STATE OF SOUTH DAKOTA)	IN CIRCUIT COURT
COUNTY OF MINNEHAHA)	SECOND JUDICIAL CIRCUIT

STATE OF SOUTH DAKOTA, Plaintiff, v. THERESA ROSE BENTAAS, Defendant	49CRI19-001657 **BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF SOUTH DAKOTA, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS DNA EXTRACTION, TESTING, AND SEQUENCING**

INTRODUCTION

Our DNA contains our entire genetic makeup, revealing such intensely personal information as whether an individual has rare genetic disorders or whether they are likely to develop breast cancer or sickle cell anemia. When combined with other personal information, DNA can reveal whether a person was adopted, and whether they come from a family with a history of miscarriages or early mortality.

Despite the sensitivity of this information, we cannot avoid leaving behind carbon copies of our entire genetic code wherever we go. In less time than it takes to order a coffee, most humans shed nearly enough skin cells to cover an entire football field.[1] The only way to avoid leaving a trail of our DNA in public spaces would be to never leave home.

Given the revealing nature of DNA and how involuntarily we shed it, the Fourth Amendment imposes a high bar for collecting DNA from a free person and searching it surreptitiously. That bar was not met here. Without a warrant or any judicial oversight, the State

[1] *See* Erin Murphy, *Inside the Cell: The Dark Side of Forensic DNA* 5 (2015).

secretly collected Ms. Bentaas's DNA from items found in her trash and then extracted and sequenced that DNA to try to link her to Baby Doe. Ms. Bentaas was not under arrest or in government custody at the time of the collection and sequencing of her DNA. Rather, she was a free person who possessed the full measure of Fourth Amendment rights.

This case is very different from those relied on by the State in its Opposition, and none of the State's cited cases are controlling. Because Ms. Bentaas was not under arrest when her DNA was first extracted and sequenced, the special-needs exception to the warrant requirement relied on by the U.S. Supreme Court in *Maryland v. King*—where the government had an interest in identifying and processing arrestees—is inapposite. Further, DNA is quite different from physical items thrown out in the trash, so cases like *Greenwood v. California* do not apply. We do not voluntarily discard our DNA when we leave traces of it behind. In fact, the contents of our DNA are never actually visible to the public—sophisticated technology is required to extract genetic information from a sample. Moreover, given the breadth of sensitive information that may be learned about a person just from their DNA, the privacy interest in unavoidably shed DNA is of a different magnitude than the interest in physical items placed in the trash.

Given recent technological advances in DNA analysis and the acute privacy implications of allowing the government to freely access our entire genome, this Court should reject the State's effort to extend older cases to bless the warrantless search at issue here. *See Riley v. California*, 573 U.S. 373, 386 (2014) (rejecting "mechanical application" of older rule to new context involving privacy-invading technology); *Maryland v. King* 569 U.S. 435, 465 (2013) (recognizing that advances in DNA analysis could "present additional privacy concerns," and therefore require greater Fourth Amendment protection). The Fourth Amendment requires a warrant to extract, sequence, and analyze the sensitive DNA we unavoidably leave behind.

ARGUMENT

I. DNA Contains a Person's Most Private and Personal Information, and We Cannot Avoid Shedding it Wherever We Go.

A DNA sample—whether taken directly from a person or extracted from items that person leaves behind—contains a person's entire genetic makeup. This genetic information is deeply private. It can reveal intensely sensitive information about us, including our propensities for certain medical conditions, our ancestry, and our biological familial relationships. Some researchers have also claimed that human behaviors such as aggression and addiction can be explained, at least in part, by genetics.[2] And private companies—including Parabon Nanolabs and GEDmatch, which the State relied on in this case—purport to be able to use our DNA for everything from identifying our eye, hair, and skin colors and the shapes of our faces[3]; to determining whether we are lactose intolerant, prefer sweet or salty foods, and can sleep deeply[4]; to discovering the likely migration patterns of our ancestors and the identities of family members we never even knew we had.[5]

