THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XVII STLR.ORG FALL 2015

ARTICLE

CODE 9: DIGITAL DATA AS A FOURTH-AMENDMENT ANALOGUE FOR "ABANDONED" DNA†

Carrie Leonetti*

* Carrie Leonetti is an Associate Professor, the Faculty Leader of the Criminal Justice Initiative at the University of Oregon School of Law in Portland and a former member of the American Bar Association DNA Task Force. She wishes to thank Zachary Smallwood for his usual brilliant research assistance

I. INTRODUCTION: IF YOU HAVE NOTHING TO HIDE, YOU HAVE NOTHING TO FEAR

> "If you've ever handled a penny, the government's got your DNA. Why do you think they keep them in circulation?"[1]

The collection of forensic DNA evidence and its use for both the inculpation and exoneration of criminal defendants has exploded over the past two decades, but courts' regulation of law enforcement's collection and use of DNA samples has been vague and disuniform. Is the unregulated collection and analysis of biological evidence permissible under the Fourth Amendment[2]?

We all involuntarily leave traces of biological evidence nearly everywhere that we go, whether its skin cells in a fingerprint, saliva on a discarded coffee cup or cigarette butt, mucous or tears on a tissue, hair in a brush or on an article of clothing, skin cells on a toothbrush, sweat during a handshake. Any of this evidence, when analyzed, can reveal our entire genetic code as well as information about our blood relatives. By leaving so much biological evidence behind, do we voluntarily give the Government wide-open access to all of the genetic information that such evidence contains? Should we be deemed to have done so?

It has become increasingly common for police officers to surreptitiously follow a suspect in order to obtain discarded biological evidence.[3] The police may then analyze this evidence

---

1. *The Simpsons: Who Shot Mr. Burns?: Part 2* (Fox Broadcasting Company television broadcast Sept. 17, 1995).

2. The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

3. This surreptitious collection of biological evidence generally occurs in two scenarios: either the police have a hunch about a suspect's involvement in a crime that does not rise to the level of probable cause to obtain a court order for a DNA sample or the police have probable cause but do not wish to obtain a court order (because of the time and effort involved or because they do not wish to alert the suspect to their suspicions). *See* Christopher Francescani, *Sex Fiend Admits He Killed 5 in Brooklyn*, N.Y. POST, Mar. 10, 2001, at 11; Tony Gordon, *DNA Sample Links Man to Burglary,* CHI. DAILY HERALD, July 3, 2001, at 5; William K. Rashbaum, *Man Cleared by DNA Tests Led Police to Murder Suspect*, N.Y. TIMES, Aug. 6, 2000, at A25; Richard Willing, *As Police Rely More on DNA, States Take a Closer Look*, USA TODAY, June 6, 2000, at A1; *see, e.g.*, People v. Gallego, 117 Cal. Rptr. 3d 907, 910–14 (Ct. App. 2010); Commonwealth v. Bly, 473862 N.E.2d 341, 356–57 (Mass. 2007); State v.

for DNA, which in turn can be used to establish a suspect's guilt. If the police wanted to search a suspect's house or car for inculpatory evidence, the Fourth Amendment would require them to have probable cause and obtain a warrant before searching.[4] But surreptitious DNA collection, by contrast, is largely unconstrained by Fourth Amendment or other concerns. This is because courts have held that DNA collection is not an invasion of privacy because, like discarded trash or fingerprint pattern impressions, DNA evidence has been voluntarily "abandoned."[5]

The goal of this Article is reformist. It proposes that the collection and analysis of forensic DNA evidence from discarded biological samples should constitute a search for Fourth Amendment purposes and therefore require a search warrant issued on probable cause.

Existing literature regarding surreptitious DNA collection focuses on "genetic exceptionalism." Proponents of genetic exceptionalism argue that it is inappropriate to compare fingerprint impressions on an abandoned coffee cup, which only reveal identity, to saliva or skin cells, which contain a person's entire genetic code.[6] The Supreme Court largely rejected this argument

---

Buckman, 613 N.W.2d 463, 474 (Neb. 2000); State v. Wickline, 440 N.W.2d 249, 253 (Neb. 1989); State v. Reed, 641 S.E.2d 320, 321 (N.C. Ct. App. 2007).

4. *See* United States v. Place, 462 U.S. 696, 701 (1983); *cf.* Terry v. Ohio, 392 U.S. 1, 20 (1968); Welsh v. Wisconsin, 466 U.S. 740, 748–49 (1984).

5. *See, e.g.*, Rise v. Oregon, 59 F.3d 1556, 1559 (9th Cir. 1995) ("The information derived from [DNA] is substantially the same as that derived from fingerprinting – an identifying marker unique to the individual from whom the information is derived."); *Gallego*, 117 Cal. Rptr. 3d 907 at 912 (The "cigarette butt, like the trash bags in *Greenwood*, was left in a place 'particularly suited for public inspection.' Defendant thus abandoned the cigarette butt in a public place, and therefore had no reasonable expectation of privacy concerning the DNA testing of it to identify him as a suspect." (internal citation omitted)); State v. Athan, 158 P.3d 27, 37 (Wash. 2007) ("Police may surreptitiously follow a suspect to collect DNA, fingerprints, footprints, or other possibly incriminating evidence, without violating that suspect's privacy."); *see also* NAT'L COMM'N ON THE FUTURE OF DNA EVIDENCE, U.S. DEP'T OF JUSTICE, USING DNA TO SOLVE COLD CASES 5 (2002) (comparing DNA evidence to fingerprint evidence).

6. *See, e.g.*, George J. Annas, *Privacy Rules for DNA Databanks Protecting Coded "Future Diaries"*, 270 J. AM. MED. ASS'N 2346 (1993); George M. Dery, III, *Opening One's Mouth for "Royal Inspection": the Supreme Court Allows Collection of DNA from Felony Arrestees in* Maryland v. King, 2 VA. J. CRIM. L. 116, 146–48 (2014) (arguing that DNA collection is a significant invasion of privacy); David H. Kaye, *A Fourth Amendment Theory for Arrestee DNA and Other Biometric Databases*, 15 U. PA. J. CONST. L. 1095 (2013) (describing a "biometric exception" to the warrant requirement); David H. Kaye, *DNA Sampling on Arrest and the Fourth Amendment*, 2 GOVT. L. & POL. 38–41 (2000) (arguing that compelling individuals to surrender DNA samples should

in *Maryland v. King*.[7] Others attack the assumption that discarded DNA evidence has been voluntarily abandoned—that is, the assumption that one who abandons a cigarette butt is intentionally and voluntarily abandoning the DNA profile that it contains, or at least knowingly failing to adequately to protect his or her privacy.

---

be deemed a search within the meaning of the Fourth Amendment); David H. Kaye, *Who Needs Special Needs? On the Constitutionality of Collecting DNA and Other Biometric Evidence Data from Arrestees*, J. L. MED. & ETHICS, 188, 192–93 (2006) (proposing a "biometric identification exception" to the special-needs doctrine); Tracey Maclin, *Is Obtaining an Arrestee's DNA a Valid Special Needs Search Under the Fourth Amendment? What Should (And Will) the Supreme Court Do??*, 33 J. L. MED. & ETHICS 102, 106–07 (2005) 165, 169–170 (2006) (proposing DNA sampling constitutes a search based on the extent to which DNA is exposed to the public, the extent of bodily intrusion, and the nature of the information extracted from DNA); Laura A. Matejik, *DNA Sampling: Privacy and Police Investigation in a Suspect Society*, 61 ARK. L. REV. 53, 81 (2008) (arguing that the Fourth Amendment should recognize a reasonable expectation of privacy regarding the information contained in DNA); Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-first Century Technologies*, 53 HASTINGS L. J. 1303, 1306 (2002) (arguing that "reasonable expectations" of privacy should be focused only on the result of the search, i.e., the type of information obtained); *see also* Paul R. Billings, *DNA Data Banks Would Taint Justice*, BOSTON GLOBE, Jan. 14, 1999, at A19 (disapproving of requirements for criminal offenders to submit DNA to state data banks because such data banks would "allow the government to violate privacy rights based on membership in a suspect class"); Editorial, *DNA Testing Proposals*, N.Y. TIMES, Dec. 17, 1998, at A32; *cf.* Patterson v. State, 742 N.E.2d 4, 10 n.3 (Ind. Ct. App. 2000) (noting privacy concerns associated with coding loci on the human genome).

