,* 544 P.3d at 645 (identifying "the degree to which a type of police surveillance can reveal intimate details" as the most important factor in determining whether there is an objective expectation of privacy).

[45] *Recreational Genealogy Databases, supra* note 5, e7.

[46] *See* Meghan Ryan, *The Privacy, Probability, and Political Pitfalls of Universal DNA Collection*, 20 SMU SCI. & TECH. L. REV. 3, 10-12 (Spring 2017) [hereinafter *Political Pitfalls of Universal DNA Collection*] (identifying the privacy concerns associated with universal DNA database subject to regulation).

[47] *Jones,* 565 U.S. at 416 (Sotomoyer, J., concurring); *see also Carbo*, 2024 WL 2035660 at *11-12 (Procaccini, J., concurring in part) ("the private nature of the

Alternatively, if the expectation of privacy is not reasonable under the Fourth Amendment, the Alaska Constitution nevertheless protects M.H. and Downs. Alaska's privacy clause[48] is most protective of personal autonomy and sensitive information.[49] And a primary motivation for enacting Alaska's privacy clause was a concern about advancing technology aggregating personal data that government could use against its people, such as by compiling "secret dossiers on Alaska citizens."[50]

That concern—and Alaskan's sense of security in light of this concern—is directly implicated by genetic genealogy searches. Such searches by law enforcement begin with the conversion of a genealogical hobby website into an unregulated DNA database, thereby taking advantage of technological aggregations of data to unwittingly collect sensitive information against its citizens. Law enforcement combines this information with other aggregated data, from public records and websites amassing a scattered disclosure of facts, to map out and investigate a person's biological traits and intimate familial associations.

Given the breadth and depth of information at issue, allowing these kinds of "unfettered searches" to occur would directly threaten "Alaskan's sense of security and privacy."[51] The Alaska Constitution thus recognizes Downs' and M.H.'s expectation of privacy as reasonable, even if the Fourth Amendment does not.

---

information revealed by a SNP analysis, the potential harm that can be wrought by its misuse, and the historical difficulty in accessing this kind of information counsel us to recognize that society would find an expectation of privacy reasonable here").

[48] ALASKA CONST. art. I, § 22.

[49] *Doe v. Dep't of Public Safety,* 444 P.3d 116, 127 (Alaska 2019).

[50] *Id.* at 128.

[51] *McKelvey,* 544 P.3d at 646.

Otherwise, Alaskans' privacy would be diminished and the potential for unwarranted governmental intrusion and misuse of intimate information would go unchecked.

iii. Neither the third-party doctrine nor GEDmatch's privacy policy undermine the reasonableness of M.H.'s and Downs' expectation of privacy.

The third-party doctrine provides that a person has no reasonable expectation of privacy in information exposed to others. But as the *Carpenter* Court recognized, there are limitations to this doctrine—particularly with regard to new technology and its potential to encroach on information long-considered private in nature.[52] A proper application of the third-party doctrine requires consideration of the nature and extent of the information at issue, how the information came into the possession of the third party, and whether a search of this information represents a new encroachment by law enforcement into previously private realms.[53]

The third-party doctrine does not defeat the reasonableness of Downs' expectation of privacy. In *Hartman,* the Washington Court of Appeals viewed the uploading of DNA as a voluntary decision by the relatives that resulted in a forfeiture of the defendant's privacy.[54] But, under *Carpenter,* this analysis is misguided and does not accord with society's, especially Alaskan's, understanding of privacy. Downs had no choice over whether a third party would possess this information, which weighs against application of the third party doctrine under *Carpenter*.[55] And to the extent

---

[52] *See Carpenter,* 138 S.Ct. at 2216-20.

[53] *Id.*

[54] *Hartman,* 534 P.3d at 43-35.

