

# Who Needs Special Needs? On the Constitutionality of Collecting DNA and Other Biometric Data from Arrestees

*D. H. Kaye*

For years, the collection of DNA samples from individuals arrested for criminal misconduct has been advocated by police officials and endorsed by politicians.<sup>1</sup> Louisiana, Virginia, California, and South Dakota have adopted laws to add DNA profiles derived from these samples to their DNA databases.<sup>2</sup> Texas provides for DNA to be taken after indictment but before conviction.<sup>3</sup> Although the U.S. Department of Justice initially shied away from the issue,<sup>4</sup> the DNA Fingerprint Act of 2005<sup>5</sup> authorizes the collection of DNA from individuals arrested for violations of certain Federal criminal laws,<sup>6</sup> and the inclusion in the national DNA database of all profiles from states that type DNA prior to conviction.<sup>7</sup>

But are these laws constitutional? In an article in a previous issue of this journal, and reprinted in this issue, Professor Tracey Maclin concludes that fidelity to precedent should lead the Supreme Court to strike down two of the Louisiana and Virginia laws as violations of the Fourth Amendment.<sup>8</sup> The article succinctly traces the background of some of this legislation, incisively identifies critical issues, and cogently describes the somewhat undisciplined body of Supreme Court case law that constitutes the “special needs exception” to the general rule that police must obtain a judicial warrant based on probable cause before searching the person or property of an individual for evidence of a crime. Yet, in the same breath that Maclin announces “an objective analysis of the statute themselves [sic], when combined with an objective reading of the Court’s precedents, indicates that the statutes should be declared unconstitutional,”<sup>9</sup> he murmurs that “I doubt the Court will strike down the law on Fourth Amendment or any other constitutional grounds” but rather will resort to “a ‘totality’ or ‘general reasonableness’ model [which] is a standardless formula that permits a majority of the Court to do what it pleases without having to justify its result or reasoning under traditional Fourth Amendment doctrine.”<sup>10</sup>

In contrast, this article shows that the Supreme Court’s opinions do not necessarily imply that DNA sampling at the point of arrest is unconstitutional. Neither do they indicate that the only way to uphold the practice is an undisciplined, result-oriented approach to the issue. To explain this different perspective on the question, Part I summarizes Professor Maclin’s

---

**D. H. Kaye** *bio*

analysis and reveals the point at which his conclusions outstrip his premises. It also explores the analogy he draws between DNA typing and the infrared scanning that was held to be a search in *Kyllo v. United States*.<sup>11</sup> Part II proposes a principled basis for permitting the government to use some systems of DNA sampling both before and after conviction.

## I. DNA Sampling and Fourth Amendment Jurisprudence

Professor Maclin's analysis proceeds in three steps. First, he maintains that "the taking and analyzing of DNA samples is a search."<sup>12</sup> Second, he contends that "under the Court's current precedents, forcibly obtaining and testing DNA samples of arrestees, absent judicial authorization or probable cause for the search, cannot be justified under the special needs exception."<sup>13</sup> Finally, on the basis of these two premises, he concludes that "the statutes should be declared unconstitutional."<sup>14</sup> Although I shall quibble over some details of the development of the first two points, my major disagreement lies in the final inference. It might be correct, but it does not follow from the first two points. Indeed, if this step in the chain of reasoning were valid, it would also follow that all convicted-offender databases are unconstitutional, for these too do not fit neatly into the special-needs doctrine as recently articulated by the Court.<sup>15</sup> This surprising result also might be correct – for a short time, the Ninth Circuit Court of Appeals embraced this view<sup>16</sup> – but it is still jarring. At the least, such potent reasoning warrants careful inspection.

I begin with the first point – the proposition that the compulsory sampling of DNA from an individual is a search of the person. I inspect this claim not to show that it is wrong, but only to explore some of the implications and limitations of the potentially far-reaching case of *Kyllo v. United States*.<sup>17</sup>

### A. DNA Sampling as a Search

Professor Maclin identifies three factors as determinative in ascertaining whether compulsory DNA sampling should be considered a search that triggers scrutiny under the Fourth Amendment: public exposure, bodily intrusion, and information extracted.<sup>18</sup> This analytical framework has been used before to show that compulsory DNA sampling is a search,<sup>19</sup> but Professor Maclin's application of it is distinctive. He seems to state that each consideration is individually sufficient to establish that compulsory DNA sampling is a search. However, only the second or third considerations can justify subjecting the procedure to Fourth Amendment scrutiny.

Under existing law, public exposure defeats a reasonable expectation of privacy, insulating the investigative

practice from Fourth Amendment scrutiny. If the details of DNA polymorphisms were routinely exposed to the public, detaining an individual would still be a seizure of the person. If the arrest were valid, the individual would have no Fourth Amendment right to resist the state's demand for a sample of his DNA. This follows from *United States v. Dionisio*,<sup>20</sup> in which the Court upheld a grand jury subpoena for a voice exemplar on the theory that the subpoena itself was not a seizure of the person, and a person's voice cannot be considered a private matter. The Court explained the second point, which is of interest here, as follows:

The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world.<sup>21</sup>

But the converse is not true. Nothing acquires Fourth Amendment protection just because it is not repeatedly produced for others to hear or see. Using a magnetometer to locate a gun buried in a national forest is not a search just because the criminal who hid it there did not want it to be exposed.

What makes the Fourth Amendment status of DNA sampling open to question is the fact that it involves a type of information that was beyond the scope of the Fourth Amendment when originally drafted. Unlike the buried gun case, it cannot be resolved simply by referring to property rights. This does not mean that biological material is unprotected, but it does mean that, as with the electronic eavesdropping on a conversation in a public telephone booth in *Katz v. United States*,<sup>22</sup> we must look elsewhere to determine whether the object that the government is seeking to obtain lies within the zone of constitutionally protected privacy. If the procedure is a search, it is either because it invades the person's body or because the information is itself quite sensitive.

Nevertheless, Professor Maclin concludes his analysis of application of the public-exposure factor with the observation that "DNA testing of arrestees would constitute a search, even if DNA, like heat emanations, is technically exposed to the public."<sup>23</sup> He seems to arrive at this point on the theory that *Kyllo v. United States*<sup>24</sup> itself establishes that compelling arrestees to give a DNA sample is a search. He writes:

[I]n *Kyllo v. United States*, the Supreme Court ruled that a thermal imaging device directed at a home constituted a search within the meaning of the Fourth Amendment. The Court explained that a search occurs when government agents use sense-enhancing technology to collect any information regarding the interior of a home that could not otherwise be obtained without a physical invasion, “at least where (as here) the technology in question is not in general public use.” Assuming that *Kyllo’s* holding is not limited to the home – where Fourth Amendment concerns have typically been the highest – one can certainly argue that DNA sampling and analysis is sense-enhancing technology that is not in general public use. Therefore, DNA testing of arrestees would constitute a search, even if DNA, like heat emanations, is technically exposed to the public.<sup>25</sup>

I may be reading too much into this brief passage, but it seems to be saying that just because the biotechnology of DNA profiling reveals features not visible to the naked eye, *Kyllo* indicates that the government’s use of it constitutes a search.<sup>26</sup> This reading far outstrips the facts and reasoning of the opinion<sup>27</sup> and conflicts with other opinions of the Court.<sup>28</sup> The majority took pains not to promulgate the broad principle that using “sense-enhancing technology” to acquire information about an individual is, *ipso facto*, a search. It tied its holding to the historical core of protecting property from physical trespass.<sup>29</sup> Thermal imaging was simply a technological substitute for a physical entry. Specifically, the Court wrote:

We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical “intrusion into a constitutionally protected area”...constitutes a search – at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.<sup>30</sup>

To extend this reasoning to DNA sampling, one must not only assume that *Kyllo’s* focus on the home as opposed to other locations is not critical, but also that the technology produces an “intrusion into a constitutionally protected area.” In addition, one must establish that DNA profiling is “not in general public use.”