7. Maryland v. King, 133 S. Ct. 1958 (2013) (upholding the constitutionality of warrantless DNA collection upon arrest for violent felonies, resulting in a "cold hit" inculpating the arrestee in an unrelated crime). King was arrested and charged with felony assault arising out of the allegation that he had menaced a group of people with a shotgun. *Id.* at 1965. After he was arrested, pursuant to Maryland's DNA collection statute, officers collected a sample of King's DNA from his mouth using a buccal swab. *See id.* at 1967–68. The police had neither a warrant nor a particularized suspicion that collecting and analyzing King's DNA would result in a "cold hit" in another unsolved case, but when King's profile was entered into Maryland's DNA database, it "matched" the profile of DNA collected at an earlier rape crime scene. *Id.* at 1965–66. On that basis, the State charged King with rape. *Id.* King argued that the warrantless and suspicionless collection of his DNA was an illegal search and seizure under the Fourth Amendment. *Id.* In rejecting his claim, the Supreme Court asserted: "A DNA profile is useful to the police because it gives them a form of identification to search the records already in their valid possession. In this respect the use of DNA for identification is no different than matching an arrestee's face to a wanted poster . . . or matching tattoos to known gang symbols . . . or matching the arrestee's fingerprints to those recovered from a crime scene." *Id.* at 1971–72.

They argue that the DNA should be treated as separate from the cigarette that contains it and that courts should recognize the existence of a reasonable expectation of privacy in the DNA itself.[8] The existing literature does not, however, propose a better analogy for discarded DNA than discarded refuse. This is because even if an individual does or should have a privacy interest in his or her genetic material that is separate from the privacy interest, or lack thereof, in the object from which it is taken (cigarette, coffee cup, etc.), it does not necessarily follow that such an interest is independently cognizable under the Fourth Amendment.

This Article does not argue that genetic material is exceptional and therefore independently cognizable under the Fourth Amendment. Instead, it first goes beyond the distinction between biological evidence and the object on which it is left, and then draws a further distinction between the collection of biological evidence and the forensic analysis of the DNA profile that it contains. It asserts that biological evidence is a "container" and that DNA is the "content." It then argues that the genetic material contained in biological evidence is analogous to text messages and other digital data contained in portable electronic devices. The courts generally grant Fourth Amendment protection to digital data (content) contained in portable electronic devices (containers) because they acknowledge that the owner of a container has a protected privacy interest in the contents of the container, even if he or she does not have a protected privacy interest in the container itself. The court should grant the same Fourth Amendment protection to the DNA contained in biological material. The principles that guide the resolution of cases involving "abandoned" DNA should be nested in the larger set of constitutional principles that guide the resolution of cases involving society's competing interests in privacy, technological

---

8. *See, e.g.*, Edward J. Imwinkelried & David H. Kaye, *DNA Typing: Emerging or Neglecting Issues*, 76 WASH. L. REV. 413, 437 (2001) (asserting that depositing DNA in the ordinary course of life "differs from placing private papers in a container on the street to be collected as garbage"); Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: the Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 870–71 (2006) (distinguishing fingerprints, which have a limited identification value, from DNA, which reveals "deeply personal information"); *cf.* People v. Perlos, 462 N.W.2d 310, 324 (Mich. 1990) (Levin, J., dissenting) (arguing that a driver for who has consented to a blood-alcohol-concentration ("BAC") test has not implicitly consented to a search of his private medical records, because seeking medical testing is not a voluntary relinquishment of the expectation of privacy regarding the records that the test creates).

advancement, and enforcement of the laws. The doctrine governing the analysis of DNA contained in shed biological material fits within the doctrine governing the search of digital data on seized computer devices, which fits within a larger doctrine governing the separation of seizures of containers from searches of their contents.

This Article does not address the sometimes conflated but doctrinally distinct issue of "DNA dragnets," large-scale DNA collection conducted prior to and for the purpose of locating a suspect,[9] because dragnet DNA collection involves the doctrine of consent, rather than abandonment, and that consent typically covers not only the collection of a biological-evidence sample (buccal cells or blood), but also the subsequent analysis of its genetic contents for forensic identification.[10] This Article also does not explicitly address the collection of biological evidence of unknown origin—DNA left at a crime scene, for example—but rather the covert and involuntary sampling of the biological material of an individual whom the police suspect of a crime, although some of its analysis might apply equally in these situations, because, typically, crime scene investigators either have a warrant to enter the premises and seize evidence (based on the probable cause arising from the crime having occurred there) or courts treat evidence gathered from a crime scene under doctrinal exceptions to the warrant requirement like plain view, exigent circumstances, and/or the inventory-search doctrine, rather than an abandonment rationale—i.e., courts do not find that, by leaving evidence at a crime scene, a suspect has relinquished a reasonable expectation of privacy in it, but rather they tend to find that there is something unique in the circumstances or location of the crime scene from which it is gathered for Fourth Amendment purposes.[11]

---

9. *See generally* Carrie Leonetti, *Motive & Suspicion:* Florida v. Jardines *and the Constitutional Right to Protection from Suspicionless Dragnet Investigations*, OHIO ST. J. CRIM. L. (forthcoming Fall 2016).

10. *See generally* Florida v. Jimeno, 500 U.S. 248, 251–52 (1991) (finding that once the defendant gave police consent to search his car, it was reasonable that the police would also search a container within the car); Schneckcloth v. Bustamonte, 412 U.S. 218, 222 (1973) (holding that consent must be voluntarily given). In other words, when conducting DNA dragnets, the police not only ask members of a community to provide a sample of their biological evidence, they also inform them that the purpose of the collection of the samples is to perform DNA analysis. For this reason, in a dragnet context, the suspect's interest in the collection of the sample and its subsequent DNA analysis are the same, and the consent is either valid for both or for neither.

11. *See, e.g.*, Michigan v. Tyler, 436 U.S. 499 (1978) (permitting firefighters to remain in a residence without a warrant after putting out a fire "for a

reasonable time to investigate the cause of the blaze," because immediate investigation might be "necessary to preserve evidence from intentional or accidental destruction"); Phillips v. State, 625 P.2d 816 (Alaska 1980) (inferring consent to search a crime scene from the initial consent to enter the home); Alford v. State, 724 S.W.2d 151 (Ark. 1987) (implying Alford's consent to search his home when he called the police to report his girlfriend's "suicide" and cooperated with their search of the premises); People v. Roark, 643 P.2d 756 (Colo. 1982) (inferring consent to enter a residence from an unidentified call to the police reporting a crime scene at the residence); Zeigler v. State, 402 So.2d 365 (Fla. 1981) (inferring consent to search a store where a murder occurred from Zeigler's invitation to the police to enter); Overman v. State, 299 S.E.2d 542 (Ga. 1983) (upholding the warrantless entry into Overman's apartment and seizure of evidence in plain view when he called the police after shooting a woman in the apartment); State v. Brady, 585 So.2d 524 (La. 1991) (upholding the warrantless search of a closet in Brady's apartment after she asked a neighbor to call the police and the responding officers observed blood on the closet door near the body of the decedent); Commonwealth v. Beldotti, 567 N.E.2d 1219 (Mass. 1991) (inferring Beldotti's consent to a search of the scene of a homicide in his home when he called the police, told them where the body was located, and cooperated with the search); State v. Fredette, 411 A.2d 65 (Me. 1979) (inferring consent to enter and search Fredette's residence when she called the police, reported that her husband had been shot by an intruder, and did not object to an extensive search of the residence when the police responded); State v. Butler, 676 S.W.2d 809, 815 (Mo. 1984) ("The opening of the house to police after calling them leads to the logical conclusion that Mr. Butler was giving permission for a general search in connection with the detection and apprehension of his assailant."); Johnson v. State, 226 S.W.3d 439, 441 (Tex. Crim. App. 2007) ("By calling 911 and asking the police to come to her home, appellant consented to the police entry and to their initial investigation of the death of her husband."); State v. Tapio, 459 N.W.2d 406, 414 (S.D. 1991) (inferring consent to search a crime scene from a 911 call for assistance, which identified the location of a homicide underway); State v. Flippo, 575 S.E.2d 170, 183 (W. Va. 2002) ("[W]hen a person summons the police to a dwelling he/she owns, possesses, or controls, and that person states that a crime was committed against him/her or others by a third person at the premises, he/she implicitly consents to a search of the premises reasonably related to the routine investigation of the offense and the identification of the perpetrator, absent a contrary limitation imposed by the person summoning the police."); Shaffer v. State, 640 P.2d 88, 95–96 (Wyo. 1982) (permitting a coroner without a warrant to enter a mobile home in which a fire had killed several children and investigate the cause of death after the fire had been extinguished). *But see* Flippo v. West Va., 528 U.S. 11, 14–15 (1999) (holding that there is no per se "murder scene exception" to the Warrant Clause of the Fourth Amendment permitting a warrantless search of every item at the crime scene after it has been secured); Mincey v. Arizona, 437 U.S. 385, 395 (1985) (rejecting the contention that there was a "murder scene exception" to the Warrant Clause of the Fourth Amendment); Alward v. State, 912 P.2d 243, 250–51 (Nev. 1996) (finding that warrantless searches of a residential crime scene were unconstitutional because they occurred after the exigency that permitted the initial entry had dissipated); State v. Hockenhull, 525 A.2d 926, 932 (R.I. 1987) (holding that the warrantless search, photographing, and diagramming of