[55] *Carpenter,* 138 S.Ct at 2220; *see also* Hillary Kody, *Standing to Challenge Familial Searches of Commercial DNA Databases*, 61 WM. & MARY L. REV. 287, 310-11

there is an absence of "historical protection for voluntarily shared genetic material" specifically[56]—itself a newly emerging concept—society and the law nonetheless recognize contexts where shared ownership or privacy interests restricts one person's ability to unilaterally waive the rights of another, such as joint tenancy.[57] More fundamentally, the idea that *your* consent amounts to *my* consent with regards to a shared intimacy or information is a "fiction that has been expressly rejected" by Alaskan courts especially "in the context of warrantless searches and seizures."[58] Downs and M.H. both had a privacy interest in the shared segments of their DNA, and M.H. could not unilaterally waive Downs' privacy interest in it.

Moreover, as in *Carpenter,* the breadth and intimacy of the information at issue, particularly in combination with other information from public records searches, potentially reveals a variety of familial and medical details that go well beyond the scope of surveillance that law enforcement has historically engaged in or that are traditionally justified under the third-party exception.[59] As one commentator put it,

> In genetic genealogy investigations, law enforcement learns not only that kinship exists, but how closely and on what side of the family, and it can draw inferences about biological characteristics of members of the family tree based upon the genetic information in the database profiles…[In the

(arguing that, under *Carpenter,* the third-party doctrine does not defeat an expectation of privacy in this context in part because of no voluntary exposure by the suspect).

[56] *Hartman,* 534 P.3d at 434-35. *But see* infra n.61.

[57] Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 336-37 (2010) (analogizing the individual's interest in "their half of the databased kin's genetic code" to "the joint interest held by property owners who share the same space;" in which context, under *Georgia v. Randolph,* 547 U.S. 103, 106 (2006), the consent of both parties, when present, is required for a valid consent to a search to exist).

[58] *Glass,* 583 P.2d at 877 (internal citations omitted).

[59] *Carpenter,* 138 S.Ct at 2216-18.

> aggregate,] genetic genealogy investigations delve very deeply into the intimate personal details of many relatives of the forensic source sample, potentially revealing if an individual was born out of wedlock, was the produce of incest, or carries genetic diseases.[60]

Given the involuntary nature with which Downs' private information came into the possession of a third party, the intimate nature and broad surveillance possibilities involved in this technology, and the reality that this kind of search would allow law enforcement to encroach upon previously private realms of life indiscriminately, the third-party doctrine should not apply here.

Nor does the third-party doctrine undermine M.H.'s reasonable expectation of privacy, given the circumstances under which she uploaded her DNA to GEDmatch, The trial court found that there was a lack of evidence that "society at large recognizes an expectation of privacy" in information voluntarily uploaded into this kind of database. [R. 1441-42] But there are compelling indications that society does recognize an expectation of privacy in this context.[61] In particular, in response to a public backlash

---

[60] *Permeating Police Surveillance*, *supra* note 7, at 1040-42 (internal quotes omitted).

[61] *Id.* at 2262 (Gorsuch, J., dissenting) (describing the possibility that the government could get a citizen's DNA from a genealogical database without a warrant or probable cause as a result that would strike "[m]ost lawyers and judges today—me included—as pretty unlikely"); Elizabth Joh, "Want to See My Genes? Get a Warrant," N.Y. TIMES (June 11, 2019), available at http://www.nytimes.com/2019/06/11/opinion/police-dna-warrant.html (advocating for legislative and judicial regulation of law enforcement's use of genetic genealogy websites); Megan Molteni, "The Creepy Genetics Behind the Golden State Killer Case," Wired (April 27, 2018), available at https://www.wired.com/story/detectives-cracked-the-golden-state-killer-case-using-genetics/ (identifying privacy concerns associated with investigative use of GEDMatch). Parabon's genealogist also testified that she believed people should be able to decide what happens to their own DNA. [Tr. 1230-31] And despite the recency of this investigative technique, four states—California, Maryland, Montana, and Minnesota—have passed laws limiting such searches. *See* M.S.A. § 325F.995, Subd.2 (Minn. 2023) (requiring a warrant or court order prior to disclosure of this genetic data to law enforcement); MCA 44.6.104 (2021 MT LEGIS 413 (H.B. 602))

to GEDmatch's cooperation with law enforcement, GEDmatch amended its privacy settings (after police obtained its lead in this case) to give users a default opt-out option with regards to whether law enforcement could search their DNA.[62] The vast majority of users remained opted out,[63] strongly suggesting that reasonable individuals and society generally expects privacy in this context—at least from indiscriminate searches by the government. Moreover, society certainly views DNA,[64] medical information,[65] and intimate familial associations as private matters.[66]

