7

Judicial Imaginaries of Technology: Constitutional Law and the Forensic DNA Databases

David E. Winickoff

The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.
—Justice Antonin Scalia, *Kyllo v. United States* (2001)

As two powerful epistemic institutions, law and technoscience work together in sustaining models of the individual and society and in producing ruling classifications and categories (Jasanoff 2008). An important case in point concerns new technologies of surveillance and their encounters with the Fourth Amendment of the U.S. Constitution. This "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" has steadily evolved through confrontations between civil liberties claims and advances in wiretapping, aerial photography, and increasingly sensitive microphones (Power 1989). Although STS scholars have closely tracked the bumpy process of bringing forensic DNA evidence into the courtroom (Aronson 2006; Lynch et al. 2008), they have not yet addressed the constitutional review of DNA collection for use in large-scale searchable databases. Merging the biological and informational, forensic DNA databases are reshaping legal understandings of security, freedom, and identity. These evolving tools are also restructuring the relations of criminal bodies and bodies politic. In short, they are deeply implicated in what this volume identifies as the evolving bioconstitutional order.

Forensic DNA databases have expanded considerably in size and scope since their inception in the early 1990s. Individual U.S. states began enacting forensic DNA data banking statutes before football star O. J. Simpson and DNA analyses of his blood infamously went to trial in 1994, and before admissibility standards for DNA evidence became stabilized. By 1999, all fifty states had enacted statutes providing for the mandatory DNA banking of blood or saliva samples from those convicted of certain

felonies (Bieber 2004). Though most of these databases were originally slated to include only persons convicted of serious sexual offenses and violent crimes, many have expanded over the years to include all convicted felons and even all arrestees: as of September 2009, fourteen states were collecting samples for their databases from many people who are merely arrested (Biancamano 2009). The U.S. government has begun collecting DNA samples from all citizens arrested in connection with any federal crime and from many immigrants held by federal authorities, which is likely to add more than one million individuals per year to the federal database (Nakashima and Hsu 2008). These state and federal databases are connected through a digital network coordinated by the FBI. This network, called CODIS (Combined DNA Index System), enables federal, state, and local crime labs to exchange and compare DNA profiles electronically, thereby linking samples found at crime scenes to other samples and, by extension, to the individuals whose samples are in the database.

Although many new forms of technological surveillance and restraint have tended to evade significant judicial review (Murphy 2008), this is not the case for large-scale forensic DNA databases. Since the 1992 case of *Jones v. Murray*, judges in the federal circuit courts of appeal have confronted Fourth Amendment challenges to the system of searches and seizures authorized under DNA database legislation and the CODIS system. These encounters have not only unsettled, but actively reconfigured, the scope of civil liberty and the doctrinal architecture of the Fourth Amendment. None of these Fourth Amendment challenges at the circuit level has succeeded, but the doctrinal dispensation of the cases has varied widely. This variability presents a good opportunity for comparison. Previous work has shown how theories and narratives of technology shape public decision making and cultural history (Wynne 1988; Callon 1987; Hughes 2004). But how do new biotechnological imaginations work their way into the legal and social order? A detailed focus on case law will be necessary to answer this question, precisely because a bioconstitutionalist research design rejects hasty generalizations and asks for attention to details, translations, and transformations.

The cases discussed here illustrate how judges determine what constitutes due process against tacit and explicit background understandings of technological risk. The decisions deploy different Fourth Amendment doctrines in effect as a form of risk management in order to control the imagined hazards of these forensic searches in silico. Constitutional legitimization of the new DNA databases thus has depended upon what I call "judicial imaginaries of technology"—including tacit analogies, framing,

models of social adoption of technology, and risk assessment. Technological imaginaries are at once ontologies, theories, sociologies, and narratives of technoscience that enable and construct social order (Jasanoff and Kim 2009). In the Fourth Amendment cases, the technological imaginaries of judges condition their doctrinal choices and the terms of technological adoption even as they help produce new categories of criminal subjects.

The Fourth Amendment

Infrared goggles, wiretaps, electronic bugs: these are the mainstays of Fourth Amendment doctrine as found in first-year law textbooks. It is here that judges consider whether new surveillance technologies violate the traditional Constitutional rubric: "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 seized."

Throughout the recent history of the Fourth Amendment, judges have struggled to define the boundaries of privacy in the face of changing technological and social norms. In *Katz v. United States*, the seminal case in modern search and seizure law, the court held that a police activity requires a warrant, or a special exception to a warrant, if it occurs in a place where the person had a "reasonable expectation of privacy."[1] Jurists have pointed out that privacy may tend to erode if reasonable expectations change, as indeed they have eroded in the era of information explosion.