DNA technology and research continue to advance, allowing ever-greater incursions into a person's genetic privacy when a DNA sample is analyzed. One study—conducted when CODIS[6] relied on 13 loci (i.e., locations of genetic markers on a chromosome), rather than the 20

---

[2] Erika Check Hayden, *Ethics: Taboo Genetics*, Nature (Oct. 2, 2013), http://www.nature.com/news/ethics-taboo-genetics-1.13858; Lizzie Buchen, *Biology and Ideology: The Anatomy of Politics*, Nature (Oct. 24, 2012), http://www.nature.com/news/biology-and-ideology-the-anatomy-of-politics-1.11645.

[3] Parabon, *Parabon Snapshot Advanced DNA Analysis*, https://snapshot.parabon-nanolabs.com/; GEDmatch, https://www.gedmatch.com/.

[4] 23andMe, *Compare DNA Tests*, https://www.23andme.com/compare-dna-tests/.

[5] Ancestry, *What to Expect from your AncestryDNA*, https://support.ancestry.com/s/article/What-to-Expect-from-AncestryDNA.

[6] "CODIS is the acronym for the Combined DNA Index System and is the generic term used to describe the FBI's program of support for criminal justice DNA databases as well as the software

loci it now includes—found that the "STR" profiles[7] in CODIS can identify information about individuals' ancestry, which may in turn be used to reveal information about their phenotypic traits (i.e., physical appearance) based on assumptions about race and ethnicity.[8] Another recent study suggested that the profiles maintained in CODIS can now be matched to single-nucleotide polymorphism ("SNP") profiles—incredibly rich genetic profiles that include intimate details like "precise ancestry estimates, health and identification information."[9]

New data aggregation techniques have only increased the amount of sensitive information that can be gleaned from our genetic material. Forensic genetic genealogy—where investigators analyze a person's DNA profile alongside vast genetic databases and public records to create detailed family histories—are just one example. These investigations, including the one in this case, are possible because direct-to-consumer genetic testing services (like Ancestry.com) and genetic genealogy databases (like GEDmatch) have proliferated in recent years. As of early 2019, more than 26 million people had uploaded their DNA to sites like GEDmatch to identify their biological relatives and build sprawling family trees.[10] Although GEDmatch's 1.3 million

---

used to run these databases." FBI, *Frequently Asked Questions on CODIS and NDIS*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet.

[7] An STR profile seeks to identify individuals by looking at how many times so-called "short, tandem, repeat" (i.e., STR) sequences occur at designated locations (i.e., loci) on the genome. *See* Murphy, *Inside the Cell*, *supra*, at 7–8.

[8] Bridget Algee-Hewitt et al., *Individual Identifiability Predicts Population Identifiability in Forensic Microsatellite Markers* 939, Current Biology (2016), https://doi.org/10.1016/j.cub.2016.01.065.

[9] Michael Edge et al., *Linkage Disequilibrium Matches Forensic Genetic Records to Disjoint Genomic Marker Sets*, Proceedings of the National Academy of Sciences (2017), https://www.pnas.org/content/114/22/5671 (finding that the STR profiles maintained in CODIS can be matched to SNP profiles).

[10] Antonio Regalado, *More Than 26 Million People Have Taken an At-Home Ancestry Test*, MIT Tech. Review (Feb. 11, 2019), https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/.

users encompass only about 0.5% of the U.S. adult population, research shows that their data alone could be used to identify 60% of white Americans.[11] When this genetic data is combined with birth, death, marriage, and other public records, the resulting web of familial relationships can expose a host of private information: adoptions, hidden infidelities, a high risk of early mortality, or a family history of certain diseases.