When M.H. uploaded her DNA sometime prior to October 2018, there was no option to opt out of law enforcement searches. [R. 49-56] Nor was it a widely known or established practice for law enforcement to engage in this kind of familial search in 2018 such that a reasonable person would have anticipated she would be subjecting

---

(requiring a warrant or consent to conduct such searches); Maryland Code of Crim. P. § 17-102 (2021 Maryland Laws Ch. 681 (H.B. 240)) (providing that such genetic searches can only occur with judicial authorization after certification before a court that certain investigative pre-conditions have been satisfied and that the genealogy website obtains explicit consent from its users); CA Civil § 56.181 (2021 Cal. Legis. Serv. Ch. 596 (S.B. 41)) (requiring customers give express consent before their DNA can be shared with a third party).

[62] *Permeating Police Surveillance*, *supra* note 7, at 1023-24.

[63] *Id.* at 1024 (noting that only 185,000 of 1.3 million GEDmatch users elected to opt-in to law enforcement being authorized to search their DNA).

[64] *See Pitfalls of Universal DNA Collection*, *supra* note 46 at 10-12 (identifying privacy concerns associated with a regulated, legislatively created universal DNA database).

[65] *See, e.g.,* Health Insurance Portability and Accountability Act of 1996 (HIPPA), 42 U.S.C. 1320 (1996).

[66] *See Jones,* 565 U.S. at 415 (Sotomayor, J., concurring) (identifying "familial…associations" as one of the intimate associations long-term GPS monitoring may intrude upon).

herself to such searches by using GEDmatch.[67]

Nor does GEDmatch's privacy policy establish that M.H. did not have a reasonable expectation of privacy in her DNA or knowingly relinquished this information to a third party for purposes of sharing with police. In *Hartman,* the Washington Court of Appeals concluded that law enforcement's compliance with GEDmatch's privacy policy suggested there was no reasonable expectation of privacy in that information.[68] But the state's purported compliance with GEDmatch's privacy policy here does not negate M.H.'s reasonable expectation of privacy nor does it demonstrate the applicability of the third-party doctrine.

The state did not establish that M.H. read the May 2018 privacy policy. But even assuming she did, the policy does not make clear that law enforcement could indiscriminately search her DNA. Though the policy identified law enforcement investigations as one of the purposes for which DNA could be uploaded to the cite, the policy also informed M.H. that her DNA or personal information "may be disclosed if it is necessary to comply with a legal obligation such as a subpoena or warrant" and that she would generally be notified of such searches. [R. 49-50] The policy also stated that M.H. was still the owner of her DNA, that her privacy was valued, that her personal information and DNA would "never" be released except as specifically noted in the

---

[67] *Id.* at 430 (Alito, J., concurring) (stating that the test is "whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated"). The Golden State Killer appears to have been the first reported use of a genealogy website for this purpose, and this individual was arrested in April 2018; Parabon conducted its search around October 2018. *See Recreational Genealogy Database, supra* n.5 at e5 [R. 1239]

[68] *Hartman,* 534 P.3d at 435.

policy, and that the site was intended to be used "solely for genealogical research" even though individual users—including law enforcement—may use it for other purposes. [R. 52, 53, 54] Reading these separate provisions together, they suggest that GEDmatch permits law enforcement to conduct familial searches when it is legally required to do so, but that this is not the website's purpose.

Moreover, M.H. shared the matching segments of DNA on GEDmatch through an alias—thus demonstrating her desire to nonetheless maintain privacy and anonymity. As LaFave has described it, the question in resolving whether an expectation of privacy should be recognized as reasonable ultimately turns on whether the relevant search would, if unchecked, "encroach too much upon an individual's 'sense of security' or impose unreasonable burdens upon those who wished to maintain that security."[69] Individuals who want to engage in recreational genealogy, but who also want to maintain their privacy from a government search, should not be forced to choose between the two.[70] Nor should the third-party doctrine defeat M.H.'s expectation of privacy, particularly under the Alaska Constitution, in light of these circumstances and the extent of intimate information at issue.

b. Law enforcement interfered with M.H.'s and Downs' property.