In particular, since 1992, courts have refereed the confrontation of CODIS and the Fourth Amendment. As a result, through inevitable processes of normative and epistemic coproduction, novel conceptions of privacy and new criminal kinds, or definitions of what constitutes a criminal, have emerged. By allowing law enforcement officers to search existing DNA samples left at crime scenes against a large database of profiles, CODIS promises an efficient way of connecting individuals to crimes without a physical roundup or questioning. In the eyes of police and prosecutors, it amounts to a powerful law enforcement tool, a huge roundup at a click whose intrusiveness is minimal, electronic, and virtual. The legal claim made by convicts, parolees, and others included or slated for inclusion in a forensic database is that the new forensic DNA statutes mandate activities that constitute an unreasonable search or seizure under the Fourth Amendment. Such activity includes blood draws or other sampling without consent, banking of samples, creation of a genetic profile

based on the sample, and inclusion of profiles within a network subject to repeated electronic scans.

None of the activities cited in the Fourth Amendment cases were being pursued with search warrants. Assuming these activities would be deemed "searches" under the amendment, would they then qualify for one of the traditional exceptions to the rule? This question has not been consistently answered by the courts, not just because of different conceptions of the technology but also because of disagreements about the scope of privacy in the face of police power.

The first clause of the Fourth Amendment is referred to as the "reasonableness" clause. Its exact relationship to the "warrant clause" is not made clear in the amendment itself, which has raised a disagreement in interpretation. Painting with broad strokes, there are two competing theories about how the two clauses relate (Bradley 1993). One theory holds that the warrant clause defines and gives meaning to the reasonableness clause (Maclin 1994, 33). According to this view, a warrant is required for every search and seizure, as long as it is "practicable" to obtain one. This view depends on what the Supreme Court has described as the "cardinal principle"[2] of the Fourth Amendment, namely 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."[3] The second and opposing viewpoint emphasizes that the Constitution's preference for warrants is a judicial construct rather than a textual requirement.[4] Advocates of this model contend that the warrant clause does not and should not inform the reasonableness clause. In this view, the reasonableness clause encompasses all searches and seizures, and requires only that such searches and seizures be "reasonable," taking into consideration all the relevant factors.

One issue not in dispute is that the doctrine of "probable cause" serves to mediate between these two positions. The existence of a "cause" that justifies the issue of a warrant disciplines both the issuing judge and the searching authority. And regardless of whether a warrant has been issued for a search of a "protected zone" of privacy, searches are almost always deemed unreasonable unless "the facts and circumstances" known by the searcher "are sufficient in themselves to warrant a person of reasonable caution in the belief" that the search will lead to evidence of a crime.

The paradigmatic rule *seems* to be one of requiring a warrant, and that a search without a warrant is deemed intrinsically unreasonable and unconstitutional unless one of the exceptions to the warrant requirement

is demonstrated. Another way of stating this is that though there is no warrant *requirement*, there is a constitutional *preference* for warrants. Exceptions exist, but a showing of "probable cause" or "reasonable suspicion" is needed to sustain the constitutionality of searches that seek to invoke one of the exceptions. Only one warrant exception does not require a showing of some sort of individualized suspicion, and that is the "special needs" exception that is invoked by some of the DNA database cases detailed shortly.

Indeterminacy in the Courts

Judges have disagreed about how forensic DNA databases engage with the doctrinal framework of the Fourth Amendment. Although courts have faced the same constitutional questions—similar statutes and nearly identical legal precedents—they have proposed three different doctrinal classifications in deciding these cases: *reasonableness*, *special needs*, and *individualized suspicion*. In short, there has been strong judicial indeterminacy, pointing toward divergent judicial imaginaries. The three positions are illustrated by leading cases from three federal circuits: *Jones v. Murray* (4th Cir. 1992), *Roe v. Marcotte* (2nd Cir. 1999), and *U.S. v. Kincade* (9th Cir. 2003), reheard *en banc*[5] in 2004 (referred to as *Kincade II* in what follows).

"Totality of the Circumstances"

The earliest federal appellate case to consider the Fourth Amendment constitutionality of a forensic DNA database statute is *Jones v. Murray*[6] in 1992, and this case became the leading exemplar of the so-called reasonableness or totality of the circumstances approach. Most other courts have taken this approach and found that forensic DNA statutes survive constitutional scrutiny. In *Jones*, six inmates from the Tazewell Correctional Unit Number 31 challenged the Virginia DNA database legislation requiring convicted felons to submit blood samples for DNA analysis. The inmates argued that coerced extraction of blood violated the rule against unreasonable searches and seizures. The court upheld the district court's view that the DNA statute did not violate the Fourth Amendment rights of the inmates.