Given that Professor Maclin makes all three assumptions, it seems worthwhile to pause to see whether they are justified. To begin with, the notion that *Kyllo* extends beyond residential areas is eminently reasonable, even if there is anticlimax language in the opinion.<sup>31</sup> Indeed, it is hard to conceive of an acceptable principle that should rigidly confine *Kyllo* to these locations.<sup>32</sup>

Second, to locate the “constitutionally protected area” implicated in DNA sampling, we must look beyond *Kyllo* to some theory of why there is a reasonable expectation of privacy in the surface of the body or in the information in the cells that are sampled. To maintain the analogy to *Kyllo*, let us imagine that a revolutionary new technology allows police to analyze the structure of the DNA strands coiled in cell nuclei without even touching a person.<sup>33</sup> The biochemical data, in other words, are extracted with no physical invasion of the person, just as the infrared emissions from *Kyllo’s* residence were detected without a physical invasion of the premises. Furthermore, what emerges from the bioscanner is just a printout of the STR types used in forensic identification – an arbitrary set of numbers.

To establish that the bioscanner invades a constitutionally protected area, it won’t do simply to say that if a man’s house is his castle, surely a person’s body is his living room (or some such slogan). The reasons that the Fourth Amendment has been applied generously to the home are not the same as those that would justify comparable protection for the body.<sup>34</sup> We are almost back to *Dionisio*. When the police photograph an arrestee’s face, they are not engaging in a search. Why should “photographing” the structure of the DNA be any different? What justifies treating the cell nucleus as “a constitutionally protected area?” In the earlier parlance of *Katz*, what gives rise to the “reasonable expectation of privacy” in the STR data? As we shall see, these questions can be answered, but the need to answer them shows that the characterization of both thermal imaging and DNA profiling as forms of sensory enhancement is far from sufficient to establish that DNA profiling of a body constitutes a search.

The final step in a full-fledged *Kyllo* analysis is an inquiry into general public usage. If this phrase is not read narrowly, it could, as Professor David Sklansky has warned, “devour much of the Fourth Amendment.”<sup>35</sup> An “objective reading” of the case law, however, inspires little hope for a narrow reading. Magnifying glasses, binoculars, telescopes, and searchlights are not the only instruments that have been classified as being in widespread use.<sup>36</sup> In *Dow Chemical Co. v. United States*,<sup>37</sup> the “EPA employed a commercial aerial photographer, using a standard floor-mounted, precision aerial mapping camera, to take photographs of [two power plants in a chemical manufacturing] facility...”<sup>38</sup> The Court

emphasized the availability of the technology to the public. It insisted that “[t]he photographs at issue in this case are essentially like those commonly used in mapmaking. Any person with an airplane and an aerial camera could readily duplicate them.”<sup>39</sup> For better or worse, the same is true of STR profiling. The biotechnology is there for any person with a checkbook. A typical advertisement from an international firm called DNA Solutions reads as follows: “Our DNA Tests start at \$205 (for testing 3 people), order our FREE Home DNA collection kit now, which has everything you need to collect a DNA sample; (cheek swabs, instructions, simple form, company information, etc.)”<sup>40</sup>

In short, Maclin’s modest claim that “one can certainly argue that DNA sampling and analysis is sense-enhancing technology that is not in general public use” is undeniable. However, the argument itself has yet to be made convincingly. Professor Maclin’s allusion to it is incomplete because dicta in *Kyllo* state that sense-enhancement and limited public use are not sufficient to render the use of the technology a search. Moreover, the allusion is dubious because the claim that DNA profiling is not in public use is, at worst, false, or at best, in need of refinement or development.

Although *Kyllo* does not seem dispositive, this does not mean that compulsory DNA profiling is outside the reach of the Fourth Amendment. The DNA scanner I have invented is science fiction. The result might well be different with real technology, which requires some cells to be removed from the body. However, I am not trying to show that Maclin’s conclusion is wrong – only that the reliance on *Kyllo* accomplishes very little. The heavy lifting comes from other well known concerns. One is the invasive nature of current collection procedures (mild but real). Under a line of cases involving blood sampling, breathalyzers, urine specimens, and nail scrapings, the Court could rely on the dignitary interests related to physical invasions to find that buccal swabbing or saliva sampling for DNA analysis is a *bona fide* Fourth Amendment event.<sup>41</sup>

Another consideration is the fact that the DNA molecules, if analyzed at certain loci that are not particularly useful for identification, could reveal the existence of rare diseases or indicate a predisposition to more common ones. (Most police laboratories are not equipped to do such testing, but with modifications to existing machinery or protocols, they certainly could.)<sup>42</sup> The most powerful argument for Fourth Amendment protection is that the DNA strands have “the potential to reveal a host of private facts.”<sup>43</sup> To the extent that the collection, analysis, and storage procedures used

in DNA identification databases present a meaningful risk of disclosing information that people have an interest in keeping confidential, Maclin is entirely correct: “taking and analyzing of DNA samples is a search”<sup>44</sup> that must be justified as “reasonable” under the Fourth Amendment.<sup>45</sup> We turn, then, to the question of reasonableness.