Lastly, the ability of forensic investigators and others to collect DNA from everyday items has also improved dramatically in recent years. Investigators are now able to detect, collect, and analyze even trace amounts of DNA, and labs can isolate and sequence DNA from tiny samples. These capabilities take on particular significance given that people cannot avoid leaving our genetic data behind wherever we go. People constantly shed staggering numbers of skin cells.[12] The average person loses between 40 and 100 hairs per day.[13] And, a single sneeze can spew about 3,000 cell-containing droplets into the world.[14] With every discarded coffee cup, crumpled tissue, plastic straw, cigarette butt, soda can, piece of gum, and drifting flake of dandruff, people unavoidably and involuntarily leave a copy of their genetic blueprint.

II. Extracting an Individual's Genetic Material and Generating a DNA Profile from it Intrudes on Reasonable Expectations of Privacy and Constitutes a Search.

Given the "vast amount of sensitive information . . . [that] can be mined from a person's DNA," courts have recognized that all individuals have "very strong privacy interests" in that

[11] Jocelyn Kaiser, *We Will Find You: DNA Search Used to Nab Golden State Killer Can Home In on About 60% of White Americans*, Science (Oct. 11, 2018), https://www.sciencemag.org/news/2018/10/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white.

[12] *See* Murphy, *Inside the Cell*, *supra*, at 5.

[13] *See* Sheldon Krimsky & Tania Simoncelli, *Genetic Justice: DNA Data Banks, Criminal Investigations, and Civil Liberties* 117 (2012).

[14] *Id.*

information. *United States v. Amerson*, 483 F.3d 73, 85 (2d Cir. 2007); *see also King*, 569 U.S. at 481 (Scalia, J. dissenting) (noting the "vast (and scary) scope" of DNA collection); *State v. Medina*, 102 A.3d 661, 691 (Vt. 2014) (DNA "provide[s] a massive amount of unique, private information about a person that goes beyond identification of that person"); *People v. Buza*, 413 P.3d 1132, 1152 (Cal. 2018) (court was "mindful of the heightened privacy interests in the sensitive information that can be extracted from a person's DNA"). Therefore, the extraction of an individual's DNA sample and "the creation of his DNA profile constitute[] a search for Fourth Amendment purposes." *United States v. Davis*, 690 F.3d 226, 246 (4th Cir. 2012).

In particular, and as discussed in detail above, much like "chemical analysis" of blood and urine samples, DNA samples "can reveal a host of private medical facts about [an individual]." *State v. Lar*, 2018 S.D. 18, ¶ 14, 908 N.W. 2d 181, 186 (citing *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 617 (1989)). "[I]t goes without saying that the most basic violation possible involves . . . the non-consensual retrieval of previously unrevealed medical information that may be unknown even to [the tested individuals]." *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1269 (9th Cir. 1998) (holding that the government's surreptitious testing of biological samples from public employees is a "search[] in violation of Fourth Amendment rights"). As with a person's comprehensive location information, the "familial . . . and sexual associations" that can be revealed through DNA also offer the government "an intimate window into a person's life." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

Relying on *Maryland v. King*, the State ignores the deeply personal and private nature of DNA samples and instead argues that there was no unconstitutional intrusion on privacy here because of the particular type of DNA profile that the government chose to generate from Ms. Bentaas's DNA. State Br. 9. But, in doing so, the State glosses over the fact that it seized and has

access to *all* of Ms. Bentaas's genetic information as a result of the underlying DNA extraction. As the U.S. Supreme Court has made clear in several cases decided after *King*, the Fourth Amendment is concerned with the *entirety* of the private information revealed to police through a search—not just the pieces of information the government ultimately considers useful. Indeed, a search that turns up nothing useful is still a search. *See Lankford v. Gelston*, 364 F.2d 197, 202 (4th Cir. 1966).

For example, in *Birchfield v. North Dakota*, the U.S. Supreme Court evaluated the Fourth Amendment implications of seizing the entirety of a driver's blood sample during blood alcohol testing. The Court recognized that a blood test "places in the hands of law enforcement authorities a sample that can be preserved and from which it is possible to extract information beyond" what the government claims to seek. 136 S. Ct. 2160, 2178 (2016). Thus, even if the law enforcement agency is precluded from testing the blood for any other purpose than to measure alcohol content, the potential of such testing remains and implicates broader privacy interests. *See id.*; *accord Lar*, 2018 S.D. 18, ¶ 14 (quoting *Birchfield*). So, too, with DNA.