True to the traditional doctrinal scheme of such inquiries, the court first considered whether this governmental activity intruded upon a traditionally protected zone of privacy, a question that it answered affirmatively. Writing for the majority, Judge Niemeyer stated that "the bodily

intrusion resulting from taking a blood sample constitutes a search within the scope of the Fourth Amendment" (*Jones*, 306). The inmates argued that *all* governmental searches conducted in the context of criminal law enforcement require a warrant, or at least some sort of "individualized suspicion," but the court rejected the application of such a rule to the case at hand. They had "not been made aware of any case establishing a *per se*" rule requiring probable cause for a "limited search" conducted "for the purpose of ascertaining and recording the identity of a person who is lawfully confined to a prison" (306).

The court reasoned that "probable cause" supplied the basis for bringing the person within the criminal justice system, and "with the person's loss of liberty upon arrest comes the loss of at least some, if not all, rights to personal privacy otherwise protected by the Fourth Amendment." The court next stated another general rule that "when a suspect is arrested upon probable cause, his identification becomes a matter of legitimate state interest and he can hardly claim privacy in it" (306). Citing the example of fingerprint and other "booking" procedures for every suspect arrested for a felony, the court wrote that "the identification of suspects is relevant not only to solving the crime for which the suspect is arrested, but also for maintaining a permanent record to solve other past and future crimes" (306).

The court next went directly to the "balancing test" required of many reasonableness judgments in the law, weighing the significance of the intrusion to privacy against the government's interest "in preserving a permanent identification record of convicted felons for resolving past and future crimes" (*Jones*, 307). In order to do this, however, the court had to justify its departure from the typical Fourth Amendment scheme of a per se requirement of at least "probable cause" for a particular crime. Accordingly, in footnote 2, the court explained: "Because we consider the cases which involve the Fourth Amendment rights of prison inmates to comprise a separate category of cases to which the usual per se requirement of probable cause does not apply, there is no cause to address whether the so-called "special needs" exception, relied on by the district court applies in this case" (307n2). In other words, the doctrinal choice to bypass the warrant requirement turns in part on the argument that prison inmates as a class have diminished rights in comparison to those of free and innocent citizens.

The court seems to suggest that arrestees held with "probable cause" forfeit any privacy interest in their "identification," which encompasses the inclusion of DNA samples in databases. Furthermore, prison inmates are

considered a class of persons for whom finding individual probable cause of new crimes is not even required: their Fourth Amendment privacy has been diminished upon conviction and confinement. Here, the implication is that the government interest in maintaining the database outweighs the privacy interests of convicted criminals. Accordingly, the intrusion to privacy and the government's interests can be balanced and weighed without imposing the mechanisms of the probable cause or warrant requirement. In *Jones*, the court concluded that the level of intrusion was minimal, whereas the state's interests were significant. Many courts since *Jones* have used this reasoning, and the balancing has always come out the same way.[7] In these cases, prisoners constitute a de facto permanent class of "usual suspects."

Jones v. Murray is of interest not only for its majority opinion, but also for a strongly worded dissent from Judge Murnaghan. Because this dissent shaped how subsequent circuit courts have addressed these cases, it is important to review his position. Judge Murnaghan concurred with the *Jones* majority to the extent that it upheld the Virginia statute "as applied to violent felons," but he dissented from "the majority's determination of the constitutionality of the statute as applied to prisoners convicted of non-violent crimes" (*Jones*, 311). Judge Murnaghan argued that although precedent established that prisoners "give up specific aspects of their reasonable expectation of privacy," these forfeitures have been necessitated by "practical concerns relating to living conditions" and "ensuring prison security" (312). These are limited exceptions to a privacy rule that protects prisoners as much as free citizens against unjustified intrusions: "Prisoners do not lose an expectation of privacy with regard to blood testing, and the Commonwealth's articulated interest in the testing of non-violent felons does not counter-balance the privacy involved in the procedure" (311).

Harkening back to concerns about generalized and overbroad search warrants, he states that "there exists no blanket authorization of searches involving intrusions under the skin, for which no individual, whether in prison or out, loses a reasonable expectation" (*Jones*, 311). Murnaghan recognizes that the majority's opinion ratifies systematic deprivation of a Fourth Amendment expectation of privacy of those in prison.