### B. Reasonableness, Special Needs, Multi-Purpose Searches, and Existing Categorical Exceptions

As a general rule, the Court has demanded that searches be based on judicial warrants supported by probable cause.<sup>46</sup> But many exceptions to this *per se* rule have developed, from “pat-down” searches for weapons (which require only reasonable suspicion),<sup>47</sup> to inventory searches of individuals placed in custody,<sup>48</sup> to searches at border crossings,<sup>49</sup> to name but a few examples. Different exceptions have different rationales, and one set of cases dispenses with the warrant requirement

**The most powerful argument for Fourth Amendment protection is that the DNA strands have “the potential to reveal a host of private facts.”**

“when ‘special needs’ beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable.”<sup>50</sup> Certain programs of compulsory drug testing of Federal employees, for example, have been upheld as reasonable because they serve the government’s special interest as an employer in reducing the use of drugs in its work force or in safeguarding the public with whom these employees deal.<sup>51</sup>

Precisely which cases belong in the “special needs” camp could be debated. Perhaps “administrative searches” such as inspections of buildings to enforce safety codes should be kept apart.<sup>52</sup> For present purposes, however, I shall use “special needs” to denote any system of inspections designed to effectuate goals other than or in addition to catching criminals. In evaluating these systems, the Court typically balances “the individual’s privacy expectations against the Government’s interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context.”<sup>53</sup> This direct balancing approach makes sense on the theory that the *per se* rule against warrantless searches reflects the constitutionally enshrined judgment that the goal of enforcing of the criminal law, standing alone, cannot justify unsupervised police searches. When additional or distinct government interests are pursued, the search might be reasonable despite the lack of a warrant and probable

cause, and “the Court [therefore] undertakes a contemporary balancing of public needs and private interests to enforce the reasonableness requirement.”<sup>54</sup>

Many lower courts have repulsed Fourth Amendment forays against DNA databanking laws for convicted offenders on the basis of the special-needs exception.<sup>55</sup> However, as Professor Maclin emphasizes, the Court has cut back on this exception by blocking its extension to programs whose “primary purpose” is the enforcement of criminal law. This primary-purpose limitation on the special-needs exception can be found in the majority opinions in *Indianapolis v. Edmond*<sup>56</sup> and *Ferguson v. City of Charleston*.<sup>57</sup> In *Edmond*, the Court held that highway roadblocks combined with drug-sniffing dogs “whose primary purpose is the discovery and interdiction of illegal narcotics”<sup>58</sup> violate the Fourth Amendment. In *Ferguson*, the Court considered a public hospital’s program of testing urine samples from pregnant patients for drugs to build criminal cases against the women that would induce them to accept substance-abuse treatment. Because “the immediate objective of the searches was to generate evidence for law enforcement purposes,”<sup>59</sup> the Court determined that the program could not be sustained under the special-needs doctrine, and remanded for a determination of whether the patients consented to the searches.

The logic of the primary-purpose limitation is not entirely clear,<sup>60</sup> and whether it will prove workable in multi-purpose search cases remains to be seen,<sup>61</sup> but this development has pulled the rug out from under special-needs balancing for DNA databanks.<sup>62</sup> The convicted-offender databases exist primarily to facilitate the identification of the perpetrators of sexual assaults, murders, and many other crimes. They have some secondary uses, such as identifying missing persons or disaster victims, but criminal investigation is their *raison d’être*. Professor Maclin’s research confirms that this is also the case for arrestee databases. He notes that the sponsors of two DNA-on-arrest laws argued that the practice would protect the public by identifying some serial rapists or murderers before they complete additional rapes or murders.<sup>63</sup> He also notes that the director of one crime laboratory in Louisiana stated, “[t]here’s no doubt in my mind that with arrestee testing...four lives would have been saved. If we had proper arrestee information, [Lee] would have been arrested after the first case.”<sup>64</sup> The same logic has been invoked by the cosponsor of the recently adopted Federal legislation, who pointed to “[a] recent case study produced by the City of Chicago” that found that thirty-one rapes and thirty-two murders “would have been prevented” had DNA from arrestees been checked against crime-scene DNA profiles.<sup>65</sup>

Thus, it appears that Maclin is on firm ground in concluding that the special-needs doctrine (as the Court has most recently articulated it) is a poor fit to DNA databases. Less persuasive, however, is the assertion that “the special needs cases...*forbid* searches that promote criminal law interests.”<sup>66</sup> If one is intent on climbing a mountain, the fact that one route is blocked does not mean that all routes are impassable. The special-needs cases constitute an exception to the warrant requirement – they are one route to a constitutional policy. *Edmond* and *Ferguson* tell us that this route is impassable when the primary purpose of the search is to produce evidence for criminal prosecution. This exception to an exception does not bar all other routes.

As such, it is quite a jump from the proposition that the special-needs exception does not apply to the further conclusion that these databases cannot fairly be reconciled with the Fourth Amendment. Maclin’s “objective analysis” takes the Supreme Court’s cases as a closed set with more or less determinate boundaries. It offers the Court the trichotomy of declaring DNA sampling on arrest to be unconstitutional, upholding the constitutionality of DNA sampling under the special-needs cases, or upholding its constitutionality in an unjustified and *ad hoc* fashion. He has a point. Many courts have resorted to what looks like *ad hoc* balancing of the sort that Maclin denigrates as “standardless”<sup>67</sup> to sustain convicted-offender databases.<sup>68</sup> Without adequately explaining why, they either have abandoned the notion that there needs to be a categorical exception to the warrant requirement, or they have created a *sui generis* exception for convicted-offender DNA databases. These courts maintain that the DNA data are extremely useful in preventing and investigating crime; while the bodily intrusion is minimal, the personal information only reveals individual identity, and the individual’s status as a convicted criminal diminishes his privacy. In this way, they have upheld taking DNA after conviction.<sup>69</sup> There is, however, a fourth alternative – upholding the constitutionality of at least some systems of DNA sampling on the basis of a “biometric identification” exception to the warrant requirement. Part II argues for such an exception.

## II. The Biometric Identification Exception

### A. Defining the Exception

The Supreme Court has never approved the practice of fingerprinting suspects in the course of booking. It has never considered whether other methods of collecting and recording anthropomorphic data on arrestees are constitutional.<sup>70</sup> It has, however, intimated that these practices do not infringe the Fourth Amendment. In *Davis v. Mississippi*,<sup>71</sup> “police, without warrants, took at least 24 Negro youths to police headquarters where

they were questioned briefly, fingerprinted, and then released without charge.<sup>72</sup> Their fingerprints “were sent to the Federal Bureau of Investigation in Washington, D.C., for comparison with the latent prints taken from the window of the victim’s house. The FBI reported that [Davis]’s prints matched those taken from the window.”<sup>73</sup> This identification “was admitted in evidence at trial, over petitioner’s timely objections that the fingerprints should be excluded as the product of an unlawful detention.”<sup>74</sup> The Supreme Court ultimately reversed the resulting conviction because even “[d]etentions for the sole purpose of obtaining fingerprints are...subject to the constraints of the Fourth Amendment”<sup>75</sup> and “the detention at police headquarters...was not authorized by a judicial officer...”<sup>76</sup>

Nevertheless, the Court regarded the fingerprinting for the purpose of generating evidence in a criminal case as such a minimal intrusion on privacy that it might justify detaining a suspect without probable cause. Speaking for the Court, Justice Brennan explained that:

Detention for fingerprinting may constitute a much less serious intrusion upon personal security than other types of police searches and detentions. Fingerprinting involves none of the probing into an individual’s private life and thoughts that marks an interrogation or search. Nor can fingerprint detention be employed repeatedly to harass any individual, since the police need only one set of each person’s prints. Furthermore, fingerprinting is an inherently more reliable and effective crime-solving tool than eyewitness identifications or confessions and is not subject to such abuses as the improper line-up and the “third degree.” Finally, because there is no danger of destruction of fingerprints, the limited detention need not come unexpectedly or at an inconvenient time.<sup>77</sup>

