2011

# DNA Database Trawls and the Definition of a Search in Boroian v. Mueller

David H. Kaye
*Penn State Law*

VIRGINIA LAW REVIEW
*IN BRIEF*

VOLUME 97 AUGUST 4, 2011 PAGES 41–49

***ESSAY***

# DNA DATABASE TRAWLS AND THE DEFINITION OF A SEARCH IN *BOROIAN V. MUELLER*

*David H. Kaye*[*]

CONVICTED offenders have brought dozens of constitutional challenges to statutes establishing DNA databases for law enforcement. Not one has succeeded. In *United States v. Weikert*, the United States Court of Appeals for the First Circuit rejected a Fourth Amendment challenge from a probationer who objected to providing the government with a sample of his DNA, explaining that

> the government's important interests in monitoring and rehabilitating supervised releasees, solving crimes, and exonerating innocent individuals outweigh Weikert's privacy interests, given his status as a supervised releasee, the relatively minimal inconvenience occasioned by a blood draw, and the coding of genetic information that, by statute, may be used only for purposes of identification.[1]

By "identification," the court meant trawling through the national database of stored DNA profiles from offenders—now exceeding nine million—for possible matches to any of the hundreds of thou-

[*] Distinguished Professor and Weiss Family Scholar, Penn State Dickinson School of Law, and Graduate Faculty Member, Forensic Science Program.

[1] 504 F.3d 1, 14 (1st Cir. 2007).

sands of DNA profiles of samples found at crime scenes or on victims.[2]

But how long can past offenders constitutionally be subject to this information-gathering practice? Is there no way an offender can escape "lifelong genetic surveillance"?[3] *Weikert* prominently left open the question of extended retention and trawling of biometric information. The court wrote that it was

> withholding judgment on whether retaining a former conditional releasee's DNA profile in [the national database] passes constitutional muster. The distinction in status between a current and a former offender clearly translates to a change in the privacy interests at stake. A former conditional releasee's increased expectation of privacy warrants a separate balancing of that privacy interest against the government's interest in retaining his profile in [the database].[4]

Now, in *Boroian v. Mueller*, the First Circuit has held that the government can keep a convicted offender's DNA profile in a law enforcement database even after he has paid his metaphorical debt to society.[5] This outcome is hardly surprising. Long-lasting, collateral consequences of convictions have become pervasive,[6] and continuing to trawl for matches to unsolved crimes after a convicted offender is no longer subject to confinement or supervision adds significantly to the power of DNA databases.

Much more surprising is the doctrinal path that the First Circuit elected to follow. The court repudiated the notion that it needed to reexamine the balance of individual and state interests. Instead, it reasoned that continuing to trawl the database for hits to crime scene DNA profiles did not rise to the level of a search that would be

---

[2] By April 2011, the national DNA database, fed by records from state and federal DNA typing laboratories and managed by the FBI, contained "over 9,635,757 offender profiles and 370,875 forensic profiles" and had "produced over 142,700 hits assisting in more than 137,100 investigations." CODIS–NDIS Statistics, FBI (May 2011) http://www.fbi.gov/about-us/lab/codis/ndis-statistics. There are no statistics that would show how much impact the assistance had on investigations or convictions.

[3] Sheldon Krimsky & Tania Simoncelli, Genetic Justice: DNA Databanks, Criminal Investigations, and Civil Liberties 83 (2011).

[4] 504 F.3d at 16.

[5] 616 F.3d 60 (1st Cir. 2010).

[6] Michael Pinard, Collateral Consequences of Criminal Convictions: Confronting Issues of Race and Dignity, 85 N.Y.U. L. Rev. 457 (2010).

subject to the strictures of the Fourth Amendment. The court's explanation of this conclusion was rather terse, consisting of but a few sentences. This Essay starts to fill the gap in the opinion. It indicates how the no-search label reflects a settled understanding of the constitutional protection from unreasonable searches and seizures. In this way, it supplies a deeper structure that supports the retention and reuse of DNA profiles beyond the sentencing period.

## I. THE CASE AND THE PRIOR FIRST CIRCUIT LAW

Martin Boroian was convicted in 2004 of making a false statement to a federal official. For this crime, he spent a year on probation. During this year, he provided (under protest) a blood sample as required by a federal statute mandating the inclusion of DNA profiles in the FBI's national DNA database. In 2008, Boroian sought to have his DNA profile expunged and his DNA sample destroyed. His complaint alleged that the retention and analysis of his DNA profile and sample—after completion of his probation term and without reasonable suspicion of any new criminal activity—violated the Fourth Amendment's prohibition on unreasonable searches and seizures.