Section II of this Article describes the courts' current approach to surreptitiously obtained DNA; most courts have held that DNA evidence has been "abandoned," as garbage set out for collection on the curb was held "abandoned," in *Greenwood v. California*.[12] Section III describes the Supreme Court's more recent jurisprudence governing the warrantless collection of data from mobile digital devices. Section IV argues that DNA is not exceptional, but rather that the distinction between surreptitiously collecting biological evidence and testing that evidence for DNA fits well within the courts' existing legally significant distinction between seizing containers and searching their contents. Section V argues that the search of digital data on mobile devices, and the larger container-contents jurisprudence, is a better analogy for the DNA analysis of shed biological evidence than the placing of a garbage can at the curb. It provides ample support for the proposition that individuals have a reasonable expectation of privacy in the "contents" of their biological samples that is independent of the expectation of privacy they may have in the "container." Section V also calls for increasing legislative protection for genetic privacy. Section VI concludes that the abandonment doctrine established in *Greenwood v. California* should not apply to genetic material because the collection of "abandoned" DNA, like the collection of personal digital information from a mobile electronic device, involves something more than the collection of Greenwood's discarded garbage from the curb.

II. GARBAGE IN, GARBAGE OUT: CURRENT REGULATION (OR LACK THEREOF) OF "ABANDONED" DNA

At present, neither the rules of criminal procedure nor the Fourth Amendment provides much protection from forensic DNA analysis of biological evidence, even when that evidence was surreptitiously collected without a warrant or probable cause. Fourth Amendment protection is only triggered when an unreasonable (i.e., warrantless) "search" or "seizure" has occurred.

As Justice Harlan articulated in his concurring opinion in *Katz v. United States*, a police investigative technique constitutes a "search" only if the subject of the technique had both a subjective and an objective expectation of privacy in the area or activity

---

Hockenhull's residence after the decedent had been removed from the premises was unconstitutional because the exigency that permitted the original entry had dissipated).

12. California v. Greenwood, 486 U.S. 35, 37 (1988).

invaded. A subjective expectation of privacy is objectively reasonable if "society is prepared to recognize" that the person's expectation was "reasonable."[13] If a court determines that a person lacks either a subjective or an objective expectation of privacy, no search has occurred for Fourth Amendment purposes.

Police collection of physical evidence constitutes a "seizure" under the Fourth Amendment only if it involves a "meaningful interference with an individual's possessory interests in [the] property [collected]."[14] The acquisition, by force, of biological material like blood or urine constitutes a seizure because it is a meaningful interference with a suspect's bodily integrity.[15] By contrast, if a suspect "abandons" an item in a public place (or other place to which the police have legal access), he or she relinquishes any reasonable expectation of privacy in the item.[16]

---

13. *See* Carrie Leonetti, *Bigfoot: Data Mining, the Digital Footprint, and the Fourth Amendment*, 15 J. HIGH TECH. L. 260, 271–73 (2015) [hereinafter Leonetti, *Data Mining*]; *see*, *e.g.*, Smith v. Maryland, 442 U.S. 735 (1979). Courts examine four factors to determine whether an intrusion is reasonable under the Fourth Amendment: (1) the individual's interest, (2) the Government's interest, (3) the necessity for the intrusion, and (4) the procedure used in conducting the search. *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602 (1989); Nat'l Treasury Emp. v. Von Raab, 489 U.S. 656 (1989); Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 664–65 (1995) (authorizing random drug testing of public-school students voluntarily participating in school athletics programs; the decision was motivated by considerable evidence of a serious drug problem in the school district).

14. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

15. *See* Schmerber v. California, 384 U.S. 757, 770 (1966); Acton, 515 U.S. 646; *see also Skinner*, 489 U.S. 602.

16. *See* California v. Hodari D., 499 U.S. 621, 628–29 (1991) (concluding that Hodari had relinquished any reasonable expectation of privacy regarding a rock of cocaine that he tossed away while fleeing a police officer because he had "abandoned" it, and therefore lost the right to challenge any subsequent chemical testing of the rock); *see, e.g.*, United States v. Eubanks, 876 F.2d 1514, 1516 (11th Cir. 1989) (holding that Eubanks lacked a reasonable expectation of privacy regarding a piece of paper containing his fingerprints and trace amounts of cocaine, because he "abandoned" the paper by dropping it on the ground); *see also* Texas v. Brown, 460 U.S. 730, 748 (1983) (Stevens, J., concurring) ("[I]f an item has been abandoned, no Fourth Amendment interest is implicated, and neither probable cause nor a warrant is necessary to justify seizure."); *see, e.g.*, United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that when Miller voluntarily relinquished checks and deposit slips that he had prepared to a bank, he relinquished any "protected Fourth Amendment interest" in them, so that the Government did not need a warrant issued on probable cause in order to obtain them from the bank); *see generally* Leonetti, *Data Mining*, *supra* note 13, at 274–75 and citations contained therein. *But see* State v. Bonnell, 856 P.2d 1265, 1275 (Haw. 1993) (holding that Bonnell had a reasonable expectation of privacy, which included freedom from warrantless covert video surveillance, while on

Even assuming that the abandonment doctrine can properly be applied to the seizure of biological evidence—that is, that the police may seize shed skin cells or hair without a warrant—there should be a separate stage of analysis regarding whether they may perform a forensic DNA analysis of the genetic information that they contain. Instead, however, courts have, without much critical reflection, extended the abandonment doctrine to apply to the genetic information obtained from forensic laboratory analysis of the biological evidence.[17] This extension is problematic.

When justifying the use of forensic DNA from surreptitiously collected biological evidence, courts most commonly cite *Greenwood v. California*. In *Greenwood*, a plaintiff left his trash bags on the curb for city collection. Local police performed a warrantless search of the trash bags after they had been removed by garbage collectors and seized incriminating evidence of narcotics trafficking. The Court held that the warrantless search was permissible, reasoning that the defendant Greenwood had no reasonable expectation in either the trash bags or their contents because he had left them in a place "particularly suited for public inspection," and anyone could have delved through his abandoned trash:

> It is 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. . . . Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to

---

break in the "break room" of the post office where he worked and noting that "[e]very individual has expectations of privacy with regard to his person wherever he may go, be it a public park or a private place").

17. *See, e.g.*, Commonwealth v. Bly, 862 N.E.2d 341, 356–57 (Mass. 2007) (holding that Bly had abandoned his DNA, which police obtained from a water bottle and cigarette butts that Bly left in an interview room); State v. Buckman, 613 N.W.2d 463, 474 (Neb. 2000) (upholding the trial court's denial of Buckman's motion to suppress the results of DNA testing of two cigarettes that he smoked and left behind at the police station after his arrest because he had abandoned the cigarettes); People v. Brown, 828 N.Y.S.2d 550, 551 (App. Div. 2007) (affirming the trial court's denial of Brown's motion to suppress DNA results obtained from a bandage soaked in his blood because he had abandoned it to emergency medical personnel when they exchanged it for a clean one); People v. LaGuerre, 815 N.Y.S.2d 211, 213 (App. Div. 2006) (holding that LaGuerre abandoned his DNA sample extracted from chewed gum when he gave it to undercover police officers pretending to conduct a soda taste test, in which he voluntarily participated, for the purpose of surreptitiously obtaining his DNA.).

> a third party, the trash collector, who might himself have sorted through respondent's trash or permitted others, such as the police, to do so.[18]

Regardless of whether or not Greenwood had a subjective expectation in the privacy of his "abandoned" garbage, that expectation was not objectively reasonable, so a warrantless search of the garbage was permissible under the Fourth Amendment.