These dicta suggest that the Supreme Court would uphold compulsory acquisition of biometric data<sup>78</sup> from a person when the process is not physically or mentally invasive, when the data are useful primarily to link individuals to crime scenes or to establish the true identity of a given individual, and when the data are valid, reliable, and effective for this purpose. In these circumstances, harms to individuals (outside of the prospect of criminal prosecution based on adequate evidence) and the benefits of judicial review are minor;<sup>79</sup> hence, the balance between individual privacy and government interests points to the reasonableness

of the collection and use of the identifying data without a judicial warrant.<sup>80</sup>

Doctrinally, one can reach the result by regarding the biometric testing as either an investigative practice that is not a Fourth Amendment event (not a “search”), or as a search that is reasonable.<sup>81</sup> It is reasonable, not because of *ad hoc* balancing, but because an entire cat-

---

**With sufficient privacy safeguards in place, an arrestee DNA database could fall within the biometric exception to the warrant requirement.**

---

egory of government conduct is acceptable regardless of the details of the case. Defining a categorical exception for biometric data collection and use is hardly “a ‘Good for This Day and Train Only’ theory.”<sup>82</sup> At the same time, the exception is narrow, and it relieves the pressure to dismiss as non-searches all sorts of data-gathering procedures that are plainly “searches” in the ordinary-language sense of the word<sup>83</sup> and to diminish the scope of the Fourth Amendment as search technologies become less physically invasive and diffuse into public usage.<sup>84</sup> It would not encompass polygraphy even though this procedure relies on biometrics.<sup>85</sup> It would not countenance systems of surveillance cameras combined with automated recognition systems to follow the movements of specific individuals everywhere they go.<sup>86</sup> The surveillance aspect of the biometrics exception is confined to sporadic determinations of an individual’s whereabouts. An automated search of the FBI’s criminal fingerprint database can produce candidates who might have left the latent print found at a crime scene. That is one invasion of what I have called “spatial anonymity,”<sup>87</sup> but it is not the Orwellian vision that motivates some of the criticism of current Fourth Amendment doctrine.

*B. Applying the Exception to DNA Sampling and Databasing*

Suppose, then, that compulsory DNA sampling is considered a Fourth Amendment search – either because of the manner of the sampling (blood is withdrawn from the body, the inside of the cheek is swabbed, or the like) or because the information content of the DNA molecule is thought to warrant this result (a criterion that departs somewhat from current doctrine).<sup>88</sup> Suppose, further, that the special-needs exception cannot sustain the practice because of the primary-purpose limitation on the exception. Can the system nevertheless be deemed reasonable under the limited and distinct biometric exception to the warrant requirement?<sup>89</sup> The proposed exception requires three inquires:

- 1.. *The process is not physically or mentally invasive.* The physical intrusion needed for DNA sampling is minimal, especially if the surface of the skin is not penetrated, and no mental probing is involved.
- 2.. *The data are useful primarily to link individuals to crime scenes or to establish the true identity of a given individual.* The loci used in identification databases are not socially or medically significant. Whether the label “junk DNA” is apt is not important. The pivotal fact is that the few STR loci that are now in use reveal nothing about propensities to disease, behavioral traits, or the like.<sup>90</sup> Of course, the samples themselves encode more sensitive information. If they are retained – a practice that I have questioned elsewhere<sup>91</sup> – strong safeguards would have to be in place to satisfy this condition of the biometric exception.<sup>92</sup>
- 3.. *The data are valid, reliable, and effective for linking individuals to crime scenes or establishing the true identity of a given individual.* The validity and reliability of DNA identification are no longer in contention. Indeed, the base of scientific research on these matters far exceeds that of fingerprinting.

Effectiveness is more complicated. DNA data provide one well-studied mechanism for authentication (establishing the true identity of a given individual).<sup>93</sup> More to the point, they are, in Justice Brennan’s words, “inherently more...effective...than eyewitness identifications or confessions”<sup>94</sup> in placing a given individual at the scene of the crime. However, it is also appropriate to consider “effectiveness” in a broader sense. The major value of DNA databases lies in reducing serious crime. DNA sampling on arrest can do this in two ways. First, an arrestee’s profile can be compared to a database of trace evidence DNA profiles from unsolved crimes. This can be called a “one-to-many” database query in that one arrestee’s DNA record is compared to the many records in the database of trace evidence. A “cold hit” could result in continued pretrial detention, prosecution, and conviction for the unsolved crime. Second, even if no unsolved-crime database exists, the arrestee’s profile can be included in a database of DNA records of arrestees. DNA found at a crime scene or on a victim in an unsolved case could be analyzed and compared to all the potential offender records. This can be called a “many-to-one” query in that the many arrestee records are compared to the one trace-evidence profile. A “hit” in the arrestee database could help solve the new case. However the “hit” comes about, this enhancement in crime-fighting is the major interest that

courts have invoked to uphold convicted-offender databanking<sup>95</sup> and that the proponents of arrestee DNA sampling have advanced.<sup>96</sup> As we have just seen, it runs in two directions. An arrestee who commits crimes after being booked might be linked to those crimes, and an arrestee who has committed other crimes before being arrested might be linked to those past crimes.

Hard data on this type of effectiveness is hard to come by. As noted, some unpublished reports have pointed to instances in which rapes or murders could have been prevented,<sup>97</sup> but no systematic analysis of effectiveness has been conducted in those states that have begun to collect DNA from arrestees.<sup>98</sup> Nevertheless, DNA is probably a more effective form of trace evidence than fingerprints. It can be recovered from many crime scenes or victims,<sup>99</sup> and the numerical STR data lends itself to efficient database queries. In sum, with sufficient privacy safeguards in place, an arrestee DNA database could fall within the biometric exception to the warrant requirement.