Similarly, in *Carpenter v. United States*, the Supreme Court looked to the full scope of the location data the government collected on the defendant (127 days) rather than the small portion of that data (16 location points from a few scattered days) that the government relied on to support its theory of the case at trial. In explaining why Mr. Carpenter had a reasonable expectation of privacy in his location information, the Court focused on the myriad "privacies of life" that could be revealed by the entirety of those 127 days of data, not just the isolated details of interest to investigators. *Carpenter*, 138 S. Ct. at 2212, 2217. And, in *Riley v. California*, the Supreme Court recognized that it is the full breadth and quality of information that exists on a cellphone seized by the government, and therefore available to be examined, that has

constitutional significance. 573 U.S. at 393 (distinguishing cell phones from other objects on an arrestee's person and requiring a warrant to search a phone incident to arrest).

This same principle applies to government collection of DNA. Whenever law enforcement collects an individual's DNA, it gains access to the entirety of that person's genetic blueprint, not just the short tandem repeats that the government uses to confirm identity.

Even if the court were to focus only on the specific type of DNA profile that the State generated from the DNA sample it extracted from Ms. Bentaas's trash, it would still implicate a reasonable expectation of privacy. Although the State argues that the profile is "[l]ike a fingerprint" and that the DNA is used only for identity, not as "evidence of any particular crime," State Br. 9 (quoting *King*, 569 U.S. at 451), actual law enforcement practice belies this claim. In this case, the generated DNA profile was used not to identify who Ms. Bentaas is, but to purportedly determine that she is the biological mother of Baby Doe. *See* State Br. 4.

In addition, since *King* was decided, scientific research has continued to show that the profiles maintained in CODIS can identify far more about individuals than their identity. The availability of these techniques matters for the Fourth Amendment analysis, which requires courts to "take account of more sophisticated systems that are already in use or in development." *Carpenter*, 138 S. Ct. at 2218. As the South Dakota Supreme Court has recognized, before extending older Fourth Amendment precedents to new contexts, courts must consider how technology has developed since those older cases were decided. *See, e.g.*, *State v. Zahn*, 2012 S.D. 19, ¶ 27, 812 N.W.2d 490, 498 (concerning advances in location tracking technology). And even in *King*, the Supreme Court recognized that if subsequent scientific advances in DNA technology allow law enforcement to learn more about a person than just who they are, future

cases "would present additional privacy concerns," *King*, 569 U.S. at 464–65, and "a new Fourth Amendment analysis will be required." *Buza*, 413 P.3d at 1152 (citing *King*).

III. The Warrantless Extraction and Indefinite Retention of Ms. Bentaas's DNA is an Unconstitutional Seizure.

The State's warrantless extraction and sequencing of Ms. Bentaas's DNA from the items it found in her trash interfered with her possessory rights in her DNA and thus constituted an unreasonable seizure prohibited by the Fourth Amendment.[15] "A seizure deprives [an] individual of dominion over his or her person or property." *Horton v. California*, 496 U.S. 128, 133 (1990); *see also United States v. Jacobsen*, 466 U.S. 109, 113 (1984) ("seizure" occurs when there is "some meaningful interference with an individual's possessory interests in that property"). Government interference with an individual's property rights is a seizure, even if the owner's privacy was not violated. *See Soldal v. Cook Cty.*, 506 U.S. 56, 62–64, 68 (1992).