In resolving cases involving abandoned biological evidence, the courts have largely followed *Greenwood*'s analysis and concluded that suspects have no objectively reasonable expectation of privacy regarding their shed biological material, such as saliva left behind on a coffee cup, soda can, or cigarette butt (or, increasingly, a fingerprint containing skin cells).[19] Under the current doctrine, the courts focus their inquiry on the means by which the police gained access to the object or biological substance containing genetic information, which is usually of no concern to the person who abandoned it.[20] If the biological substance is "knowingly exposed" to the public, so is the genetic information that it contains. The courts rarely question police collection of the genetic information itself—information that the person may well wish to keep private.[21] As a result, no court has held that the warrantless collection and analysis of shed DNA collected from items left in public places is impermissible under the Fourth Amendment. Once the biological evidence itself is deemed

---

18. California v. Greenwood, 486 U.S. 35, 40. (1988).

19. *See*, *e.g.*, People v. Thomas, 200 Cal. App. 4th 338 (Cal. 2d. Dist. 2011); Williamson v. State, 413 Md. 521 (Md. 2010); State v. Athan, 158 P.3d 27 (Wash. 2007).

20. When courts determine what "society is prepared to recognize as reasonable," the existence of a legally cognizable property interest is one factor that they consider (e.g., whether a trespass has occurred). *See* Oliver v. United States, 466 U.S. 170, 183 (1984) ("The existence of a property right is but one element in determining whether expectations of privacy are legitimate."); *see also* Rakas v. Illinois, 439 U.S. 128, 143–44 n.12 (1978) (noting, however, that "a property interest in premises may not be sufficient to establish a legitimate expectation of privacy with respect to particular items located on the premises or activity conducted thereon."). This is why "abandonment" typically defeats the reasonableness of an expectation of privacy, even post-*Katz*: a person no longer has a property interest in that which he or she has abandoned.

21. Some state courts have rejected the Supreme Court's reasoning in *Greenwood* on similar grounds. For example, in *State v. Hempele*, 576 A.2d 793, 798–99 (N.J. 1990), the New Jersey Supreme Court, in declining to follow *Greenwood* in interpreting its state constitution, reasoned that, because people retain subjective privacy interests in their garbage even after placing it out for collection, the court's "abandonment" analysis was inapposite.

abandoned or knowingly exposed, the courts do not separately analyze the expectation of privacy in its contents (the genetic profile that it contains).

Prior to the advent of modern forensic DNA analysis, the genetic privacy and anonymity that people enjoyed was not the result of legal or constitutional protections, but rather technological unavailability. Today, by contrast, forensic DNA analysis can be performed relatively quickly and inexpensively on increasingly smaller biological samples. The police can therefore amass an enormous amount of personal genetic information from items inadvertently left in public places.[22] Courts should recognize the independent significance of the genetic information contained inside discarded biological substances, rather than declaring that such information is akin to garbage abandoned at the curb and granting the government unfettered license to search and seize the information without a warrant.

III. THE INFORMATION SUPERHIGHWAY: REGULATION OF THE WARRANTLESS COLLECTION OF DIGITAL DATA

Mobile digital devices are becoming smaller, more powerful, and more capable of containing intimate details of their users' personal lives. These technologies have become so ubiquitous that the Supreme Court recently noted that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[23] In *Riley v. California*, the Supreme Court recognized that a separate justification, usually a warrant issued on probable cause,[24] is necessary to search data contained on a cellular telephone, beyond the justification already present for seizure of the phone itself.[25] The Court acknowledged its preference, forcefully expressed in *United States v. Robinson*,[26] for categorical rules governing searches incident to arrest (as opposed to a case-

22. *Cf.* Leonetti, *Data Mining*, *supra* note 13, at 295–98 (describing the way that technological advances have allowed police to surveil "everyone" instead of just "anyone").

23. Riley v. California, 134 S. Ct. 2473, 2484 (2014).

24. *See id.* at 2482; *see also* Kentucky v. King, 131 S. Ct. 1849, 1856–57 (2011); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653. (1995).

25. While *Riley* dealt with a search of a mobile device incident to arrest, rather than an "abandoned" mobile device, its bimodal analysis (separating the seizure of the mobile device from the search of its digital contents) nonetheless sheds light on the distinction that this Article proposes between an abandoned sample of biological evidence (e.g., a skin cell) and a subsequent analysis of its genetic contents. *See infra* Section V.

26. 414 U.S. 218 (1973).

by-case determination of whether officer safety or evidence destruction were at issue),[27] but characterized its holding as refusing to apply *Robinson*'s categorical rule categorically— i.e., to a "particular category of effects."[28]

Courts apply similar rules to the search and seizure of text messages outside of the search-incident-to-arrest context. As a general rule, in order to obtain a warrant to search or seize text messages, the police must have probable cause to believe that the possessor of the phone has used and will use the text-messaging feature to facilitate the predicate crimes, separate and apart from whatever justification they have to seize the device in the first instance. Such probable cause must be separate and apart from whatever justification that they have to seize the device in the first instance: individualized probable cause to engage in seizure and analysis of the contents of the text messages.[29]

This Article proposes an analogous relationship between biological evidence, as a container, and genetic information, as its contents, by suggesting that even when the police have legally seized the biological evidence without a warrant or probable cause, the further analysis of the genetic code inside should be treated as a separate Fourth Amendment moment.

IV. JUNK IN THE TRUNK: THE CONSTITUTIONAL DIFFERENCE BETWEEN CONTAINERS AND THEIR CONTENTS

A. Old School Containers: Luggage and the Like

One way to understand the Court's requirement that the police have a warrant based on probable cause to search the digital

27. *See id.* at 235 ("[O]ur more fundamental disagreement . . . arises from [the] suggestion that there must be litigated in each case the issue of whether or not there was present one of the reasons supporting the authority for a search of the person incident to a lawful arrest. We do not think the long line of authorities of this Court . . . or what we can glean from the history of practice in this country and in England, requires such a case-by-case adjudication. A police officer's determination as to how and where to search the person of a suspect whom he has arrested is necessarily a quick ad hoc judgment which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search.").

28. *Riley*, 134 S. Ct. at 2485.

29. *See* 18 U.S.C. §§ 3121–3123 (2012). *But see* City of Ontario v. Quon, 560 U.S. 746, 760–65 (2010) (holding that a city police department's warrantless review of an officer's text messages was reasonable and did not violate the Fourth Amendment because the department owned the electronic device on which the text messages were stored and the search was conducted for the purpose of reviewing the city's contract with its wireless service provider).

contents of a cell phone already legally seized is as a recognition of some kind of digital communications exceptionalism—i.e., that digital data is fundamentally different and more private than other, non-digital possessions. Another way to understand it, however, is precisely the opposite: as an extension of an older and broader jurisprudence recognizing an important distinction between containers and their contents.[30] In *Bond v. United States*,[31] the Court held that a border-patrol agent had violated Bond's reasonable expectation of privacy when the agent squeezed his soft luggage that was placed in the overhead storage area of a bus, even though the storage area itself was public and the bag was in plain view. The Government argued that a passenger had no reasonable expectation of privacy in luggage sitting exposed to public view. Rejecting that argument, the Court distinguished plain view of the outside of the bag from groping the contents inside, reasoning: "Physically invasive inspection is simply more intrusive than purely visual inspection."[32] In reaching its holding, the Court distinguished between the passenger's interest in the bag itself (i.e., the luggage as a container) and its contents, and applied a two-step analysis to the two interests:

> When a passenger places a bag in an overhead bin, he expects that other passengers or bus employees may move it for one reason or another. Thus, a bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner. But this is exactly what the agent did here. We therefore hold that the agent's physical manipulation of petitioner's bag violated the Fourth Amendment.[33]

The Court has drawn a similar line between containers and their contents in the context of searches incident to arrest. In *United States v. Chadwick*,[34] the Court limited the scope of the

30. *See, e.g.*, Robbins v. California, 453 U.S. 420, 428 (1981) (holding that a lawful vehicle search did not extend to a search a closed piece of luggage inside); Arkansas v. Sanders, 442 U.S. 753, 763–64 (1979) (same); United States v. Block, 590 F.2d 535, 541–42 (4th Cir. 1978) (holding that valid consent to search a room did not encompass the search of a footlocker contained in a room because they were two separate searches).

31. 529 U.S. 334, 338–39 (2000).

32. *Id.* at 337.

33. *Id.* at 338–39.

34. 433 U.S. 1, 15 (1977).