### *C. The Supreme Court and the Biometric Identification Exception*

Although *Davis* plants the seed for a generic biometric exception to the warrant requirement, no courts and few commentators have seen fit to discuss it. Professor Maclin’s otherwise comprehensive article pretermits it. Likewise, a recent article by Professor Sandra Carnahan, which insists that “[t]he only logical conclusion is that the national law enforcement DNA database [for convicted offenders] is unconstitutional,”<sup>100</sup> dismisses it in a few sentences:

Given its current constitutional infirmities, however, maintaining CODIS would likely call for the Supreme Court to create a new category of suspicionless searches....Certainly, the Supreme Court may, given the opportunity, create another exception to the Fourth Amendment’s warrant preference. As Professor Kaye notes: “[T]he existing exceptions to the warrant requirement are not ancient specimens of an extinct species frozen in amber. They are living creations whose structures continue to evolve and whose number is not fixed.” Nonetheless, the Court has not created a new exception to the Fourth Amendment in decades, and would likely do so now with great hesitation. The Supreme Court has never approved a suspicionless search involving bodily intrusion for a law enforcement purpose, and to do so here would be a substantial departure from traditional Fourth Amendment principles.<sup>101</sup>

To some extent, this is true. The Court should not make new exceptions lightly. It has properly resisted adding dubious exceptions to the extant species.<sup>102</sup> A biometric-identification exception, however, is more appropriate than the current approach of denying that fingerprinting is a search or pursuing the convoluted logic of finding that its primary purpose is not normal law enforcement, but then countenancing its use for this purpose. These stratagems may work for the moment, but a well cabined exception is more direct and may be valuable in analyzing a variety of biometric identification systems that are being researched and introduced. As for the DNA identification technology,

“there are powerful crime-control reasons for a state to establish DNA databases for convicted offenders or arrestees, the databases can be structured to respect most individual privacy interests, they can be administered fairly, and they can be accommodated with a specific and limited exception to the warrant requirement. Consequently, it is neither heretical nor Quixotic to pose the question whether such an exception should be recognized.”<sup>103</sup>

With the advent of DNA databases for arrestees, the Supreme Court soon may need to answer the question.<sup>104</sup>

#### Acknowledgements

This article was supported by a grant from NIH (R01-HG002836).

#### References

1. See D. H. Kaye, “The Constitutionality of DNA Sampling on Arrest,” *Cornell Journal of Law and Public Policy* 10 (2001): 455-509, at 457-458.
2. The Louisiana law dates back to 1999, and the Virginia statute was enacted in 2002. For descriptions of these statutes and the legislative history, see T. Maclin, “Is Obtaining an Arrestee’s DNA a Valid Special Needs Search Under the Fourth Amendment? What Should (And Will) the Supreme Court Do?” *Journal of Law Medicine and Ethics* 33 (2005): 102-124, at 104-105. Reprinted, *Journal of Law Medicine and Ethics* 34 (2006): \_\_\_\_-\_\_\_\_, at \_\_\_\_\_. The California law came by way of a popular referendum (Proposition 69) in November 2004 extending the DNA and Forensic Identification Database and Data Bank Act of 1998, Cal. Penal Code § 295, to include collection of DNA. See U. Torassa, “San Francisco ACLU Sues to Scrap Prop. 69 and its DNA Databank, Invasion of Privacy Charged; Backers Say Law on Solid Ground,” *San Francisco Chronicle*, December 8, 2004, at B3. The South Dakota law, which has been repealed, provided that “[t]he Attorney General shall procure and file for record genetic marker grouping analysis information from any person taken into custody for [certain criminal] violation[s].” S.D. Codified Laws Ann. § 23-5-14 (1998 & Supp. 2002).
3. Tex. Gov’t Code § 411.1471(a)(2) (2004), authorizing collection of DNA at the same time as fingerprinting in kidnapping, sexual assault, and other cases and providing for destruction of samples and records on acquittal or dismissal of the charges. This provision became effective in 2002.
4. Then Attorney General Janet Reno referred the question to the National Commission on the Future of DNA Evidence, which recommended that arrestee sampling not be undertaken before the backlog of unanalyzed samples from convicted offenders is largely eliminated. This recommendation once appeared at <<http://www.ojp.usdoj.gov/nij/dna/arresttrc.html>> (**Please check this link, it does not work**) on January 16, 2000, as “Recommendation of the National Commission on the Future of DNA Evidence to the Attorney General Regarding Arrestee DNA Sample Collection.” A transcript of the discussion and voting on the recommendation is still *available at* <<http://www.ojp.usdoj.gov/nij/topics/forensics/events/dnamtgtrans5/trans-i.html>> (last visited February 13, 2006).
5. Title X, Pub. L. No. 109-162, 119 Stat. 2960.
6. *Id.* § 1004(a)(1)(A), amending the DNA Identification Act of 1994, 42 U.S.C. § 14132, by providing that “[t]he Attorney General may, as prescribed by the Attorney General in regulation, collect DNA samples from individuals who are arrested or from non-United States persons who are detained under the authority of the United States.”
7. *Id.*, at § 1003, amending the DNA Analysis Backlog Elimination Act of 2000, 42 U.S.C. § 14135(a)(1). The DNA Fingerprint Act of 2005 is part of the Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. 109-162, 119 Stat. 2960. Added in committee by Senators Jon Kyl and John Cornyn (see Cong. Rec. S13756 December 16, 2005, statement of Senator Kyl), the expansion of the Federal database had the firm support of the administration. See R. Willing, “White House Seeks to Expand DNA Database,” *USA Today*, April 15, 2003; Letter from Assistant Attorney General William E. Moschella to the Honorable Arlen Specter Concerning S. 1197, September 29, 2005, at A-33; Letter from Assistant Attorney General William E. Moschella to the Honorable Orin G. Hatch Concerning H.R. 3214, April 28, 2004, at 3-7; Letter from Assistant Attorney General William E. Moschella to the Honorable Orin G. Hatch Concerning S. 1700, April 28, 2004, at 5-6.
8. Maclin, *supra* note 2, at 118.
9. *Id.*
10. *Id.*, at 124, note 261.
11. 533 U.S. 27 (2001).
12. Maclin, *supra* note 2, at 107.
13. *Id.*, at 118.
14. *Id.*
15. For this very argument, see S. J. Carnahan, “The Supreme Court’s Primary Purpose Test: A Roadblock to the National Law Enforcement DNA Database,” *Nebraska Law Review* 83 (2004): 1-37.
16. *United States v. Kincade*, 345 F.3d 1095 (9th Cir. 2003), vacated en banc, 379 F.3d 813 (9th Cir. 2004).
17. 533 U.S. 27 (2001).
18. *Id.*, at 106-107.
19. A 1999 report to the National Commission on the Future of DNA Evidence outlines and applies these three factors to conclude that compelling individuals to surrender DNA samples should be deemed a search within the meaning of the Fourth Amendment. D. H. Kaye, *The Constitutionality of DNA Sampling on Arrest: An Interim Report to the National Commission on the Future of DNA Evidence*, October 1, 1999, *available at* <[www.law.asu.edu/kaye/pubs/genlaw/ncfdna-report1-000122.htm](http://www.law.asu.edu/kaye/pubs/genlaw/ncfdna-report1-000122.htm)> (last visited February 13, 2006). A condensed version appears as D. H. Kaye, “DNA Sampling on Arrest and the Fourth Amendment,” *Government, Law, and Policy* 2 (2000): 38-41, and an expanded and slightly updated version appears as Kaye, *supra* note 1. Lower courts passing on the constitutionality of convicted-offender DNA databases have not hesitated to treat compulsory DNA sampling as a search of the person. These cases are tracked in Robin Cheryl Miller, “Validity, Construction, and Operation of State DNA Database Statutes,” *American Law Reports* 5th 76: 239-88.
20. 410 U.S. 1 (1973).
21. *Id.*, at 14.
22. 389 U.S. 347 (1967).
23. Maclin, *supra* note 2, at 106.
24. 533 U.S. 27 (2001).
25. Maclin, *supra* note 2, at 106.
26. Cf. D. Prosnitz, “WMD Sensors – Search and Seizure,” *Science* 310 (2005): 978-979.