The *Katz* reasonable expectation of privacy test supplements but does not

[69] Search & Seizure, at 2.1(d) (internal citations omitted).

[70] *See McKelvey,* 544 P.3d at 644 & 648 (rejecting that individuals in a free society should be forced to "give up the privacy of their yards just because it is not feasible to block aerial surveillance" and stating that, under the Alaska Constitution, the reasonableness of a search is a value judgment that depends on "whether the government's unregulated use of technology to observe is consistent with Alaskans' expectation of a free society")).

encompass the entirety of protections offered by the Fourth Amendment.[71] If property is "your(s)," then it may receive Fourth Amendment protection regardless whether the traditional *Katz* test would be satisfied.[72] Moreover, "[u]nder this more traditional approach, Fourth Amendment protections do not automatically disappear just because you share them with third parties."[73] That is because, as Justice Gorsuch has explained, assuming the risk of or consenting "to give a third party access" to one's property or papers is not the same thing as assuming the responsibility for, or consenting to, a search of those things by the government.[74]

Here, under the terms of the policy with GEDmatch, M.H.'s DNA remained her property. [R. 52] And Downs never relinquished his authority over the segments of DNA he shared with M.H.. Nor does it matter that they shared these segments of DNA since Downs need not demonstrate exclusive ownership in order to assert a property-based Fourth Amendment right.[75] This is particularly true given the extensive rights Alaska law affords to individuals over any form or analysis of their own genetic code, including the right to consent before disclosure of their DNA.[76]

---

[71] *Jones,* 565 U.S. at 408-12.

[72] *Carpenter,* 138 S.Ct at 2264 & 2267-71 (Gorsuch, J., dissenting).

[73] *Id.* at 2268. (Gorsuch, J., dissenting).

[74] *Id.* at 2263 (Gorsuch, J., dissenting).

[75] *Id.* at 2269 (Gorsuch, J., dissenting) (stating that "complete ownership or exclusive control of property" is not required for "the assertion of a Fourth Amendment right").

[76] *See* ALASKA CONST. Art. I § 21 ("The enumeration of rights in this constitution shall not impair or deny others retained by the people"); AS 18.13.010(a)(1) (stating that "a person may not collect a DNA sample from a person, perform a DNA analysis on a sample, retain a DNA sample or the results of a DNA analysis, or disclose the results of a DNA analysis unless the person has first obtained the informed and written consent of the person, or the person's legal guardian or authorized representative, for the collection, analysis, retention, or disclosure"). Alaska Statute 18.13.010(b) does

As such, GEDmatch acted, at best, as a bailee who held on to this property for a limited purpose, that of "genealogical research."[77] [R. 53] Law enforcement was not engaged in genealogical research when they conducted (through Parabon) a search of M.H./Downs' DNA, they were generating leads in order to solve a crime. As such, their use of this property amounted to an improper conversion that triggers constitutional protections.[78]

c. Downs has standing to challenge the search.

The trial court determined that Downs lacked standing to challenge the search. [R. 1437-39] Standing in the criminal context is policy-based, rather than being jurisdictional in nature,[79] and exists whenever a person has a "reasonable expectation of freedom from governmental intrusion" in the place or information searched, and thus is largely duplicative of the previous reasonable expectation of privacy analysis.[80] The state violated Downs' privacy when it searched the segments of DNA he shares with M.H. and combined that with other information to reconstruct his own background

---

create an exception for a "law enforcement purpose, including the identification of perpetrators and the investigation of crimes." AS 18.13.010(b)(2). But the Fourth Amendment places limits on the extent to which the government can create exceptions in positive law to allow its own warrantless searches. *Carpenter,* 138 S.Ct. at 2270-71 (Gorsuch, J., dissenting).

[77] *Carpenter*, 138 S.Ct at 2268-69 (Gorsuch, J., dissenting) (explaining how bailments have historically functioned under property law).

[78] *Id.* at 2269.

[79] *Byrd v. United States*, 138 S.Ct. 1518, 1530 (2018).