Chimel[35] and *Robinson*[36] doctrine to "personal property . . . immediately associated with the person of the arrestee," holding that the Fourth Amendment did not permit agents to search a 200-pound locked footlocker without a warrant incident to his arrest, even though they had probable cause to believe that it contained drugs.[37] Instead, the Court held that agents could seize the locker, but had to get a warrant for the search of its contents.[38]

---

35. Chimel v. California, 395 U.S. 752, 762–63, 766–67 (1969) (limiting the search-incident-to-arrest exception to the warrant requirement to "the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence"—because of significant invasion of privacy that would result from a search of Chimel's entire house). The *Chimel* rule was justified by, and limited to situations that evoked concerns with officer safety and evidence preservation. *See* Arizona v. Gant, 556 U.S. 332, 343 (2009) (permitting searches of the passenger compartments of vehicles incident to an occupant's arrest only in situations in which either the arrestee is unsecured and within reaching distance of the passenger compartment or where there is reason to believe that evidence relating to the crime(s) of arrest might be found in the vehicle); *Chimel*, 395 U.S. at 763, 768.

36. United States v. Robinson, 414 U.S. 218, 236 (upholding, as a categorically valid search incident to Robinson's arrest, a pat-down of his person and removal and opening of a crumpled cigarette package from his coat pocket, which turned out to contain heroin, even though the arresting officer had no concerns for his safety at the time that he conducted the search).

37. United States v. Chadwick, 433 U.S. 1, 3–4, 15 (1977). Lower courts, on the other hand, have often permitted searches of areas with greater privacy for, and a farther distance from, arrestees' incident to arrest. *See, e.g.*, United States v. Carrion, 809 F.2d 1120, 1123, 1128 (5th Cir. 1987) (permitting the search of Carrion's billfold and address book incident to arrest); United States v. Lee, 501 F.2d 890, 891–92 (D.C. Cir. 1974) (permitting the search of Lee's purse incident to arrest); Ricks v. State, 586 A.2d 740, 743, 746 (Md. 1991) (upholding a warrantless search of Rick's luggage incident to his arrest).

38. *See Chadwick*, 433 U.S. at 3, 14. *But see* Wyoming v. Houghton, 526 U.S. 295, 302 (1999) (holding that the Fourth Amendment permitted the warrantless search of a passenger's purse discovered in the passenger compartment of a vehicle when the police had probable cause to believe that the driver of the vehicle had illegal drugs inside, even though the police lacked any individualized suspicion that the drugs were in the passenger's purse); California v. Acevedo, 500 U.S. 565, 579–80 (1991) (holding that the police did not need a warrant to search a container in a car as long as they had probable cause to believe that it contained evidence of a crime); United States v. Ross, 456 U.S. 798, 825 (1982) (holding that, when the police had probable cause to believe that there was contraband or evidence of a crime in a vehicle, they could search every part of the vehicle, including inside containers that could hold the item for which they had probable cause). In *Houghton*, *Acevedo*, and *Ross*, the Court relied on the *Carroll* doctrine (the so-called automobile exception) and distinguished, rather than overruling, *Chadwick* and *Sanders*, thus significantly narrowing their doctrinal reach. *See Acevedo*, 500 U.S. at 580.

While the early container-search cases often involved containers like luggage, the Court has made clear that the definition of "container" is not so limited.[39] In keeping with what can broadly be construed as the container doctrine, the Court should distinguish between biological samples, as containers, and DNA,[40] as their contents, in the same way that some courts have found that the expectation of privacy in the digital data in mobile devices and laptop computers to be analogous to, or even greater than, the expectation of privacy that one has in the contents of a closed container or in a personal telephone book containing directory information.[41]

B. Modern Containers: Computers and Other High-Volume Digital Devices

---

39. *See* New York v. Belton, 453 U.S. 454, 460 n.4 (1981) (defining a container as "any object capable of holding another object").

40. *Cf.* Cynthia Lee, *Package Bombs, Footlockers, and Laptops: What the Disappearing Container Doctrine Can Tell Us About the Fourth Amendment*, 100 J. CRIM. L. & CRIMINOLOGY 1403, 1414 (2010) ("Even the human body can be considered a container since the body, as drug smugglers and savvy inmates know, is capable of holding or concealing various objects."); Charles E. MacLean, *But, Your Honor, a Cell Phone Is Not a Cigarette Pack: An Immodest Call for a Return to the* Chimel *Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 37, 38–39 (2012) (arguing that the Supreme Court should distinguish cell phone memories from other containers, recognize that cell phone users have an objectively reasonable expectation of privacy in their cell phone memories, and permit searches of them incident to arrest only when necessary to ensure officer safety or safeguard evidence from destruction or loss).

41. *See* United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) ("[T]he Fourth Amendment protection of closed computer files and hard drives is similar to the protection it affords a person's closed containers."); United States v. David, 756 F. Supp. 1385, 1391 (D. Nev. 1991) (treating a handheld computer memo book as a closed container for Fourth Amendment purposes); People v. Emerson, 766 N.Y.S.2d 482, 487, 490 (Sup. Ct. 2003) (treating computers as closed containers and the digital files that they contain as their contents entitled to separate protection); *see also* State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) ("[B]ecause a cell phone is not a closed container, and because an individual has a privacy interest in the contents of a cell phone that goes beyond the privacy interest in an address book or pager, an officer may not conduct a search of a cell phone's contents incident to a lawful arrest without first obtaining a warrant."); *see generally* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 195 (2005) (arguing that computer searches should be treated like other container searches). *But see* United States v. Simpson, 152 F.3d 1241, 1248 (10th Cir. 1998) (rejecting Simpson's argument that his computer disks and hard drive were the equivalent of closed containers requiring a search warrant and probable cause to search).

These personal property cases dovetail with the jurisprudence governing the required procedures for execution of search warrants issued for the seizure of computers and search of the electronically stored information that they contain. For example, in *United States v. Comprehensive Drug Testing, Inc.*,[42] the United States Court of Appeals for the Ninth Circuit reviewed the execution of several warrants during the course of the Government's investigation into the Bay Area Laboratory Collective, which it suspected of providing steroids to Major League Baseball players.[43] During the investigation, the Government developed probable cause to believe that ten players had tested positive for steroid use during the anonymous drug testing to which they were subjected as part of their collective bargaining agreement with the league.[44] On the basis of that probable cause, the Government obtained a warrant to search the facilities of the contractor who performed the tests, Comprehensive Drug Testing, Inc. ("CDT"), and seized the records of the ten players.[45] However, when agents executed the warrant, they copied from CDT's computers records pertaining to drug testing hundreds of other baseball players and athletes engaged in other professional sports.[46] CDT and the Major League Baseball Players Association moved, pursuant to Federal Rule of Criminal Procedure 41(g),[47] for the return of the seized information, and the district court granted the motion. Rejecting the Government's argument that the other players' data was in plain view during its

---

42. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) [hereinafter *CDT*].

43. *See id.* at 1166.

44. *See id.*

45. *See id.* at 1166–67.

46. *See id.* at 1166, 1169.

47. *See* F. R. CRIM. P. 41(g); *CDT*, 621 F.3d at 1172–74; *see also* United States v. Calandra, 414 U.S. 338, 354 n.10 (1974) (holding that the Fourth Amendment exclusionary rule did not apply to grand-jury proceedings in part because of the availability of the substitute remedies, including a motion to return property under Rule 41); Ramsden v. United States, 2 F.3d 322, 327 (9th Cir. 1993) (explaining that Rule 41(g) authorizes district courts to return illegally seized evidence to a non-defendant prior to trial); *see generally* Carrie Leonetti, *Independent and Adequate: Maryland's State Exclusionary Rule for Illegally Obtained Evidence*, 38 U. BALT. L. REV. 231, 261–63 (2009) (discussing the history of Rule 41(g) and its use as the functional equivalent of a pretrial motion to suppress illegally obtained evidence). *But see* United States v. Payner, 447 U.S. 727, 735 (1980) (holding that "the supervisory power does not authorize a federal court to suppress otherwise admissible evidence on the grounds that it was seized unlawfully from a third party not before the court").

legal search for records pertaining to the ten initial targets, the district court suppressed the other players' information because of the Government's failure to "segregate information as to which the government had probable cause from" the other records that were "swept up" during the seizures.[48]

Affirming the suppression order below, the Ninth Circuit emphasized the importance of "maintain[ing] the privacy of materials that are intermingled with seizable materials" and "avoid[ing] turning a limited search for particular information into a general search of office file systems and computer databases."[49] The court also emphasized the fact that individuals cannot opt out of storing their data electronically: "Government intrusions into large private databases thus have the potential to expose exceedingly sensitive information about countless individuals not implicated in any criminal activity, who might not even know that the information about them has been seized and thus can do nothing to protect their privacy."[50]

Much of the court's overbreadth analysis[51] applies with equal, if not more, force, to the seizure in "plain view" and from public places not only of raw biological evidence (saliva) but also the genetic information that it contains. Computers like those at CDT are large digital containers. They contain a great deal of data, in this case simultaneously including that of the "innocent" non-targets of the Government investigation, that is private and sensitive. The court was concerned with the Government's treatment of the digital contents of the computer that it seized as no more private than its container. This concern is similar to the concern with the forensic analysis of DNA as being no more of an invasion than seizure of a skin cell or drop of saliva in the first instance.