27. Cf., e.g., D. A. Sklansky, "Back to the Future: *Kyllo*, *Katz*, and Common Law," *Mississippi Law Journal* 72 (2002): 143-211, at 144, observing that "[t]he ruling in *Kyllo* was relatively narrow: police officers need a warrant to aim a thermal imaging device at a house."
28. Professor Maclin in particular has explored with great skill and insight the unresolved tension between the broad interpretation of *Kyllo* and other cases. See T. Maclin, "Katz, *Kyllo*, and Technology: Virtual Fourth Amendment Protection in the Twenty-first Century," *Mississippi Law Journal* 72 (2002): 51-142.
29. For recent efforts of commentators to confine the Fourth Amendment's scope to real property concepts, see O. S. Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution," *Michigan Law Review* 102 (2004): 801-888; D. E. Steinberg, "The Original Understanding of Unreasonable Searches and Seizures," *Florida Law Review* 56 (2004): 1051-1096.
30. 533 U.S. at 34-35.
31. See *id.*, at 33, distinguishing "enhanced aerial photography of an industrial complex," which was held not be a search in *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986), on the ground that "we found 'it important that this is not an area immediately adjacent to a private home, where privacy expectations are most heightened,' 476 U.S., at 237, n. 4 (emphasis in original)."
32. See Maclin, *supra* note 28; Sklansky, *supra* note 27.
33. In reality, compulsory DNA sampling is unlike infrared scanning in that it involves removing some cells. Scraping the inside of the cheek with a toothbrush-like implement or having the individual spit into a cup are practical techniques, but they are arguably intrusive enough to be searches under existing cases. This is not because of *Kyllo*; rather, it reflects the Court's "concerns about bodily integrity." *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 617 (1989) (dealing with the sampling of air from the alveoli for breath alcohol testing). See Kaye, *supra* note 1.
34. For a cogent exposition of the bases for heightened protection of the home, see Sklansky, *supra* note 27, at 191-192.
35. Sklansky, *supra* note 28, at 202. Indeed, Professor Sklansky urges a rethinking of the very doctrine that public usage of a technology precludes Fourth Amendment protection against governmental usage. *Id.*, at 210, concluding that "[i]n the long term, sensible interpretation of the Fourth Amendment will require the Court to acknowledge the differences between government surveillance and private snooping, and to abandon the assumption that anything knowingly exposed 'to the public' is therefore fair game for the police."
36. Cf. *On Lee v. United States*, 343 U.S. 747, 754 (1952), stating that "[t]he use of bifocals, field glasses or the telescope to magnify the object of a witness' vision is not a forbidden search or seizure, even if they focus without his knowledge or consent upon what one supposes to be private indiscretions."
37. 476 U.S. 227 (1986).
38. *Id.*, at 229.
39. *Id.*, at 232.
40. *DNA Solutions*, available at <<http://www.dnanow.com/>> (last visited February 13, 2006). The cost of aerial photography is hundreds of dollars per hour. See, e.g., *Aerial Photography*, at <<http://www.austinphoto.com/airinfo.html>> (last visited February 13, 2006), quoting \$200 per hour for helicopter photography. Of course, this comparison might not be decisive. One can argue that notwithstanding its references to *Dow*, *Kyllo* itself points the way to a more restrictive reading of "not in general public use." See *Kyllo*, 533 U.S. at 47 n.5, Justice Stevens, dissenting, noting that the thermal imager at issue was "just an 800-number away from being rented from 'half a dozen national companies' by anyone who wants one." Perhaps one can say, as Maclin did in considering whether *Kyllo* is limited to the home, "[w]hile I agree that in future cases the Court is likely to read *Kyllo*'s holding narrowly, there is nothing in *Kyllo* itself that demands this narrow interpretation." Maclin, *supra* note 28, at 116, note 291.
41. *United States v. Nicolosi*, 885 F. Supp. 50 (E.D.N.Y. 1995). Contra *In re Nontestimonial Identification Order*, 762 A.2d. 1239, 1247 (Vt. 2000).
42. Maclin states that "all loci, coding and noncoding alike, can be used for parentage testing." Maclin, *supra* note 2, at 107 (quoting D. H. Kaye, "Two Fallacies About DNA Databanks for Law Enforcement," *Brooklyn Law Review* 67 (2001): 179-206, at 187). Indeed, they can be used for siblingship testing as well. This would be significant if police had DNA samples from all the individuals whose familial relationships they wanted to test. Inasmuch as testing for siblingship or parentage is not possible with a sample from an arrestee alone, however, the extent to which this possibility implicates a meaningful privacy interest resulting from the practice of DNA sampling on arrest is unclear.
43. *Id.*, at 106.
44. *Id.*, at 107.
45. *Id.* The Court has adopted many devices to avoid denominating information-gathering practices as "searches" just because the information is sensitive. See S. F. Colb, "What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy," *Stanford Law Review* 55 (2002): 119-189; R. Simmons, "From *Katz* to *Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-first Century Technologies," *Hastings Law Journal* 53 (2002): 1303-1358. These avoidance strategies are themselves questionable, however, and they should not apply to the forcible extraction of matter that the individual has not exposed to private parties.
46. See, e.g., *Kyllo v. United States*, 533 U.S. 27, 32 (2001), referring, somewhat disparagingly, to "our doctrine that warrantless searches are presumptively unconstitutional;" *Nat'l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 665 (1989), observing that "we have often emphasized, and reiterate today, that a search must be supported, as a general matter, by a warrant issued upon probable cause;" *Mincey v. Arizona*, 437 U.S. 385, 390 (1978), asserting that "[t]he Fourth Amendment proscribes all unreasonable searches and seizures, and it is a cardinal principle that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment - subject only to a few specifically established and well-delineated exceptions,'" quoting *Katz v. United States*, 389 U.S. 347, 357 (1967) (footnotes omitted); *Terry v. Ohio*, 392 U.S. 1, 20 (1968); *Trupiano v. United States*, 334 U.S. 699, 705 (1948). But see T. Maclin, "The Central Meaning of the Fourth Amendment," *William & Mary Law Review* 35 (1993): 197-249, at 199-200, 206, asserting that despite these declarations, "law enforcement officials rarely must comply with the procedural safeguards of the amendment's Warrant Clause.... Instead, [i]f the Court can identify any plausible goal or reason that promotes law enforcement interests, the challenged police intrusion is considered reasonable" and predicting that "for the foreseeable future, the rational basis model likely will remain the constitutional test for judging government intrusions, whereas the importance and need to obtain warrants likely will continue to decline".
47. *Terry v. Ohio*, 392 U.S. 1 (1968).
48. *Illinois v. LaFayette*, 462 U.S. 640 (1983).
49. *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976), upholding warrantless vehicle stops and interrogation at a fixed checkpoint sixty-six miles from the border.
50. *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987), quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Justice Blackmun, concurring).
51. Maclin, *supra* note 2, provides a lucid exposition of these cases.
52. See *United States v. Kincade*, 379 F.3d 813, 822-823 (9th Cir. 2004) (en banc), distinguishing among searches at "exempted areas," "administrative" searches, and "searches [for] 'special needs'"; Maclin, *supra* note 2, at 107-08, differentiating "as a doctrinal matter" between "the special needs cases...and the administrative search cases." But see D. A. Sklansky, "Police and Democracy," *Michigan Law Review* 103 (2005): 1699-1830, at 1735, pointing out that "the administrative search doctrine was broadened into the 'special needs' doctrine, applying relaxed standards to searches by public school teachers, government office managers, and so on."