[80] *Mancusi v. DeForte,* 392 U.S. 364, 368 (1968); *see also Rakas v. Illiinois*, 439 U.S. 128, 149 (1978) (explaining that standing to assert Fourth Amendment violation exists when the person can satisfy *Katz,* i.e., can "legitimately expect privacy in the areas" searched); SEARCH & SEIZURE, at 11.3(f) (stating "reasonable expectation of freedom from governmental intrusion" or reasonable expectation of privacy test is applicable to standing questions for places or items storing things or information).

and family tree.[81] The state gained access to Downs' genetic traits and medical conditions, as much as M.H.'s, though its search; and it researched and investigated Downs' living and financial history and intimate familial associations through this information. [R. 3645-49] Because the trial court's determination that Downs lacked standing was premised on its incorrect conclusion that Downs lacked a reasonable expectation of privacy in this context, Downs has standing. [R. 1439-42]

The trial court also rejected Downs' claim that he had vicarious standing under a broad construction of Alaska's vicarious standing doctrine. [R. 1438-39] In *Waring v. State*, the Alaska Supreme Court recognized two contexts where the purposes of the exclusionary rule – deterrence of law enforcement and protection of judicial integrity – support allowing an individual to challenge the violation of a co-defendant's constitutional rights: when the search involves "gross or shocking misconduct" and when a co-defendant's rights are purposefully violated (so as to secure evidence against the defendant).[82] The court found that neither exception applied and also rejected Downs' request to expand vicarious standing.[83] [R. 280-283, 1439]

An expanded notion of standing, however, more fully protects and vindicates the Alaska Constitution's privacy and search and seizure clauses when the person

---

[81] *Recreational Genealogy, supra* note 5, at e5 (describing SNP profiles as informationally rich and capable of revealing a person's "disease carrier status, predictive wellness, and cosmetic conditions").

[82] 670 P.2d 357, 360-63 (Alaska 1983). The United States Supreme Court has largely rejected the doctrine of vicarious standing. *See Rakas,* 439 U.S. at 133-38.

[83] Specifically, the court refused to apply the *Falcon* test, Alaska's expanded civil test for determining standing, stating that *Waring* controlled the issue of vicarious standing in the criminal context. [R. 1437-39] 570 P.2d 469 (Alaska 1977).

whose privacy was violated is not a party, at least where the privacy interests of the defendant are closely aligned with the uninvolved third party. The *Waring* court explained that, absent a deliberate violation or shocking police misconduct, the deterrent purpose of the exclusionary rule is generally met when the police violate the rights of a co-defendant—because the co-defendant can himself invoke the exclusionary rule.[84] But the same is not true when police violate the rights of uninvolved third parties. In those instances, there will generally be no one to invoke the exclusionary rule, and thus no effective deterrent will exist.[85] At least where the defendant has a closely-aligned privacy interest with the third party, such as here, it is fully consist with—and more adequately ensures—vindication of Alaska's constitutional provisions to extend standing.[86] Thus, even if Downs does not have direct standing, he may still challenge the search under the Alaska Constitution.[87]

---

[84] *Waring,* 670 P.2d at 361.

[85] *Dimmick,* 473 P.2d at 627 (Connor, J., dissenting in part) (citing *Mapp v. Ohio,* 367 U.S. at 652 (1961), and explaining that remedies other than the exclusionary rule have proved "worthless and futile" at deterring police misconduct).

[86] *See Waring,* 670 P.2d at 363 n.12 (recognizing that vicarious standing should be expanded further "if the goals of deterring unlawful police conduct require"); *Dimmick,* 473 P.2d at 626-27 (Connor, J., dissenting in part) (advocating for an expanded notion of standing focused on deterring police misconduct) *Samson v. State,* 919 P.2d 171, 173-75 (Alaska App. 1996) (Mannheimer, J., concurring) (recognizing, with Judge Bryner, the potential inadequacies of *Waring* when rights of individuals other than co-defendants are violated, and proposing an extension of standing if a pattern of violations occur).