---

48. *CDT*, 621 F.3d at 1166–67, 1170. There were actually multiple warrants and/or subpoenas issued and quashed in multiple districts, *see id.* at 1166–71, but this Article refers to them collectively in the singular for simplicity.

49. *Id.* at 1170.

50. *Id.* at 1177. *But see* United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) (upholding the warrantless, suspicion-less search of Arnold's laptop under the border-search doctrine and rejecting his argument that laptop searches should require individualized suspicion, even at the border, because they are repositories of highly personal information).

51. This term refers to search warrants that fail to meet the particularity requirement of the Fourth Amendment—the areas to be searched and/or items to be seized are "overbroad" in comparison to the probable cause justifying the search.

V. TMI: DIGITAL DATA AS A MORE APT ANALOGY

The searches that the Court recognized and limited in *Riley* are a good analogy for warrantless DNA analysis. In *Riley,* the Court recognized the searches of the digital contents of legally-seized cell phones should be subject to the warrant requirement, in part because the privacy interest in digital data was both greater than the privacy interest and less likely to harm officers or be subject to destruction than the physical objects at issue in *Robinson*.[52] The court reasoned that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[53]

Those same considerations (high privacy interest and low likelihood of threatening safety or being subject to evidentiary destruction) are even more acute in the context of the genetic information contained in biological evidence already seized.[54] The Court also reasoned that the search of the digital contents of a cell phone "bears little resemblance to the type of brief physical search considered in *Robinson*"[55]—an observation also at least as true of the forensic analysis of the DNA in a biological evidence sample. The Court specifically pointed to the possibility of discovering sensitive medical information through an arrestee's Internet browsing history in deciding that a search of a cell phone was qualitatively different than a search of a physical object removed from an individual incident to arrest. [56] This concern, again, seems

52. *See* Riley v. California, 134 S. Ct. 2473, 2493–94 (2014).

53. *Id.* at 2488–89.

54. In *Riley*, the State of California and the United States (as *amicus*) defended the warrantless search of Riley's seized cell phone (unsuccessfully) in part on the ground that he might be able to use it to tip off accomplices of an impending arrest, which they characterized as a potential threat to officer safety. *See id.* at 2485. Obviously, the same could not be said of a suspect's access to biological evidence. *Cf. id.* at 2486 (noting that "once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone"). They also defended it on the ground that digital data on a cell phone could be subject to unique forms of destruction through remote wiping and data encryption. *See id.* There is also no comparable form of genetic wiping or encryption.

55. *Id.* at 2485.

56. *See id.* at 2490. While forensic DNA analysis focuses on "noncoding" regions of the genome for identification purposes, those regions are noncoding only in the sense that the current state of genomics has not identified that for which they code. They are not inherently noncoding. *See* Guy Gugliotta, *Rush to Use of DNA Sampling Raises Questions About Privacy*, L.A. TIMES, Sept. 5, 1999, at A12 (discussing the possibility of identifying behavioral predispositions through DNA analysis in the future); *cf.* Simon A. Cole, *Is the "Junk" DNA*

more acute in the context of genetic information, the forensic analysis of which carries even more potential to reveal the presence of certain medical conditions.

The Fourth Amendment jurisprudence can distinguish between biological evidence like skin and hair cells (the containers) and the genetic code inside (the contents) by analogy to cell phone searches. Like digital data on a cell phone, a forensic DNA profile is available only after additional investigation that is far more extensive and intrusive than the original seizure of its container. Even when there is legal cause to seize biological evidence on a container, like a discarded coffee up, additional justification (presumptively a warrant based on probable cause) should be required to analyze (search) the genetic code inside. Courts should construe this second step (analyzing the genetic code within a biological evidence sample) as a search for many of the same reasons that the search of a mobile device is considered a "search" under the Fourth Amendment: individuals have a reasonable expectation of privacy in the genetic code inside of their shed biological material that is different from (and independent of) whatever expectations they may have in its container.[57]

The analogy, of course, is an imperfect one, since the digital data cases deal with primary seizures of the digital device that are legally justified by either probable cause (e.g., to believe that the digital device is an instrumentality of crime) or an exception to the warrant requirement (like the search-incident-to-arrest doctrine), rather than abandonment.[58] Courts have not yet addressed the question of whether the police could search the digital data on a mobile device that had, for example, been left behind in a restaurant or disposed of without destruction of its hard drive.[59]

Designation Bunk?, 102 NW. U. L. REV. 54, 56–57 (2007) (arguing that even if short-tandem-repeat regions of the genome have no biological functionality, they could still be associated with the presence of certain diseases or medical conditions).

57. *Cf.* Oliver v. United States, 466 U.S. 170, 181 (1984) (holding that agents had not conducted a "search," for Fourth Amendment purposes, of the "open fields" beyond the curtilage of Oliver's home because he had no expectation of privacy in them).

58. *Compare Riley*, 134 S. Ct. at 2473, *and* State v. Smith, 920 N.E.2d 949, 949 (Ohio 2009) (rejecting the warrantless search of the contents of a cell phone incident to arrest), *with* United States v. Brown, 473 F.2d 952 (5th Cir. 1973) (holding that the Fourth Amendment did not require the police to obtain a search warrant before seizing, opening, and searching a suitcase containing stolen money that an accused bank robber had abandoned in an open field).

59. *Cf.* California v. Greenwood, 486 U.S. 35, 45 (1988) (permitting the warrantless search of the contents of the garbage can because the can had been

The Court has, however, extended the container doctrine to containers no longer in the immediate control of the suspect. For example, in *Arkansas v. Sanders*,[60] the Court required a search warrant for police to open and search an unlocked suitcase

"abandoned" at the curb for disposal); United States v. Jones, 406 F. App'x 953, 954–955 (6th Cir. 2011) (holding that the Fourth Amendment did not require law enforcement officers to obtain a warrant before seizing and searching Jones's jacket, which he left in the back of a bar); United States v. Rem, 984 F.2d 806, 814 (7th Cir. 1993) (holding that the Fourth Amendment did not require agents to obtain a warrant before seizing and searching a suitcase containing cocaine because Rem had abandoned it by leaving it on the train when he deboarded and denied that he had been on the train when asked by agents); United States v. Liu, 180 F.3d 957, 961–962 (9th Cir. 1999) (holding that the Fourth Amendment did not require agents to secure a warrant before seizing and searching a suitcase that Liu had abandoned by leaving it on a train when he nervously fled an agent's request to see his ticket); United States v. Landry, 154 F.3d 897, 899 (8th Cir. 1998) (holding that the Fourth Amendment did not require agents to obtain a warrant to a seize a paper bag containing crack cocaine that Landry had abandoned by leaving it in a dumpster while he used a nearby pay phone); United States v. Washington, 12 F.3d 1128, 1132 (D.C. Cir. 1994) (holding that Washington had abandoned his overturned vehicle and its contents in an alley when he fled the scene after a high-speed chase and that the Fourth Amendment did not require the police to obtain a warrant to search a plastic bag, containing drugs, that was in plain view inside); United States v. Wilder, 951 F.2d 1283, 1286 (D.C. Cir. 1991) (holding that the Fourth Amendment did not require the police to obtain a warrant before seizing and searching a paper bag containing crack cocaine after Wilder left it on the steps of a public building and began to walk away after noticing the police watching him); People v. Roybal, 966 P.2d 521, 536–37 (Cal. 1998) (holding that the Fourth Amendment did not require the police to obtain a warrant to seize and search the contents of a plastic bag that Roybal abandoned by placing it on a peripheral cinder-block wall that separated his mother's backyard from her neighbors'); State v. Belcher, 759 P.2d 1096, 1097 (Or. 1988) (holding that the Fourth Amendment did not require the police to obtain a warrant to seize and inspect the contents of a backpack that Belcher had abandoned by leaving it behind in the parking lot of a tavern when he fled the scene of a fight that the police had come to investigate). Of course, these "abandonment"-of-container cases involve factual scenarios suggesting that the suspect's abandonment is much more knowing and intentional than the "abandonment" that occurs with shed microscopic biological material. *See* State v. Joyce, 639 A.2d 1007, 1016–17 (Conn. 1994) (holding that an arson suspect had not abandoned his clothing, when he left it by the side of the road after an emergency medical technician removed it before transporting him to the hospital for treatment of the burns that he received in the suspicious fire); State v. Westover, 666 A.2d 1344, 1348–49 (N.H. 1995) (holding that a passenger in an automobile did not abandon his sweatshirt, which contained marijuana revealed in a warrantless search, when he tossed it aside before entering a store). They also suggest facts that would likely amount to probable cause and, in at least some cases, exigent circumstances, neither of which is present in the typical "abandoned"-DNA case.