One of the most crucial property rights is the right to exclude others. *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982). This right may be violated even if the owner retains an exact copy of the property seized if it means the owner is unable to control subsequent uses of their once-private information. *See, e.g., United States v. Jefferson*, 571 F. Supp. 2d 696, 703 (E.D. Va. 2008) (copying contents of a person's documents interferes with the person's sole possession of the information contained in those documents); *Caldarola v. Cty. of Westchester*, 343 F.3d 570, 574 (2d Cir. 2003) ("Fourth Amendment seizure has long encompassed the seizure of intangibles [such as a person's image] as well as tangibles."); Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 711 (2010) ("[w]hen the government

[15] As discussed further in Part IV.A below, this is true even if this court finds Ms. Bentaas lacks a privacy or property interest in her trash.

makes an electronic copy of data, it obtains possession of the data that it can preserve for future use"); *see also Davis*, 690 F.3d at 245–46 (recognizing a continuing privacy interest in DNA).

The State's extraction and sequencing of Ms. Bentaas's DNA significantly interferes with her ability to control and exclude others from accessing her private genetic information. Once the State isolates a DNA sample, *all* the data in that sample is in the government's possession and outside the individual's control. This seizure is not momentary; in most cases, the state retains both the DNA sample and the DNA profile indefinitely. DNA profiles are entered into state and federal databases accessible to all manner of law enforcement agencies, making those profiles subject to search again and again in future investigations. And, unlike DNA samples collected upon arrest or conviction, South Dakota state law places no explicit limits on what the State may do with a surreptitiously collected DNA sample,[16] so nothing prevents the state from testing and extracting data from the sample again and using it for other purposes. *See Birchfield*, 136 S. Ct. at 2178.

Because the warrantless extraction and sequencing of Ms. Bentaas's DNA from items found in her trash meaningfully interferes with her right to exclude others from her private genetic data, the government's actions constitute a seizure under the Fourth Amendment.

IV. Police Must Get a Warrant before Extracting and Analyzing Unavoidably Shed DNA.

The Fourth Amendment's central aim is to deny "police officers unbridled discretion to rummage at will among a person's private effects," *Arizona v. Gant*, 556 U.S. 332, 345 (2009), and thus "to secure the privacies of life against arbitrary power," *Carpenter*, 138 S. Ct. at 2214

[16] *See, e.g.*, S.D. Codified Laws § 23-5A-17 (limiting the purposes for which a "DNA sample *collected pursuant to this chapter* shall be used"); *id.* § 23-5A-22 (limiting the State's ability to disclose or share DNA collected "*pursuant to this chapter*"); *id.* § 23-5A-28 (allowing a "person whose DNA record or DNA profile has been included in the State DNA Database *in accordance with this chapter*" to request that their data be expunged). *Cf. King*, 569 U.S. at 465 (highlighting that Maryland arrestee DNA collection statute "provides statutory protections that guard against further invasion of privacy").

(quotation marks and citation omitted). To protect against the "serious and recurring threat to the privacy of countless individuals" posed by unconstrained police incursions into Americans' private affairs, warrantless searches "are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Gant*, 556 U.S. at 338, 345; *accord Zahn*, 2012 S.D. 19, ¶ 29. No exception applies here.

A. The abandonment doctrine does not eliminate an individual's privacy or proprietary interests in their genetic information.

The State argues that because there is no reasonable expectation of privacy in *physical items* in garbage left out for collection, government agents should be free to extract, sequence, and use the *genetic material* that individuals have inadvertently deposited on those items, all without any constraint under the Fourth Amendment. *See* State Br. 8. But DNA is not analogous to curbside trash, and cases finding diminished Fourth Amendment interests in abandoned property simply do not control when it comes to our private genetic information. While it may be permissible for police to seize a *physical* item in the trash without a warrant, extracting and sequencing a DNA sample found on that item without a warrant violates the Fourth Amendment.