53. *National Treasury Employees Union v. Von Raab*, 489 U.S. 656, 665-666 (1989).
54. Kaye, *supra* note 1, at 492, elaborating on this theory. Whether the Court has been sufficiently rigorous in its balancing is another matter. See Maclin, *supra* note 46.
55. See, e.g., *Roe v. Marcotte*, 193 F.3d 72, 79 (2d Cir. 1999), holding a convicted-sex-offender database constitutional under “a reasoned interpretation of the ‘special needs’ doctrine” where the special need was said to be the prevention of recidivism; *State v. Olivas*, 856 P.2d 1076, 1088 (Washington 1993), upholding a statute convicted-offender statute under the special-needs theory rather than relying on the theory that “the privacy rights of convicted persons” are “diminished.”
56. 531 U.S. 32 (2000).
57. 532 U.S. 67 (2001).
58. 531 U.S. at 34.
59. 532 U.S. at 83.
60. See Kaye, *supra* note 1, at 494-495, observing that “it seems odd to maintain that the balance of interests permits dispensing with warrants or individualized suspicion when non-law-enforcement interests alone are pursued, but not when both law enforcement and non-law enforcement interests reinforce each other.”
61. See D. H. Kaye, “Two Fallacies About DNA Databanks for Law Enforcement,” *Brooklyn Law Review* 67 (2001): 179-206, describing a possible “frontal assault” on the primary-purpose test.
62. See S. J. Carnahan, *supra* note 15; Kaye, *supra* note 61; M. Rothstein and S. Carnahan, “Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks,” *Brooklyn Law Review* 67: (2001): 127-170; J. Kravis, “A Better Interpretation of ‘Special Needs’ Doctrine after Edmond and Ferguson,” *Yale Law Journal* 112 (2003): 2591-2598.
63. Maclin, *supra* note 2, at 115-116.
64. *Id.*, at 105.
65. See Senator Jon Kyl Press Office, Press Release, *Judiciary Committee Adds Kyl DNA Bill to Violence Against Women Act* (September 8, 2005), available at <<http://kyl.senate.gov/record.cfm?id=245432>> last visited February 13, 2006). In relevant part, the press release reads: “In early 1993, [Andre] Crawford was arrested for felony theft. Under the DNA Fingerprint Act, DNA could have been taken from him at that time and kept in NDIS [the national DNA database]. Because it was not, when Crawford murdered a 37-year-old woman in September 1993, although he left DNA at the scene, he could not be identified as the perpetrator. Over the next six years, Crawford went on to commit one rape and to murder ten more women between the ages of 24 and 44. If Crawford’s DNA sample had been taken and kept in NDIS after his March 1993 arrest, he could have been identified and arrested after the September 1993 murder, and ten more murders and one rape would have been prevented. The Chicago study examines 7 other serial rapists, and concludes that 30 rapes and 22 murderers committed by these perpetrators could have been prevented by an all-arrestee database.” The Chicago cases are described more fully in the *Congressional Record*, July 29, 2005, at S9529-S9531 (statement of Senator Kyl).
66. Maclin, *supra* note 2, at 108 (emphasis added).
67. *Id.*, at 124 note 261.
68. See, e.g., *United States v. Kincaid*, 379 F.3d 813 (9th Cir. 2004) (en banc); *State v. Raines*, 857 A.2d 19 (Md. 2004). Another unpalatable strategy is to rely on the theory a conviction ipso facto works a forfeiture of Fourth Amendment rights. See D. H. Kaye and M. E. Smith, “DNA Identification Databases: Legality, Legitimacy, and the Case for Population-wide Coverage,” *Wisconsin Law Review* (2003): 413-459, at 417-419.
69. See, e.g., *United States v. Sczubelek*, 402 F.3d 175, 184-187 (3d Cir. 2005), applying these factors under a “totality of circumstances” reasonableness standard to uphold compelling a federal probationer to submit to DNA sampling; *Padgett v. Donald*, 401 F.3d 1273, 1280 (11th Cir. 2005), same reasoning with regard to a Georgia convicted-offender statute.
70. For the views of the circuit courts, see, e.g., *Napolitano v. United States*, 340 F.2d 313, 314 (1st Cir. 1965), “Taking of fingerprints [prior to bail] is universally standard procedure, and no violation of constitutional rights;” *Smith v. United States*, 324 F.2d 879, 882 (D.C. Cir. 1963), “[I]t is elementary that a person in lawful custody may be required to submit to photographing...and fingerprinting...as part of routine identification processes.”
71. 394 U.S. 721 (1969).
72. *Id.*, at 722.
73. *Id.*, at 723.
74. *Id.*
75. *Id.*, at 727.
76. *Id.*, adding that “petitioner was unnecessarily required to undergo two fingerprinting sessions; and petitioner was not merely fingerprinted during the [first] detention but also subjected to interrogation.”
77. *Id.* Fingerprinting following an arrest for which there is probable cause to detain the suspect should be even less objectionable.
78. Biometrics are measurable physiological or behavioral characteristics that can be used to verify the identity of an individual. (In an older and more general usage, the term “biometrics” refers to measuring and statistically analyzing any biological data.) Physiological characteristics that have been used or studied in biometric identification or authentication systems include features of the iris, fingerprints, hand, face, voice, retina, odor, earlobe, sweat pores, lips, and DNA. Behavioral characteristics are manifested in such activities as writing, keystroking, speaking, and walking. Biometric identification or authentication systems are essentially pattern recognition systems.
79. For an analysis of the very limited value of judicial warrants for routine sampling on arrest, see Kaye, *supra* note 1.
80. The balancing, in the context of DNA identification profiling, is discussed further in Kaye, *supra* note 1.
81. *Davis* itself concerns the reasonableness of the detention of a suspect – the seizure of a person. The dicta seem to allow this seizure for the “nontestimonial” purpose of fingerprinting or even of obtaining a blood sample if a judicial officer determines that the state has reasonable suspicion to believe that the sample would link the suspect to the crime. The DNA-on-arrest laws discussed here are quite different. They contemplate collecting and storing DNA from a person even when there is no reasonable basis to suspect that the DNA will link the individual to the offense for which the arrest was made. Nevertheless, the logic of *Davis* is that collecting the biometric data (in that case, the fingerprints) is so limited an invasion of bodily integrity and privacy and that it is sufficiently valuable in generating evidence that it can justify the seizure of the person. These same considerations probably would lead the Court to conclude that, as to persons who are legitimately placed in custody, routine fingerprinting for the purpose of building a database or checking against latent fingerprints from unsolved cases is a reasonable search even without a warrant and individualized suspicion. If so, the Court would have to declare one of two things: (1) that fingerprinting is not even a search, or (2) that it is a reasonable search because it falls within a previously unarticulated exception to the warrant requirement.
82. Maclin, *supra* note 2, at 124, note 261, reprinted this volume at \_\_\_, note \_\_\_.
83. For an expression of this concern, see, e.g., Christopher Slobogin, “Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity,” *Mississippi Law Journal* 72 (2002): 213-315, advocating Fourth Amendment protection for the operation of public surveillance cameras.
84. On the issue of invasiveness, see, e.g., R. Simmons, “From *Katz* to *Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-first Century Technologies,” *Hastings Law Journal* 53 (2002): 1303-1358.
85. A fortiori, it would not include the hypothetical “brain wave recorder” posited in S. F. Colb, “A World Without Privacy: Why Property Does Not Define the Limits of the Right Against Unreasonable Searches and Seizures,” *Michigan Law Review* 102 (2004): 889-903. These techniques do not fulfill the first or second requirements of the categorical exception.
86. For commentary arguing that such systems such be classified as searches and thereby subject to Fourth Amendment scrutiny, see, e.g., M. J. Blitz, “Video Surveillance and the Constitution of Pub-