[87] Alaskan courts—unlike federal and many state courts—also provide for automatic standing, i.e., removing standing requirements when the government charges the defendant with possessing an item that it also argues the defendant lacks standing to move to suppress; this relaxation of standing in other contexts further supports broadening vicarious standing when appropriate. *See Jarnig v. State,* 309 P.3d 1270, 1273-74 (Alaska App. 2013).

2. The search was unreasonable.

This search occurred without a warrant and no exception to the warrant requirement existed.[88] The search, therefore, was presumptively unreasonable.[89] Under both the federal and state constitutions, this presumption of unreasonableness cannot be overcome.

In *Maryland v. King,* the Supreme Court held that Maryland's DNA Collection Act, which required felony arrestees to submit to DNA searches upon their arrest, was reasonable despite the absence of a warrant or exception to the warrant requirement.[90] It did so by first concluding that a warrant was not required in that context, and by then concluding that the warrantless search was reasonable under the circumstances.[91] But that same analysis leads to the opposite conclusion here.

In *King*, Maryland had a non-investigative special need for their search (to confirm the identity of the arrestee), and the Supreme Court explained that this non-investigative purpose, in combination with the fact that the statute left no discretion in the hands of law enforcement, ultimately preponderated against requiring a warrant in this context.[92]

The *King* court then concluded the search was reasonable. First, the DNA collected under the act could only be analyzed under the "junk" non-coding regions

---

[88] The state did not argue that an exception to the warrant requirement existed, nor did the trial court find that one existed. [R. 38-48,1435-1443]

[89] *See Schikora v. State,* 652 P.2d 473, 475 (Alaska App. 1982) ("A warrantless search is presumed unreasonable unless justified by the state").

[90] 569 U.S. 435, 447-465 (2013).

[91] *Id.* at 465.

[92] *Id.* at 447-48.

and thus could only provide information about identity, rather than implicating any medical or other private information from DNA.[93] Indeed, the relevant statute regulated law enforcement's conduct in this area and protected against any "further invasion of privacy."[94] Second, the arrestees as a class had a diminished privacy interest because of their arrest and because probable cause of serious wrong-doing had been established, thus reducing the arrestee's "expectations of privacy and freedom from police scrutiny."[95] Given these factors, as well as the minimal physical intrusion involved, the Court concluded the search was reasonable.

Here, however, a warrant was required. Unlike the search in *King*, a genealogical search is not motivated by a special need separate from investigation. It is conducted to solve a crime, and the federal constitution requires individualized suspicion for such searches.[96] Moreover, the genealogical search here was not the kind of regulated, discretion-less search approved in *King*.[97] Quite the opposite, here there was no statute or regulation overseeing law enforcement's conduct in this case

---

[93] *Id.* at 464-65.

[94] *Id.* at 465.

[95] *Id.* at 463.

[96] *See Ferguson v. City of Charleston,* 532 U.S. 67, 68 (2001) (holding that in the absence of a warrant or particularized suspicion, the special need justifying the search must be "one divorced from the State's general interest in law enforcement"); *City of Indianapolis v. Edmond,* 531 U.S. 32, 42-43 (2000) ("We are particularly reluctant to recognize exceptions to the general rule of individualized suspicion where governmental authorities primarily pursue their general crime control ends"); *Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 653 ("Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, this Court has said that reasonableness generally requires the obtaining of a judicial warrant").

[97] *King,* 569 U.S. at 447-48 (recognizing that the statute's regulation of what, who, and how DNA could be searched under the statute was a factor weighing against the need for a warrant in that instance).

and this lack of oversight weighs heavily in favor of requiring a warrant.

And even if a warrant was not required, the search was nonetheless unreasonable. In *King,* the Court relied on the limited nature of the information that could be recovered from the DNA and the diminished expectation of privacy in concluding the warrantless search was reasonable.[98] But here, the information available in a SNP profile uploaded into GEDmatch is not limited practically (as a STR profile is) or legally (such as by Maryland's DNA Collection Act) to confirming identity; instead, a broad amount of sensitive information can be obtained from the DNA revealed on GEDmatch. Additionally, neither Downs nor M.H. had a diminished expectation of privacy from arrest or any other special status. Rather than constituting a targeted search of an individual with a diminished right to privacy for a precise purpose apart from investigation, a genealogical search is purposefully broad and indiscriminate, implicating the privacy of virtually every citizen of European descent.[99] Such a search is not reasonable under the federal constitution.