60. Arkansas v. Sanders, 442 U.S. 753, 766 (1979).

containing marijuana that Sanders had given to another man, who placed it in the trunk of a taxi and drove away, before being stopped by the police. The Court did so, in part, because once the police had secured the suitcase, there was no reason to dispense with the requirement that they obtain a warrant for its contents.[61]

This distinction between "abandoned" property and property seized incident to arrest also indirectly points to greater ones between digital and genetic containers: unlike digital data, the genetic code is (at least for the time being) immutable and indestructible. One who disposes of an old cell phone not only realizes its private, digital contents, but can take steps to delete or destroy them. One cannot choose to "delete" genetic information from cells—or realistically choose not to shed biological samples at all. For this reason, the "abandonment" of the container should not entail "abandonment" of the contents in the context of biological evidence. The Court has, in other contexts, used the type of container and contents as a factor in determining whether an individual has a reasonable expectation of privacy in them.[62] For example, in *Sanders*, the Court emphasized the personal nature of the typical contents of luggage.[63] Post-*Katz*, of course, this inquiry would not turn on the physical nature of the container itself,[64] but rather societal expectations about whether certain containers and their contents are inherently more private than others.[65]

---

61. *See id.* at 755, 762.

62. *See* Albert W. Alschuler, *Bright Line Fever and the Fourth Amendment*, 45 U. PITT. L. REV. 227, 278 (1984) (noting that some courts "distinguish 'worthy containers' whose search ordinarily would require advance judicial approval, from 'unworthy containers,' which police officers could search without warrants and without probable cause"); *see*, *e.g.*, *Sanders*, 442 U.S. at 764 n.13 ("Not all containers and packages found by police during the course of a search will deserve the full protection of the Fourth Amendment. Thus, some containers (for example a kit of burglar tools or a gun case) by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance.").

63. *See Sanders*, 442 U.S. at 762.

64. *See* United States v. Ross, 456 U.S. 798, 822 (1982) (refusing to determine whether a particular container was entitled to Fourth Amendment protections on the basis of its physical configuration).

65. *Cf.* Lee, *supra* note 40, at 1424 (arguing that the home could be viewed simply as the type of container most associated with personal privacy and therefore most worthy of Fourth Amendment protection); Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 1000 (1982) (arguing that the Supreme Court affords less protection to vehicles under the Fourth Amendment because it (wrongly) views them as areas of diminished societal expectations of privacy).

The primary factor that courts consider in determining whether an expectation of privacy is objectively reasonable (i.e., whether society is prepared to recognize such an expectation as reasonable)[66] is whether there is a "societal understanding that certain areas deserve the most scrupulous protection from government invasion."[67] In making this determination, the courts often look to the way that the legislature treats the area. For example, in *New York v. Burger*,[68] the Court allowed the warrantless search of a "chop shop" in New York in part because the New York State Legislature highly regulates automobile junkyards, and owners or operators of commercial premises in a closely regulated industry have a reduced expectation of privacy.[69] In *Riley v. Florida*,[70] the Court upheld the warrantless helicopter surveillance of Riley's backyard in part because the police helicopter was flying at an altitude that was "legal" under Federal Aviation Administration ("FAA") regulations.[71] In *Skinner v. Ry.Labor Execs. Ass'n*,[72] the Court held that the warrantless extraction of breath and urine from railroad employees for drug and alcohol testing was reasonable under the Fourth Amendment in part because railroad employment is heavily regulated, so railroad employees have a diminished expectation of privacy regarding their bodily fluids.[73]

---

66. While the *Katz* test is conjunctive (i.e., an expectation of privacy must be subjective/actual *and* objectively reasonable), courts historically give more weight to the second prong (objective reasonableness) for the simple reason that defendants who have moved to suppress seized evidence almost always have a subjective belief that the evidence was private. *See* Hudson v. Palmer, 468 U.S. 517, 525 n.7 (1984).

67. Oliver v. United States, 466 U.S. 170, 178 (1984). *See* United States v. Rakas, 439 U.S. 128, 143 n.12 (1978) (the defendant Rakas failed to demonstrate that he had an objectively reasonable expectation of privacy regarding the car that he was driving, because he had neither a property interest nor a possessory interest in the car).

68. New York v. Burger, 482 U.S. 691, 702–04 (1987).

69. *See id.* at 698–99, 706 n.17.

70. Florida v. Riley, 488 U.S. 445, 445-46 (1989).

71. *See id.* at 449–51 (noting that it was "of obvious importance that the helicopter in this case was not violating the law" in determining that Riley did not have a reasonable expectation of privacy in being free from aerial surveillance in his backyard). *But see id.* at 454 (O'Connor, J., concurring) (concurring in the Court's result that the warrantless surveillance was reasonable but disagreeing that the legality of the surveillance under FAA regulations was the reason for that result).

72. Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 627 (2004).

73. *See id.* at 624, 627. The Court has similarly found diminished expectations of privacy in vehicles in part because of their pervasive statutory

The converse is also true: courts sometimes find an expectation of privacy to be reasonable if it is consistent with a statutory scheme of protection. For example, in *Chapa v. State*,[74] the Texas Court of Criminal Appeals held that taxi passengers have a sufficiently reasonable expectation of privacy in the interior of a taxi to contest its warrantless search. The holding was based on municipal ordinances in several Texas cities that give taxi passengers the right to exclude others from the taxis in which they are riding.[75] The reasoning in these cases tends to be that a legislature's collective judgment that a particular area or activity warrants heightened protection is a good indication of whether that area or activity is one that society is collectively prepared to protect.

Applying this reasoning to the context of warrantless DNA collection and analysis, our society has indicated that it is prepared to protect expectations of genetic privacy as reasonable. Returning to the analogy to digital information, depending on the circumstances, an unauthorized search of text messages may violate the Wiretap Act,[76] the Stored Communications Act ("SCA"),[77] the Electronic Communications Privacy Act ("ECPA"),[78] and state wiretapping statutes.[79] Similarly,

---

regulation. *See* South Dakota v. Opperman, 428 U.S. 364, 367–68 (1976); Cady v. Dombrowski, 413 U.S. 433, 440–42 (1973); *see also* United States v. Rakas, 439 U.S. 128, 154 n.2 (1978) (Powell, J., concurring).

74. Chapa v. State, 729 S.W.2d 723, 728 (Tex. Crim. App. 1987).

75. *See id.* at 728–29. *But see* California v. Greenwood, 486 U.S. 35, 43–44 (1988) (rejecting Greenwood's reliance on municipal ordinances requiring disposal of garbage at the curbside to demonstrate that a reasonable expectation of privacy in garbage disposed of in compliance with the ordinances and noting that "the law of the particular State in which the search occurs" did not determine its reasonableness under the Fourth Amendment); Dow Chem. Co. v. United States, 476 U.S. 227, 232 (1986) (upholding the warrantless aerial surveillance of two power plants in a chemical-manufacturing facility and holding that trade-secrets statutes, which protected Dow's privacy, were irrelevant to determining the constitutionality of the Government's surveillance).

76. 18 U.S.C. §§ 2510–2522 (2002) (governing the interception of electronic communications).

77. 18 U.S.C. §§ 2701–2712 (2002) (governing the disclosure of information by electronic-communications providers). The SCA was enacted as Title II of the ECPA.