In making a substantive distinction between the constitutionality of searches with respect to violent versus nonviolent offenders, Judge Murnaghan relied heavily on statistical studies of criminal recidivism. Murnaghan cited a Virginia governmental report that came into the record, the Report of the Joint Subcommittee Studying Creation of a DNA Test Bank. He noted that the Report concluded only that "the recidivism

data supported the inclusion of plaintiffs convicted for felony sex offenses, assault, capital murder, first and second degree murder, voluntary manslaughter, larceny and burglary" (314).

Nonetheless, the report recommended the testing of *all* remaining felons, not because such testing would be likely to help solve crimes, but only because their inclusion would make the data bank "more efficient and cost effective" (Virginia Joint Subcommittee 1990). Judge Murnaghan pointed out that a similar rationale could be used to justify the inclusion of any citizen if it lessened the state's workload.

"Special Needs"

When the Second Circuit Court encountered the virtual roundup in 1999, Judge Murnaghan's dissent in *Jones* helped convince the court to choose a different theory of constitutionality for the DNA databases. In the case of *Roe v. Marcotte*, a group of convicted sexual offenders challenged the constitutionality of a Connecticut statute that, among other things, required all convicted sexual offenders to submit a blood sample for analysis and inclusion in the state DNA databank. Relying on arguments set out in Murnaghan's dissent, the court came to the same result as *Jones* but used a different legal doctrine.

Writing for the unanimous three-member panel in *Roe v. Marcotte*, Judge Poole declared that Judge Murnaghan's analysis "provides a more compelling rationale for upholding the DNA statute's constitutionality than does the *Jones* majority opinion."[8] Indeed, Judge Poole repeated Murnaghan's acerbic critique of the *Jones* majority's "strikingly truncated view of the Fourth Amendment protections afforded to a convicted felon" (*Roe*, 81).

The Second Circuit shared Murnaghan's concern at least enough to require a finding that the case at hand fall within an established exception to a per se rule of probable cause. The court recites the rule that "in general, searches performed in the absence of a warrant and pursuant to an exception must nevertheless be predicated upon 'probable cause to believe that the person to be searched has violated the law,' or at the very least, 'some quantum of individualized suspicion.'"[9] Rather than moving directly ahead to a balancing test, as the *Jones* court did on the idea that all prisoners lose their "expectation of privacy," the *Roe* court attempted to preserve the presumption against warrantless and suspicionless searches, even for incarcerated prisoners.

The *Roe* court explained that an exception to this "individualized suspicion" rule applicable in the case at hand was the so-called special

needs doctrine, which states: "In certain circumstances, generally outside the traditional law enforcement setting, a search may be reasonable even when predicated upon less than probable cause or individualized suspicion where 'special needs, beyond the normal need for law enforcement render those requirements impracticable'" (*Roe*, 77). If courts determine that the searches in question qualify under this exception, then and only then may they proceed to a balancing analysis for "reasonableness."

But this doctrine is reserved for those "special needs, beyond the normal need for law enforcement." In order to make the case that the DNA database program constituted such a special need, the *Roe* court looked to a 1987 Supreme Court case, *Griffin v. Wisconsin*.[10] In *Griffin*, the Supreme Court reasoned that a state's operation of a probation system looked sufficiently like its operation of schools, government offices and prisons––other situations in which the special needs reasoning had been used to justify generalized regulatory searches. In discussing this precedent, the *Roe* court singled out one piece of the Supreme Court's reasoning in particular, namely empirical "research that indicated that more intensive supervision of probationers reduced recidivism" (*Roe*, 79). The *Roe* majority seized upon the idea that the aim of reducing recidivism helped the Wisconsin statute qualify for a "special needs" exemption.

After its discussion of *Griffin*, the *Roe* court concluded that the statute indeed passed constitutional muster, stating that "a reasonable interpretation of the 'special needs' doctrine supports the constitutionality of the DNA statute" (79). The court proceeded with a balancing test of the interests implicated by the statute. Motivated by the concerns of Judge Murnaghan in his *Jones* minority opinion, the *Roe* majority pointed first and foremost to social science suggesting that the database would be especially efficacious with respect to the included populations: "In defense of the statute, defendants cite studies indicating a high rate of recidivism among sexual offenders. Moreover, DNA evidence is particularly useful in investigating sexual offenses and identifying the perpetrators because of the nature of the evidence left at the scenes of these crimes and the demonstrated reliability of DNA evidence" (79). Balanced against these interests, and a general interest in deterring crime, the court assessed "an intrusion that the Supreme Court has characterized as minimal," namely the "drawing for blood for testing."[11] Notably, the *Roe* court diverged from the *Jones* analysis by specifically considering statutory safeguards enacted "to ensure that the intrusion is minimal," including regulations on the handling and analysis of blood, restriction of access to and confidentiality of the database, and provision for expungement of the profile from

the database after reversal or dismissal of a conviction (80). Nevertheless, the *Roe* court concluded that the special needs balancing weighed in favor of constitutionality, a result that many other courts have followed.