The U.S. Supreme Court has held that people have no reasonable expectation of privacy in garbage left out for collection because they have knowingly exposed their trash to any member of the public. *California v. Greenwood*, 486 U.S. 35, 40 (1988). The Court has similarly held that people have no Fourth Amendment privacy or property interest in items they knowingly abandon. *See Abel v. United States*, 362 U.S. 217, 239 (1960) (no warrant required for police to seize items a suspect left behind in a hotel room after checking out); *Hester v. United States*, 265 U.S. 57, 58 (1924) (no Fourth Amendment seizure when police obtain jug containing moonshine whisky after suspect abandoned the jug). The principle from these cases is often referred to as the "abandonment doctrine." But while the abandonment doctrine cases may permit police to

seize and visually examine an item discarded by a suspect, they do not permit police to search the DNA unavoidably deposited on that item without a warrant.

The U.S. Supreme Court has repeatedly cautioned that "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, [courts must seek] to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) (last alteration in original). Courts must therefore avoid "mechanically applying" older doctrines to new types of searches made possible by modern technologies, which can reveal myriad "privacies of life" in ways that are "remarkably easy, cheap, and efficient compared to traditional investigative tools." *Id.* at 2217–19; *see also Riley*, 573 U.S. at 393 ("any extension of [pre-digital] reasoning to digital data has to rest on its own bottom"). That is why the Supreme Court has declined to extend the search-incident-to-arrest exception to permit warrantless searches of cell phones, *Riley*, 573 U.S. at 386; the third-party doctrine to permit warrantless searches of cell phone location information held by a cellular service provider, *Carpenter*, 138 S. Ct. at 2217; and the public-exposure doctrine to permit warrantless surveillance of a home using thermal imaging technology, *Kyllo*, 533 U.S. at 34–36. The South Dakota Supreme Court has similarly recognized that a warrant is required before police can conduct GPS tracking of a person's car, *Zahn*, 2012 S.D. 19, ¶ 31, or long-term video surveillance of a person's home, *State v. Jones*, 2017 S.D. 59, 903 N.W. 2d 101, even though older doctrines allowed more limited surveillance without a warrant.

Likewise here, applying the abandonment doctrine to permit warrantless extraction and sequencing of DNA samples that people unavoidably leave behind as they move through the world would "untether the rule from the justifications underlying" the doctrine. *Riley*, 573 U.S. at

386 (quoting *Gant*, 556 U.S. at 343). The key rationale of the abandonment doctrine is that people voluntarily expose an item to public view by abandoning it. *See Greenwood*, 486 U.S. at 40–41. But unlike physical items, the contents of DNA are never actually visible to the public, and sophisticated technology is required to extract genetic information from a sample. While it may be "common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public," *id.* at 40, it is not common knowledge or even reasonably foreseeable that any member of the public will go through someone's trash, obtain a sample of their DNA, and send that sample to a lab to be sequenced.[17]

Moreover, the protection afforded by the South Dakota Constitution is at least as strong as the Fourth Amendment's protection when it comes to these novel searches, if not even stronger. As the state Supreme Court has made clear, there is no "blanket rule" about whether "the constitutional protection against unreasonable searches and seizures" extends to trash under the South Dakota Constitution. *State v. Schwartz*, 2004 S.D. 123, ¶ 17, 689 N.W.2d 430, 435 (plurality op.); *see also id.* at ¶ 33 (Konenkamp, J., concurring in result). Rather, when it comes to discarded items, courts are to "employ our general two-part test to determine whether an individual has a sufficient privacy interest in the area searched for constitutional protection to apply: '(1) whether the defendant has exhibited an actual subjective expectation of privacy and (2) whether society is willing to honor this expectation as being reasonable.'" *Id.* at ¶ 17. Thus,

[17] It does not matter that a member of the public could theoretically send a DNA sample to a lab for sequencing. As the South Dakota Supreme Court explained in *Zahn*, "[w]e do not believe the popularity of [a particular] technology constitutes a surrender of personal privacy." 2012 S.D. 19, ¶ 28 n.5.

although traditional trash pulls may not require a warrant, courts must engage in a new analysis before extending that the abandonment doctrine to a new context.