78. Pub. L. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). The ECPA systematically restructured the Wiretap Act, effectively combining the Wiretap Act, the SCA, and the Pen Register Act, 18 U.S.C. §§ 3127(3)–3127(4) (1968) (governing the collection of incoming and outgoing phone numbers to/from a target phone), into a single legislative system. *See* Colin Shaff, *Is the Court Allergic to* Katz*? Problems Posed by New Methods*

approximately a dozen states have genetic-information laws that could, at least theoretically, prohibit DNA theft.[80] Alaska, the state with the most stringent standards, requires written consent from individuals before collecting, analyzing, and retaining their DNA and disclosing the results of the analysis.[81] Florida, New Jersey, New York, and Oregon have also criminalized DNA theft, although violation of these prohibitions is generally classified as a misdemeanor.[82]

In 2011, legislatures in Massachusetts, Vermont, and California considered "Genetic Bills of Rights," which would have granted individuals explicit property and privacy rights in their genetic information, although they contained exceptions for law-enforcement collection.[83] At the federal level, the new Genetic Information Nondiscrimination Act[84] prohibits genetic profiling by some employers and health-insurance companies.[85]

---

of Electronic Surveillance to the "Reasonable-Expectation-of-Privacy" Test, 23 S. CAL. INTERDISC. L.J. 409, 441 (2014). Congress passed the ECPA to prevent the "unauthorized interception of electronic communications" and "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. No. 99-541, at 1 (1986).

79. These statutory violations are of limited importance in a criminal prosecution because suppression of evidence is rarely required for a violation of the Wiretap Act and is explicitly precluded by the SCA, which authorizes solely civil remedies for its violation.

80. *See, e.g.*, COLO. REV. STAT. § 10-3-1104.7(1)(a) (2009) ("Genetic information is the unique property of the individual to whom the information pertains"); GA. CODE ANN. § 33-54-1 (1995); LA. REV. STAT. § 22:213.7(E) (2011).

81. *See* ALASKA STAT. § 18.13.010-100 (2004); *see generally* Patrick G. Lee, *DNA Theft Wades into Largely Uncharted Territory*, WALL ST. J. L. BLOG (Aug. 8, 2011, 5:16 PM), http://blogs.wsj.com/law/2011/08/08/dna-theft-wades-into-largely-uncharted-legal-territory.

82. *See, e.g.*, FLA. STAT. ANN. § 760.40 (2009); *cf.* People v. Dolan, 408 N.Y.S.2d 249, 252 (Sup. Ct. 1978) (suggesting that Dolan had a property interest in a vial of his blood retained by a private hospital). *But cf.* Moore v. Regents, 793 P.2d 479, 487–97 (Cal. 1990) (holding that Moore did not own a cell line derived from his cells such that he was entitled to recover their commercial value in a conversion suit against the researchers that retained them).

83. *See* Kevin Hartnett, *The DNA in Your Garbage: Up for Grabs*, BOSTON GLOBE (May 12, 2013), http://www.bostonglobe.com/ideas/2013/05/11/the-dna-your-garbage-for-grabs/sU12MtVLkoypL1qu2iF6IL/story.html; Lee, *supra* note 40 at 1427.

84. 42 U.S.C. §§ 2000ff–2000ff-11. (2008).

85. *See* Kathy L. Hudson, et al., *Keeping Pace with the Times: The Genetic Information Nondiscrimination Act of 2008*, 358 NEW ENG. J. MED. 2661 (2008), *available at* http://www.nejm.org/doi/full/10.1056/NEJMp0803964.

What this Article proposes is also analogous to the Supreme Court's recent decision in *United States v. Jones*[86] and, in particular, the way that the Court distinguished *Jones* from its earlier decision in *United States v. Knotts*.[87] In *Knotts*, the Court upheld the warrantless tracking of Knotts using the signal from a radio beeper placed in a drum of chloroform with permission from the chloroform manufacturer, but without permission from Knotts.[88] In *Jones*, the police engaged in similar warrantless surveillance of Jones by planting a GPS device on his vehicle, which allowed the police to monitor the vehicle's physical movements twenty-four hours per day for twenty-eight days.[89] *Knotts* notwithstanding, the Court unanimously held that the Government's installation of the GPS device constituted a search, albeit on very narrow grounds: the installation constituted an unreasonable search because the police had physically invaded Jones's private property in order to plant the device.[90]

For five concurring justices,[91] the issue was a broader one: the Government's warrantless access to and use of the satellite transmission of Jones's location.[92] As Justice Sotomayor explained in her concurring opinion: "[o]f course, the Fourth Amendment is not concerned only with trespassory intrusions on property. Rather, even in the absence of a trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'"[93] Removing the trespass issue underlying the narrow majority

86. United States v. Jones, 132 S. Ct. 945, 948–954 (2012) (holding that the Government's installation of a GPS device on Jones's vehicle and monitoring its publicly visible movements without a valid warrant constituted a search for Fourth Amendment purposes).

87. United States v. Knotts, 460 U.S. 276, 281 (1983) (holding that a person "travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another").

88. *See id.* at 278–85. *But see* United States v. Karo, 468 U.S. 705, 714–15 (1984) (distinguishing *Knotts* and holding that the monitoring of a beeper in a private residence, whose location was not open to visual surveillance, violated the Fourth Amendment rights of those who had a cognizable privacy interest in the residence).

89. *Jones*, 123 S. Ct. at 948.

90. *Id.* at 949.

91. *See id.* at 954 (Sotomayor, J., concurring) (noting that, although she joined the majority in its narrow property-rights holding, she would have agreed with the four concurring justices finding that the GPS tracking was a search even if the placement of the device had not occurred on Jones's private property).

92. *See id.* at 964 (Alito, J., concurring).

93. *Id.* at 954 (Sotomayor, J., concurring) (internal citation omitted).

opinion, for the five concurring justices, the intellectual exercise of *Jones* is more difficult, of course: distinguishing the GPS search in Jones from the beeper search in *Knotts* on some alternate, broader ground.[94]

The analogy that this Article proposes is a four-part one, which can be reduced as follows: the relationship between Justice Sotomayor's concurring opinion in *Jones* and the majority's decision in *Knotts* is equivalent to the relationship between this proposal regarding the DNA analysis of "abandoned" biological evidence and the Court's decision in *Greenwood*. Just as the warrantless GPS search in *Jones* was different, in a legally meaningful way, from the beeper search in *Knotts*, the search of the contents of a biological sample (the genetic code that it contains) should be viewed as different, in a legally meaningful way, from the seizure of the biological sample that contains it. The mere fact of being, or leaving a sample, in "public" is different than what the police do to surveil or analyze that public presence.[95]

VI. CONCLUSION: THE PATH FORWARD

By its text, the Fourth Amendment only guarantees the right to privacy in "persons, houses, papers, and effects." But the Supreme Court, decades ago, took a broader view, ruling in *Katz* that a search could be unreasonable even without a physical intrusion into a private place. The Court concluded that "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[96]

Since deciding *Katz* in 1967, the Supreme Court has defined the protections of the Fourth Amendment in terms of this "reasonable expectation of privacy." How does that definition apply in the context of the surreptitious collection of "abandoned" DNA? The key issue in answering this question is where to draw

---

94. *Cf. id.* at 958 (Alito, J., concurring) ("I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.").

95. *Cf. In re* Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not voluntarily shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information." (emphasis in the original)).

96. Katz v. United States, 389 U.S. 347, 359 (1967).

the line between warrantless surveillance that society would and should view as reasonable, and surveillance that it would view as unreasonable.

On the one hand, the courts have long held that people have no expectation of privacy in items that they "knowingly expose" to public view—the collection of those items falls outside the Fourth Amendment's protections.[97] On the other hand, people have the expectation that the police are not following their every move to collect the microscopic genetic information that they involuntarily shed as they go about their daily lives.[98] As technology develops, the police are gaining more ability to collect anyone's DNA at any time, particularly through the increasing ubiquity of "fingerprint" DNA analysis.[99] A great deal of personal, identifying biological information can be learned by surreptitiously following someone for a few days and waiting for them to discard a cigarette butt or a coffee cup. If technology makes having any modicum of genetic privacy functionally impossible, then an individual can never have a reasonable expectation of it.

The plain view and abandonment doctrines make less and less sense when courts apply them to "abandoned" genetic material. In 2015, it is hard to credit the notion that we are "voluntarily" sharing our genetic information with third parties by leaving cells behind as we travel through the world and thereby forfeiting the protections of the Fourth Amendment. In other words, the collection of "abandoned" DNA, like the collection of personal digital information from a mobile device, involves something more than the collection of Greenwood's discarded garbage from the curb.

---

97. *See* Leonetti, *Data Mining*, *supra* note 13, at 274–75.

98. *Cf.* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L. J. 213, 272–85 (2002) (demonstrating empirically that Americans have an expectation of privacy to be free from unconstrained public video surveillance).

99. *See* NAT'L COMM'N ON THE FUTURE OF DNA EVIDENCE, U.S. DEP'T OF JUSTICE, WHAT EVERY LAW ENFORCEMENT OFFICER SHOULD KNOW ABOUT DNA EVIDENCE 2 (1999) (noting that "only a few cells can be sufficient to obtain useful DNA information").