"Individualized Suspicion"

Just as the majority of federal and state courts were settling into a pattern of affirming the constitutionality of forensic DNA database statutes, the Ninth Circuit dropped a bombshell in October 2003. In *United States v. Kincade (Kincade I)*, a three-judge panel of the Ninth Circuit ruled that the DNA Analysis Backlog Elimination Act (DABEA), the federal DNA statute enacted in 2000, was unconstitutional under the Fourth Amendment.[12] The decision caused a firestorm in the law enforcement community and among forensic scientists. Importantly, this decision was vacated soon after and the case was reheard *en banc* by the full Ninth Circuit (*Kincade II*). A plurality opinion reversed the first decision, declaring that the DABEA passed constitutional muster after all.[13] But in his majority opinion in *Kincade I*, and in his dissent in *Kincade II*, Judge Reinhardt strongly articulated a third possible doctrinal treatment for forensic DNA databases.

In the *Kincade* cases, a parolee appealed from a sentence imposed by the district court for his refusal to comply with a compulsory blood extraction pursuant to the DABEA. The three-judge panel split 2–1, with Judge Reinhardt, known to be a strong supporter of civil liberties, writing on behalf of Judge Paez for the majority and Judge O'Scannlain writing a strong dissent. The main holdings of the case were twofold: (1) "forced blood extractions from parolees pursuant to the database act required individualized suspicion" and (2) the "special needs doctrine" did not apply.[14]

The legal reasoning in *Kincade I* began, as all the others, by asserting that searches requiring mandatory blood extraction constitute an intrusion into an area, the body, normally protected by the Fourth Amendment. But Judge Reinhardt went further in characterizing the social significance of this intrusion, stating, "In virtually every culture in the world, human blood possesses great symbolic power, and its spillage—whether in a drop or in a torrent—has carried enormous cultural significance. Throughout history, we have waged war, organized societies and religions, and created myths based upon the substance."[15] That opening remark laid the groundwork for a centerpiece of Reinhardt's argument, namely that the analogy between fingerprinting and blood draws is a "false" one. The differences between fingerprinting, which requires the "examination or recording of physical attributes that are generally exposed to public view," and DNA

profiling, requiring a "forced intrusion into an individual's body," are constitutionally significant (*Kincade I*, 1100).

According to Judge Reinhardt in *Kincade I*, the nature of the intrusion triggered a typical Fourth Amendment analysis. But rather than jumping to a formal analysis of whether DABEA falls within a legitimate exception to a warrant requirement, Judge Reinhardt conducted a balancing test. Unlike nearly every other court, this opinion characterized the intrusion as "substantial," emphasizing bodily integrity as a "cherished value of society," and that parolees' privacy rights in their bodies, though diminished, were not extinguished (*Kincade I*, 1102). But neither were they absolute. Reinhardt stated that the purpose of obtaining samples

> is to further "the overwhelming public interest in creating a comprehensive nationwide DNA bank that will improve the accuracy of criminal prosecutions" for generations to come. It is undoubtedly true that, were we to maintain DNA files on all persons living in this country, we would even more effectively further the public interest in having efficient and orderly criminal prosecutions, just as we would were we to sacrifice all of our interests in privacy and personal liberty. (1103)

Reinhardt thus concluded that the government's interest did not outweigh Kincade's privacy interest "in his body." But he went one step further, saying that all of the considerations in the balance of interests must be weighed "in light of the fact . . . under controlling Supreme Court authority we are not free to approve suspicionless searches conducted for law enforcement purposes" (1103). Though the results of the balancing test might affect the "degree of suspicion or cause required to conduct such searches, it could not serve to eliminate the requirement of individualized suspicion entirely" (1103). For Reinhardt, the need to find individualized suspicion remained important, resisting the logic of the previous DNA database cases that swept this requirement away in favor of generalizing suspicion across all classes of criminal subjects.