The district court dismissed the complaint. The court decided that even if the factual allegations were true, the government was acting constitutionally. First, the court concluded that the government's retention and periodic accessing of his lawfully obtained DNA profile was not a new search within the meaning of the Fourth Amendment. Second, the court held that although a new analysis of the DNA sample could constitute a separate search under the Fourth Amendment, Boroian's complaint contained no allegations of a present or imminent analysis of the sample. In short, the district court determined that the government can hold on to the physical evidence Boroian was required to provide as long as it wanted to, and it could use the information it had extracted from the evidence—Boroian's DNA identification profile—over and over, in checking profiles from new crime scene DNA samples against Boroian's (and those of the millions of convicted offenders with profiles in the national database).

The court of appeals adopted this reasoning. *Boroian* explicitly repudiated *Weikert*'s "dicta that the government's retention and periodic matching of a lawfully obtained profile after the offender had completed his term of supervised release would require a rebalanc-

ing of the relevant government and privacy interests to determine the reasonableness of the search."[7] Without undertaking the "separate balancing" demanded in *Weikert*, it concluded that the government can retrawl ad infinitum. The lynchpin in this result is the definition of a "search" emerging from the precedent-shattering opinion in *Katz v. United States*.[8]

## II. THE DEFINITION OF A SEARCH

*Katz* famously adopted a reasonable-expectation-of-privacy standard, rather than a pure ownership or possession of property test, to mark the boundaries of the Fourth Amendment.[9] For example, without probable cause and a warrant, the police may not place a hidden microphone and transmitter on a public telephone booth to eavesdrop on calls made inside the booth,[10] but they may send a business associate with the same equipment hidden on his person to talk to a suspect.[11] The difference, according to this line of cases, is that one can reasonably expect telephone booths to be free of electronic eavesdropping devices, but one cannot reasonably expect that an associate will not be reporting to the authorities. If an individual has no reasonable expectation that his communications will not be monitored, then the Fourth Amendment, with its preference for warrants, does not come into play and the police can gather information without any reason to suspect an individual of wrongdoing and without prior judicial approval.

*Boroian* used the reasonable-expectation standard, not to expand the boundaries of the Fourth Amendment as *Katz* did, but to keep them confined. Analogizing DNA identification profiles to "fingerprints or mugshots [that] are routinely retained by the government after . . . sentences are complete,"[12] the First Circuit wrote that "we join the other courts to have addressed the issue in holding that the

[7] *Boroian*, 616 F.3d at 68 n.6.

[8] 389 U.S. 347, 351 (1967).

[9] But see Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 816 (2004) (contending that "the *Katz* 'reasonable expectation of privacy' test . . . has not substantially changed the basic property-based contours of Fourth Amendment law").

[10] *Katz*, 389 U.S. 347 (1967).

[11] United States v. White, 401 U.S. 745 (1971).

[12] *Boroian*, 616 F.3d at 67.

government's retention and matching of Boroian's profile against other profiles in CODIS does not violate an expectation of privacy that society is prepared to recognize as reasonable, and thus does not constitute a separate search under the Fourth Amendment."[13]

In general, rejecting the suggestion that every trawl of information in a database is a separate search that requires independent justification is sensible. Once the government lawfully acquires the information, the marginal invasion of privacy that comes from using it later is minimal. Consequently, the government should not be forced to use the data once and then forget it. Suppose that in executing a valid warrant permitting the seizure of a stolen personal computer with serial number C2011A from a warehouse, government agents observe and record the serial numbers C2013A and C2013C on other computers. A week later, they receive a report of a theft of the PC with serial number C2013A. The warrant did not authorize the agents to compare the numbers a week later, but one of them remembers the number (or looks up the record of the first search), thus linking the owner of the warehouse to the second crime. What meritorious privacy interest can the owner assert to stop the government from checking for a match in the serial numbers? Treating the simple trawl of the stored information as not subject to the strictures of the Fourth Amendment—because it is not a "search"—seems appropriate.