Critically, the DNA we unavoidably shed on discarded items is not "voluntarily" shared in any meaningful sense. Application of the abandoned property doctrine hinges on "whether the owner has *voluntarily* discarded, left behind, or otherwise relinquished his interest in the property in question." *State v. Valles*, 2019 N.D. 108, ¶ 7, 925 N.W.2d 404, 408 (emphasis added) (quoting 6 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 11.3(f), at 286–88 (5th ed. 2012 & Supp. 2018)).

As the U.S. Supreme Court recently made clear in *Carpenter*, voluntariness under the Fourth Amendment cannot be assumed. Like the abandonment doctrine, the third-party doctrine applies to information that is "voluntarily conveyed." *United States v. Miller*, 425 U.S. 435, 442 (1976). But as the Court explained in *Carpenter*, the third-party doctrine does not extend to cell phone location information because it "is not truly 'shared' as one normally understands the term." 138 S. Ct. at 2220. That is because cell phones "are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Id.* (quoting *Riley*, 134 S. Ct. at 2484). And once a person carries a cell phone, location information is logged "by dint of its operation, without any affirmative act on the part of the user… Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." *Id.*

Similarly, because we shed DNA constantly, *see supra* Part I, "[t]here is no way to avoid leaving behind a trail" of DNA, and "[a]s a result, in no meaningful sense does the [individual] voluntarily assume the risk of turning over a comprehensive dossier" of genetic information.

Carpenter, 138 S. Ct. at 2220.[18] A person attempting to avoid depositing DNA in their wake would have to relinquish the ability to participate in necessary human activities, to leave their home, and even to touch items that might then end up in their recycling or trash.

Moreover, the privacy interest in unavoidably shed DNA is of a different magnitude than the interest in physical items placed in the trash. As described above, *supra* Part I, DNA reveals one's propensity for medical conditions, from breast cancer to Huntington's disease; biological familial relationships, including unexpected or unknown parentage; and ancestry. As the U.S. and South Dakota Supreme Courts have made clear, analysis of bodily fluids that can reveal "a host of private medical facts about [a person]" implicates strong privacy interests. *Lar*, 2018 S.D. 18, ¶¶ 14, 16, (alteration in original) (quoting *Skinner*, 489 U.S. at 617); *see also Zahn*, 2012 S.D. 19, ¶ 22 (the government intrudes on reasonable expectations of privacy when it conducts technology-aided surveillance that "reveal[s] an intimate picture" of a person's life).

Of course, examining physical items in a person's trash can itself reveal some "intimate details of a person's life." *Schwartz*, 2004 S.D. 123, ¶ 58 (Sabers, J., dissenting). But whatever the privacy interest in the personal details that happen to be discoverable in household trash, the privacy interest in DNA is categorically greater because it reveals "not just one such fact about a person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom United States v. Jones*, 565 U.S. 400 (2012); *see also Lar*, 2018 S.D. 18, ¶ 14 (distinguishing alcohol breath testing from chemical analysis of urine on the basis that breath

[18] The cases from other jurisdictions cited by the State, *see* State Br. 8–9, 10, all predate *Carpenter*, and so are no longer persuasive authority. Moreover, many of them involve situations factually distinct from the instant case, including DNA samples obtained from individuals who, unlike the Defendant here, had been arrested or were otherwise in custody, and therefore who may have been deemed to have diminished expectations of privacy, and DNA taken off of "lawfully seized evidence of a crime," *id.* at 17, rather than off of completely innocuous items like those at issue here.

testing can reveal only blood alcohol content, but urinalysis "can reveal a host of private medical facts about [a person], including whether he or she is epileptic, pregnant, or diabetic"). A warrant is therefore required.

B. The special needs identified in *Maryland v. King* do not apply.

The State's reliance on *Maryland v. King*, 569 U.S. 435, is misplaced. *See* State Br. 9–10. *King* addressed only the diminished privacy interests and heightened government interests in searches designed to identify and process arrestees. That situation is quite unlike the government conduct at issue here.