A significant portion of Reinhardt's opinion in *Kincade I* is devoted to rebutting the availability of the "special needs" doctrine, a conclusion that few legal scholars disagree with (Maclin 2005; Carnahan 2004, Kaye 2006). In *Kincade I*, the government's own characterization of the DNA statute's "primary purposes" were "to help law enforcement solve unresolved and future cases," and "to increase accuracy in the criminal justice system." Reinhardt used these statements to conclude that the government's goals were nothing more than the normal need for law enforcement, therefore putting the special needs exception out of reach.

As mentioned previously, after the Ninth Circuit declared DABEA unconstitutional in *Kincade I*, the decision was vacated and the case was

reheard *en banc*. In a plurality opinion, the *en banc* court upheld the constitutionality of the DABEA. As in *Jones*, the Ninth Circuit applied a "totality of the circumstances" test to find the search "reasonable" given the substantially diminished expectation of privacy by the parolee, the minimally intrusive nature of blood sampling, and the important social interest "furthered by the collection of DNA" (*Kincade II*, 839). The court found that a special needs analysis was not required in determining the constitutionality of the statute. Judge Reinhardt reiterated his "individualized suspicion" doctrine in a scathing dissent, analyzed in more detail in the following section.

Analysis

After *Kincade II*, the circuit courts are no longer split on the question of whether the collection of DNA from those enmeshed in the criminal justice system violates their Fourth Amendment rights. The Supreme Court recently refused an opportunity to clarify the law further when Kincade appealed the Ninth Circuit's *en banc* ruling. Nevertheless, doctrines diverge in interesting ways. Close attention to the *dicta* in these cases (that is, their nonbinding language) suggests a close interaction between the technological and legal imagination.

First, the judges in these cases conceive of technology and its potential impact on civil liberties quite differently from one another. They engage in a form of technological risk assessment, in which short- and long-term hazards to those within the criminal justice system, and to society as a whole, need to be imagined and balanced against potential benefits. These assessments, in turn, depend upon competing conceptions of the technology in question, variously described as a fingerprint, a type of information, and a large state-operated surveillance network. These doctrinal choices and risk assessments also depend on prior conceptions of how, as a general matter, the Fourth Amendment responds to new technologies. In particular, there is a stark split between those judges who imagine the continuous development of law enforcement technologies as benign, and those who see a malignant trend that slowly erodes Fourth Amendment protections. These views take different positions on the trade-off between individual freedom and collective security.

Second, these technological imaginaries help condition and construct the legal identities of criminal kinds. Thus, the "reasonableness" approach simultaneously constructs a newly legalized forensic technology and a broad and undifferentiated set of future "usual suspects," from convicts

to arrestees. By contrast, the "special needs" approach constructs a narrower set of subjects, the recidivists, who justifiably suffer the brunt of the extra privacy intrusion. The "individualized suspicion" approach resists reifying these criminal kinds. Conditioned by a pessimistic paradigm of technological authoritarianism, this last position resists normalizing the technology as an unproblematic intrusion on those who have already, to some degree, forfeited their freedom.

"Totality of the Circumstances"

In *Jones*, Judge Niemeyer characterized the new forensic DNA technology as a high-tech fingerprint: no more threatening to privacy than the normal booking procedure but much more powerful and precise than existing fingerprinting. Niemeyer emphasized the way in which nucleotides "are arranged differently for every individual except for identical twins" (*Jones*, 303). This set up his statement that "improved scientific technology has prompted efforts to use the individuality of a person's DNA in the context of criminal law enforcement," and he proceeded to describe the "DNAPrint": the digital and/or visual representation of a set of thirteen short tandem repeats (STRs) on the human genome analyzed for an entry onto any forensic DNA database (304). Today, "DNA Profile" is the dominant name.

Fingerprinting is the key analogy in the opinion. As we have already seen, the use of fingerprints ends up providing the foundation for his constitutional argument. Because the Virginia statute authorizes a blood draw, there is a search involved in using this technology, but because it is merely a "limited search for the purpose of ascertaining and recording the identity of a person who is lawfully confined to prison," it is functionally analogous to the constitutionally accepted practice of fingerprinting, and therefore deemed minimally invasive (*Jones*, 306).