- lic Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity," *Texas Law Review* 82 (2004): 1349-1422; J. J. Brogan, "Facing the Music: the Dubious Constitutionality of Facial Recognition Technology," *Hastings Communications & Entertainment Law Journal* 25 (2002): 65-96; R. H. Thornburg, "Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment," *John Marshall Journal of Computer and Information Law* 20 (2002): 321-346; cf. Slobogin, *supra* note 83.
87. D. H. Kaye and M. E. Smith, "DNA Identification Databases: Legality, Legitimacy, and the Case for Population-wide Coverage," *Wisconsin Law Review* (2003): 413-459.
88. See, e.g., Simmons, *supra* note 84.
89. It is not strictly necessary to invoke the biometric exception for fingerprinting in the course of a custodial arrest. Historically, the practice arose from the need to establish the true identity of the arrestee for administrative purposes. See Kaye, *supra* note 1. Originally, computer-searchable databases of fingerprints were not available. The system having been instituted for purposes other than generating evidence for use in a criminal case, standard doctrine would allow the secondary use. If, however, the proposal to realign or jettison the subsequent-use doctrine advanced in H. J. Krent, "Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment," *Texas Law Review* 74 (1995): 49-100, were adopted, the exception might be necessary to sustain the practice of collecting fingerprints on arrest for administrative purposes and then turning around and using them to solve cases in which fingerprints provide trace evidence. Certainly, deciding on whether there should be a biometric exception that would justify the secondary use is more satisfying than the two-step subsequent-use analysis. The latter simply avoids a frank balancing of the relevant interests in favor of the government's power to search.
90. Neither do arrestee databases lend themselves to routine parentage testing. See *supra* note 42.
91. D. H. Kaye, "Behavioral Genetics Research and Criminal DNA Databanks," *Law and Contemporary Problems* 69 (2006) (in press).
92. "Front-loaded" and "back-loaded" systems to protect genetic information are discussed in Kaye, *supra* note 1.
93. They are somewhat less discriminating than fingerprints, since they do not distinguish between monozygotic twins.
94. *Davis*, 394 U.S. at 727.
95. See, e.g., *Boling v. Romer*, 101 F.3d 1336, 1340 (10th Cir. 1996), noting "the legitimate government interest in the investigation and prosecution of unsolved and future criminal acts by the use of DNA in a manner not significantly different from the use of fingerprints."
96. See *supra* notes 63-65.
97. See *supra* notes 63-65.
98. As of November 30, 2005, the state of Virginia had assembled DNA profiles from 236,511 convicted felons. These produced some 2,617 hits, a little more than one percent. The arrestee database does not grow in the same manner, for profiles are removed when prosecutions do not proceed to convictions or when defendants plead guilty to misdemeanors. These events occur in about half of all felony arrests, and the arrestee database has been hovering at around 4,000. The cumulative number of hits in this database is 233, or about six percent. E-mail from Dr. Paul Ferrara to D. H. Kaye, December 5, 2005. Of course, the two percentages are not directly comparable; removing profiles from the arrestee database decreases the denominator of the proportion of hits, and increases the resulting percentage. Moreover, for many reasons, hits in both groups do not always produce convictions. See R. Willing, "DNA Matches Win Few Convictions in Va.," *USA Today*, November 7, 2005, reporting that "Virginia's crime lab has found there were convictions in less than one-quarter of more than 3,000 cases in which analysts matched crime-scene DNA to a genetic profile in the state's databases." It would be interesting to know how many of the arrestee hits came from records that have been expunged. Expungement reduces the effectiveness of these databases, at least to some extent, and it is not obvious that the Fourth Amendment necessitates expungement. Cf. *Hodge v. Jones*, 31 F.3d 157 (4th Cir. 1994), holding that, given the state's interest in maintaining a computerized database of investigations of child abuse, the constitution does not require the files of parents who had been investigated and cleared of child abuse charges to be removed from the database. Also missing is information on how many of the people who are arrested already were represented in a convicted-offender database. Presumably, they were not included in the arrestee database, but their DNA might have produced hits had it been collected and analyzed at the time of their first arrest.
99. A pilot project in New York produced eighty-six DNA profiles from 201 burglaries (forty-three percent). National Institute of Justice, "DNA in 'Minor' Crimes Yields Major Benefits in Public Safety," November 2004, available at <<http://www.ncjrs.org/pdffiles1/nij/207203.pdf>> (last visited February 13, 2006).
100. Carnahan, *supra* note 15, at 37; cf. E. Curtis, "An Unwarranted Intrusion: the Constitutional Infirmities of Washington's DNA Collection Law," *Washington Law Review* 80 (2004): 447-476, arguing that the Washington state convicted-offender DNA law violates the state constitution because it compels searches that do not fall into one of the previously recognized exceptions.
101. *Id.*, at 35.
102. See, e.g., *Mincey v. Arizona*, 437 U.S. 385, 390 (1978).
103. Kaye, *supra* note 1, at 499.
104. See J. A. Alfano, "Look What Katz Leaves Out: Why DNA Collection Challenges the Scope of the Fourth Amendment," *Hofstra Law Review* 33 (2005): 1017-1047.