## III. THE ACT OF TRAWLING: OLD INFORMATION, NEW FINDINGS, NO SEARCH

Although no court has treated the reuse of legitimately acquired data as a separate search, a recent article questions the view that "[l]awful collection simply ends the analysis: anything further is fair play."[14] According to Professor Erin Murphy, "sensitive and scrupulous" judicial analysis requires asking whether all the steps up to and including the trawls—namely, "offender sample collection, sample testing, sample retention, sample databasing, database searching, possible sample retesting, and so on"—are separate "constitutional moments" under the Fourth Amendment.[15]

[13] Id. at 67–68 (footnote omitted).

[14] Erin Murphy, Relative Doubt: Familial Searches of DNA Databases, 109 Mich. L. Rev. 291, 334 (2010).

[15] Id. at 332–34.

A mechanical rule that would exempt from all Fourth Amendment analysis anything done with data acquired for one purpose might not fit all situations, but a simple rule allowing reuse of data works well enough as long as the additional interests in the privacy of the information are either outside the scope of the Fourth Amendment or too tenuous to justify the usual need for individualized suspicion or warrants.

*Boroian* correctly reflects the conclusion that these premises hold for ordinary retrawls of databases—both before and after the sentence has been served. Despite its rejection of "rebalancing," the First Circuit considered the impact of retrawling on the individual interests that belong in a balancing test. *Boroian* explains that "the government's [additional trawling] is limited to a comparison of the identification records already in its lawful possession and does not reveal any new, private or intimate information about Boroian."[16] The determination that the marginal Fourth Amendment privacy cost is absolutely zero is the crux of the opinion. If it is correct—if post-sentence searches add *nothing* to the invasion of cognizable individual interests that the *Weikert* court already decided must yield to the government's interests—then they also would be permissible as part of the balancing applied to the statutory system *ab initio*. Declaring that there is no reasonable expectation of privacy as to retrawls, and hence no new search, is not to say that anything goes after the initial cheek swab.[17] It merely deems constitutionally permissible the trawling and retrawling of purely identifying profiles, both during and after sentences.

But is the theory that retrawling is constitutionally insignificant correct? Does retrawling really reveal nothing private or intimate about the individual? The court stopped with the observation that continued trawls generate no new information about the structure of the past offender's DNA. But surely retrawls could reveal things a person would rather keep private. For example, an individual whose DNA profile is in the database—a database inhabitant, so to speak—might well be concerned that later trawls will expose him as the perpetrator of an unsolved crime. A later trawl with this outcome

[16] 616 F.3d at 67.

[17] It lends no legitimacy to producing an army of clones from the lawfully acquired sample, to use Professor Murphy's fanciful example, supra note 14, at 335, that resides at least a galaxy away from the Fourth Amendment.

certainly would harm the database inhabitant. But this kind of harm cannot count in any Fourth Amendment calculus. By itself, the discovery that an individual is responsible for a crime does not infringe a legitimate interest, let alone an interest that the Fourth Amendment respects.[18] The Fourth Amendment does not protect information per se. It protects individuals against oppressive methods for acquiring that information.[19]

A slightly more plausible argument for Fourth Amendment protection is that retrawls expose database inhabitants to at least a small risk of becoming suspects even if they are innocent of new crimes. A false incrimination could occur if the database inhabitant is not the source of the crime scene DNA, but coincidentally shares that DNA profile. For full profiles, the probability of such sharing is minuscule, but when the crime-scene DNA is highly degraded (and hence ambiguous), a match is less definitive.[20] A false hit also could occur if the past offender is indeed the source but the police or someone else planted his DNA at the crime scene.[21]

This argument also fails, for much the same reason. The individual interest in being free from falsely incriminating trawls is legitimate enough, but it too does not count in the Fourth Amendment calculus. The false-incrimination objection to DNA database trawls goes not to the impact of the information-gathering technique on privacy, but to the accuracy of the inferences that can be drawn from the information. For better or worse, the Fourth Amendment does not protect against mistaken reasoning about evidence. In a classic search of a home, police also could find planted contraband or ambiguous evidence. It is enough that police, in the judgment of a magistrate issuing a warrant, have a sufficient basis to believe that the search will produce potentially useful information. The Fourth Amendment protects certain kinds of privacy, such as the undisturbed possession or enjoyment of one's dwelling. It does not protect against mistaken inferences from the fruits of a search, whether

[18] See, e.g., United States v. Jacobsen, 466 U.S. 109 (1984).