A logic of equivalence drives Niemeyer's tacit risk assessment of the new technology. For the judge, the DNA databases do not differ significantly from forensic fingerprinting, which also involves the indefinite storage of bodily information, searchable at a click. But Niemeyer neglects to consider the ways in which fingerprints, though also undergoing the material to informational shift, remain a different kind of thing from DNA. Prints are not bodily material, they are not potentially health-related, and they do not implicate genetic relatives. For these reasons, DNA can be considered special, a finding that was reinforced (albeit in a very different context) by a widely discussed gene patenting case in 2010.[16] Further, the judge's analysis of the degree of intrusiveness of the search only considers the blood

draw, not the continuing technological surveillance, the banking of DNA samples indefinitely, and the frequent searches of biometric information.

Niemeyer's technological optimism carries the day. Whereas the new technique poses few new risks to the incarcerated, and none to greater society, it does bring significant new benefits. The power of this "dramatic new tool," increased precision, helps justify what has already been sanctioned in the fingerprint context: "The government justification for this form of identification, therefore, relies on no argument different in kind from that traditionally advanced for taking fingerprints and photographs, *but with additional force because of the potentially greater precision of DNA sampling and matching records*" (307; emphasis added).

The new technology becomes simply a better case of an adequately controlled technology and well-known practice. Just as genetically modified crops were normalized by the Food and Drug Administration through an across-the-board determination of "substantial equivalence," so too a judgment of equivalence operates to normalize the DNA database within legal and cultural logics. Having read the DNA technology as equivalent to the fingerprint, Niemeyer deemed the objective of the Virginia statute "significant" and "the privacy intrusion limited" (*Jones*, 308).

This logic of controlled equivalence has been evident throughout the expansion of forensic databases, from including only felons convicted of violent crimes to those convicted of lesser offenses, parolees, and now arrestees. An unstated logical implication of this rule, however, is that arrestees of particular crimes—not just "all convicted felons"—would become fair game for DNA profiling and banking because they are sufficiently suspicious to satisfy a probable cause standard for future database searches.

Such a logical implication could not have escaped the *Jones* majority. It is too obvious. And indeed the case has provided the doctrinal structure and rationale for a number of courts to uphold arrestee inclusion statutes, including the Virginia Supreme Court in 2007 and a California District Court in 2009.[17] In effect, the risk management strategy is to limit the threat of civil liberty deprivation to convicts, and at its broadest, arrestees, as this population is deemed, in turn, to pose unacceptable risks to society. Such a rule carries clear potential for increasing existing inequalities in the criminal justice system. Because blacks and other minorities are more often targeted for pretextual arrests and police profiling, they will bear a disproportionate amount of intrusion (Kaye and Smith 2003, n153). Most often, blacks and the poor will be in the database, and whites and the privileged out.

"Special Needs"

The special needs opinions discussed previously provide a contrast with the technological imaginary of the *Jones* majority. In the *Jones* dissent, Judge Murnaghan expressed skepticism toward the majority's blanket assumptions about the efficacy of the new technology. With the danger of database expansion in mind, these special needs opinions carve out a narrow exception to the individualized suspicion rule for felons who have perpetrated crimes with high recidivism rates. Rather than identifying the prisoner/nonprisoner boundary as relevant for Fourth Amendment protection, the "recidivist" rule posits subcategories of felons discernable through empirical findings and scientifically grounded classification. The general presumption against inclusion is maintained, creating a more precautionary approach with respect to the general erosion of civil liberties.

Judge Murnaghan exhibited a general wariness toward what he perceived as a dangerous trend in the erosion of civil liberties in the face of creeping police power. He was concerned that under the majority's logic, the "disturbing restriction of the Fourth Amendment protections afforded to the nation's prisoners" could easily be extended to all citizens (*Jones*, 313). Murnaghan's explicit invocation of "citizens in a free society still clinging to disappearing Fourth Amendment protections" painted a picture of liberties in grave danger. The judge confessed to "a deep, disturbing and overriding concern that, without proper and compelling justification, the Commonwealth may be successful in taking significant strides towards the establishment of a future police state, in which broad and vague concerns for administrative efficiency will serve to support substantial intrusions into the privacy of citizens" (315).

To place brakes on this slippery slope, he looked to the empirical data before the court, which included two reports on prisoner recidivism,[18] to establish a constitutionally relevant distinction between violent and nonviolent felons for purposes of database inclusion. Such reasoning had no precedent in the Fourth Circuit, but it proved persuasive to the *Roe* court and became law in the Second Circuit.