Finally, even if reasonable under the federal constitution, such a search was not reasonable under the Alaska constitution. Alaskan appellate courts have not yet definitively addressed whether Alaska's DNA Collection Act, AS 44.42.035, is constitutional nor have they analyzed or applied *King*.[100] But this court has noted the

---

[98] *Id.* at 463-65.

[99] *Recreational Genealogy Databases, supra* n.5 at e7.

[100] In *Nason v. State,* the Alaska Court of Appeals upheld AS 44.42.035(b) as "presumptively constitutional" but did not ultimately resolve the issue of whether the statute violated the Alaska Constitution's privacy or search and seizure clauses due to deficiencies in the briefing and the "difficult legal issues" at play, including this court's observation that "each rationale for DNA collection holds the potential for

"potential for government abuses" inherent in the collection of its citizens DNA,[101] and the "more protective requirements of the Alaska Constitution" would afford even broader protections and a greater weighing of the privacy interests in this matter.[102] Thus, even if reasonable under the federal constitution, such a warrantless and unrestricted search would be unreasonable under the Alaska Constitution.

II. The Trial Court Erred in Excluding an Alternative Suspect's Confession.

A. Standard of review

This court reviews evidentiary rulings for an abuse of discretion but reviews constitutional or legal questions raised by evidentiary rulings de novo.[103]

B. Factual background

Downs moved to present evidence regarding several alternative suspects at trial. [R. 438-53, 1394-1416, 3654-3999] One of those alternative suspects was Kenneth Moto, a student attending UAF at the time of S.S.'s murder[104] who police

---

government abuses and infringement of citizen privacy"). 102 P.3d 962, 963-66 (Alaska App. 2004).

[101] *Id.*

[102] *See Anchorage Policy Dep't Employees Ass'n v. Municipality of Anchorage,* 24 P.3d 547, 558-59 (holding that parts of a random drug testing policy for firefighter and police officers violated the Alaska Constitution's search and seizure provision regardless of whether it violated the federal constitution).

[103] *Smithart v. State,* 988 P.2d 583, 586 (Alaska 1999); *see also Dague v. State*, 81 P.3d 274, 282 (Alaska 2003) (explaining that existence of prejudice is legal question); *Booth v. State*, 251 P.3d 369, 372-73 (Alaska App. 2011) (explaining that standard of review is legal question).

[104] Moto testified UAF did not allow Moto to return to school the following year because he was a suspect in S.S.'s murder "just because I was in the building." [Tr. 4690]

The state relied on evidence of the 2019 H&R gun in its opening and closing and numerous witnesses testified extensively regarding it. [Tr. 2177-78, 3029, 3083-84, 3090-91, 4161-65, 4195-4239, 4461-64, 4635-75, 4752-63, 4966-67, 4983-84, 5048-49] The state's opening and closing summations acknowledged the 2019 H&R may not be the murder weapon but nonetheless encouraged the jury to speculate that it was or could be. [Tr. 2177-78, 4967, 5048-49]] The state also encouraged the jury to overvalue the forensic evidence. During Gillis' testimony, this exchange occurred:

> DA: So on cross, you were asked about millions of unrelated firearms in this case. Is that true?
> Gillis: Yes.
> DA: okay. Were millions of firearms seized from Mr. Downs' house?
> Gillis: No.

[Tr. 4236-37] That is, the state encouraged the jury to reach exactly the improper inference Downs had warned against: making the unsupported leap that the gun he owned in 2019 was "somehow, miraculously, the gun he used to kill [S.S.] in 1993." [Tr. 1680] Given the state's reliance on this evidence and the significant risk of unfair prejudice, this error requires reversal of Downs' convictions.

CONCLUSION

Based on the foregoing argument and authority, this court should reverse Downs' convictions and remand for a new trial.

SIGNED on May ___17__, 2024, at Anchorage, Alaska.

ALASKA PUBLIC DEFENDER AGENCY

___/s/ Emily Jura_____
Emily Jura (0906031)
ASSISTANT PUBLIC DEFENDER