In narrow circumstances, "special needs, beyond the normal need for law enforcement," can justify warrantless searches under the Fourth Amendment. *Chandler v. Miller*, 520 U.S. 305, 313 (1997). Accordingly, *King* permitted limited use of DNA testing, post-arrest, to serve "the need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody." *King*, 569 U.S. at 449. *King* emphasized that the government's interest in identification is connected to the "routine administrative procedure[s] at a police station house incident to booking and jailing the suspect." *Id.* (quoting *Illinois v. Lafayette*, 462 U.S. 640, 643 (1983) (quotation marks omitted)).

In contrast, the DNA evidence here was obtained as part of the normal law enforcement process of gathering evidence to investigate crime, which is decidedly *not* a "special need" allowing law enforcement to escape the Fourth Amendment's warrant requirement. *Ferguson v. City of Charleston*, 532 U.S. 67, 79 (2001). Despite the State's specious claims to the contrary, *see* State Br. at 18-19 (describing an "unknown sample"), police were surveilling Ms. Bentaas and knew her identity, *see id.* at 3 (noting the trash was taken from Ms. Bentaas's house and had her name on it). The sole purpose of seizing and searching her DNA was to use her genetic

information as evidence to attempt to link her to an unsolved crime. Such investigative activity is precisely the situation where the warrant requirement applies. *See King*, 569 U.S. at 447, 449 (distinguishing the special "need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody" from normal law enforcement investigations, which require a warrant).

In addition, none of the diminished privacy interests in *King* apply here. *King* dealt with the privacy interests of people who have been arrested and charged with a crime. *Id.* at 443, 462 ("The expectations of privacy of an individual taken into police custody 'necessarily [are] of a diminished scope.'" (alteration in original)). In contrast, here, police gathered DNA evidence from a person outside the custody or control of the state, who, as such, possessed the full measure of Fourth Amendment rights.

King also relied heavily on the Court's understanding of the relatively limited DNA analysis involved there, which entailed processing only "13 CODIS loci" for identification purposes, which were understood to "come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee." *Id.* at 464. As noted above, since *King*, however, CODIS testing has expanded to 20 loci, and experts have discovered that these allegedly "non-coding" parts of our DNA actually do provide genetic information beyond just identity. *See, e.g.,* Andrea Roth, *"Spit and Acquit": Prosecutors As Surveillance Entrepreneurs*, 107 Calif. L. Rev. 405, 414 (2019). As the Supreme Court itself recognized in *King*, these technological advances "present additional privacy concerns," *King*, 569 U.S. at 465, and therefore require a different Fourth Amendment analysis.

CONCLUSION

For the foregoing reasons, *amici* respectfully urge the Court to hold that extraction and sequencing of a person's unavoidably shed DNA is a search and seizure under the Fourth Amendment, for which a warrant is required.

Respectfully Submitted,

Dated: March 9, 2020

By: /s/ Stephen Pevar

Stephen Pevar (SD Bar #1364)
American Civil Liberties Union Foundation
765 Asylum Avenue
Hartford, CT 06105
Tel.: 860-570-9830
pevaraclu@aol.com; spevar@aclu.org
Counsel for Amici Curiae

On the Brief:

Vera Eidelman
Alexia Ramirez
Nathan Freed Wessler
Patrick Toomey
Jason D. Williamson
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
veidelman@aclu.org
aramirez@aclu.org
nwessler@aclu.org
ptoomey@aclu.org
jwilliamson@aclu.org

Kimberly Craven
Andrew Malone*
American Civil Liberties Union
of South Dakota
P.O. Box 1170
Sioux Falls, SD 57101
(201) 284-9500
kcraven@aclu.org
amalone@aclu.org

Jennifer Lynch
Andrew Crocker
Jamie Lee Williams
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
jlynch@eff.org
andrew@eff.org
jamie@eff.org

* *Not yet admitted. Application for admission to the South Dakota bar pending.*

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 9th day of March, 2020, the foregoing amicus brief was served upon counsel for the parties via email.

/s/ Stephen Pevar
Stephen Pevar