[19] Compare Boyd v. United States, 116 U.S. 616, 622 (1886) (describing the Amendment as protecting information in the form of business records), with Hale v. Henkel, 201 U.S. 43, 76 (1906) (moving away from *Boyd*'s information-centric perspective).

[20] David H. Kaye, The Double Helix and the Law of Evidence (2010).

[21] See, e.g., David H. Kaye et al., The New Wigmore, A Treatise on Evidence: Expert Evidence § 13.3.1 (2d ed. 2011).

warranted or warrantless. Consequently, the risk of a falsely incriminating trawl does not undercut *Boroian*'s conclusion that weekly trawls of a DNA database are not "separate . . . search[es]."[22]

Still, a database inhabitant also could complain that forging the link to the new crime scene invades the distinct interest in keeping one's whereabouts secret. An individual's concern with spatial privacy seems to sit more comfortably within the Fourth Amendment than the desire for freedom from prosecution or inferential accuracy. In *United States v. Karo*, for example, the Supreme Court held that planting a beeper in a container of ether and tracking the container's movements through houses and other locations constituted a search.[23] A database trawl might produce a match to DNA recovered from the bedroom of a murdered woman, which in turn, might lead to the discovery that the database inhabitant was having an affair with her. *Boroian*'s assurance that "the government's use of [the database] does not reveal any new, private or intimate information"[24] now seems less reassuring.

Nonetheless, trawling differs from the investigatory technique in *Karo*, and the Supreme Court never has viewed the Fourth Amendment as protecting mere information about a person's locations. "Staking out" a suspect's residence and "tailing" him give the police a record of the individual's movements, but that does not make these time-honored practices "searches" that trigger Fourth Amendment protections. Only when the government has entered—physically or technologically—spaces cloaked in a reasonable expectation of privacy has the Court treated the gathering of intelligence about the locations of people or objects as a search.[25] Just because police investigations establish that individuals visited certain places at certain times does not mean that they implicate a reasonable expectation of privacy. It is one thing to place a television monitor in a bedroom, as

[22] Boroian v. Mueller, 616 F.3d 60, 68 (1st Cir. 2010).
[23] 468 U.S. 705 (1984).
[24] 616 F.3d at 67.
[25] See, e.g., Kyllo v. United States, 533 U.S. 27 (2000); United States v. Karo, 468 U.S. 705 (1984).

in Orwell's *1984*.[26] It is another to discover trace evidence that might have come from an intruder in the same bedroom.[27]

*Boroian*'s insistence that later inspection of recorded biometric information is not a new search is thus one viable route to the conclusion that "the state need not destroy records of identification—such as fingerprints, photographs, etc.—of convicted felons, once their sentences are up."[28] This conclusion often is taken for granted, but the permissibility of reusing information is a consequence, and not an axiom, of Fourth Amendment jurisprudence. In *Boroian*, the First Circuit offered a somewhat superficial justification for rejecting the attack on post-sentence DNA trawling. Other courts have done the same. Relating the no-new-search theory to the range and nature of the interests cognizable under the Fourth Amendment provides a deeper structure for the position that retrawls are not new searches that require probable cause, warrants, or other Fourth Amendment protections.[29]

[26] Or even to use GPS devices to monitor every movement of a suspect's car every minute of every day. One circuit court has held that this practice constitutes a search. United States v. Maynard, 615 F.3d 544, 555–56 (D.C. Cir. 2010).

[27] But cf. Tovia Smith, Critics Challenge Familial DNA Testing, NPR (Feb. 28, 2007), http://www.npr.org/templates/story/story.php?storyId=7641971 (quoting Tania Simoncelli as referring to "cameras in everybody's living rooms" in arguing against kinship searches with DNA databases).

[28] United States v. Amerson, 483 F.3d 73, 86 (2d Cir. 2007). A biometric-identification exception to the warrant and probable cause requirements for acquiring and using DNA profiles also would support the result in *Boroian*—and avoid the instability in Fourth Amendment doctrine caused by the "totality of the circumstances" balancing test used in *Weikert* (and derived from the Supreme Court's decision in *Samson v. California*, 547 U.S. 843 (2006)). See David H. Kaye, Who Needs Special Needs? On the Constitutionality of Collecting DNA and Other Biometric Data from Arrestees, 34 J.L. Med. & Ethics 188, 192–95 (2006) (proposing such an exception).

[29] That the Fourth Amendment allows indefinite retention of records is not to say that there should be no time limit on the practice.