Judge Pooler's opinion for a unanimous three-judge panel in *Roe* grappled with further details of the statute with regard to the handling of physical samples and the continued use of DNA profiles. This analysis explicitly acknowledged that more is at risk than the intrusion into criminal bodies and brought ongoing possession of samples and use of information into the frame of judicial risk assessment. However, as noted previously, the unanimous *Roe* panel was satisfied with the statute's mitigating safeguards (e.g., securing the confidentiality of the results, and providing for

expungement of profiles upon reversal). These safeguards help contain the risk of slippage toward a police state, but they are complemented by another critical management strategy: a legal boundary between the recidivist and nonrecidivist classes of criminals. This boundary establishes a firewall against the possible expansion of surveillance from the criminal classes to the rest of society, from "them" to "us." This position embodies a general distaste for blanket suspicionless searches, but creates a limited exception where there is, in essence, "statistical probable cause" to believe that particular groups (i.e., recidivists) will commit future crimes.

Embedded within this risk management strategy, we see a particular characterization of the Fourth Amendment-technology interface, that is, as a system that is controllable through legal rules based on good social science. The view relies on a prediction model to justify inclusion: because recidivists are likely to commit more crimes, inclusion in the database may deter this class of individuals, or help us take them off the street. The fact that this form of statistical probable cause needs to be established through scientific inquiry affords society its necessary protection against universal inclusion and a "future police state."

"Individualized Suspicion"

In *Kincade I*, Judge Reinhardt focused on the blood draw as a clear privacy intrusion requiring some degree of individualized suspicion in lieu of a warrant. In his *Kincade II* dissent, he focused more attention on the nature of the technology itself. For Reinhardt, forensic DNA is not simply a booking tool like a fingerprint, but a large centralized technological system for rounding up the usual suspects and a repository of potentially sensitive information. In both opinions, Reinhardt considered the case against a backdrop of judicial suspicion toward new surveillance technologies, a tradition that recognizes a slippery slope toward the erosion of privacy. The individualized suspicion approach draws a firm line in the sand against the construction of forensic DNA databases, refusing to corral felons or prisoners en masse for inclusion.

In characterizing CODIS, Reinhardt described what Langdon Winner would call an artifact with politics (Winner 1986), a technology that necessitates a particular form of political power: in this case a strongly authoritarian police state that can bully vulnerable elements of the public. The majority's decision in *Kincade II*, Reinhardt argued, "encourages the very centralization of government authority that has repeatedly resulted in the sacrifice of our liberties in the name of law enforcement" (*Kincade II*, 843–844). Accordingly, he drew comparisons to the abuses of J. Edgar

Hoover in monitoring civil rights leaders in the 1960s, and the country's use of central databases to "round up" Japanese-Americans and Communists during the 1940s and 1950s (843). Furthermore, in contrast to the judges in *Jones* and *Roe*, Reinhardt dwelt on the nature of the information contained in the DNA profiles and the retention of samples under the statutes. He emphasized the sensitivity of biometric information and also the fact that, "as technology evolves," the maintenance of DNA "will permit a myriad of other known and unknown uses of the samples (870).

Reinhardt projects these images of forensic DNA profiling onto an existing tradition of constitutional concern with new surveillance technologies. In its first sentence, Judge Reinhardt's majority opinion in *Kincade I* emphasizes the special hazards posed by technological developments to Fourth Amendment protections: "Each leap forward in forensic science promises ever more efficient and swift resolution of criminal investigations. At the same time, technological advances frequently raise new constitutional concerns and threaten our basic liberties" (*Kincade I*, 1096).

To support this statement, Reinhardt cites the 2001 Supreme Court case of *Kyllo v. United States*.[19] Writing for the 5–4 majority in that case, Justice Scalia maintained "it would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology" (*Kyllo*, 33–34). In that case, law enforcement agents suspected that marijuana was being grown in a home belonging to Danny Kyllo. Without a warrant, agents used infrared-detecting thermal imagers to scan Kyllo's apartment for heat emissions typical of lamps needed to grow marijuana indoors. Justice Scalia held that the surveillance constituted a Fourth Amendment search, and was therefore presumptively unreasonable without a warrant. He cited the 1961 case *Silverman v. United States*, in which the court notes the "frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society."[20] Reinhardt in turn invoked this pattern of technological skepticism in *Kincade I*, sharing with Judge Murnaghan a fear of the loss of a free society.

It is Judge Kozinski in *Kincade II*, not Reinhardt, who in dissent imagined the slippery slope in the starkest terms. He emphasized the power of a tempting new technology to lure society onto the slippery slope by its very efficiency. Born in Communist Romania of parents who were Holocaust survivors, Kozinski criticized what he called the plurality's "exuberant faith in the positive power of technology" (*Kincade II*, 872), and discussed the attitude-skewing effects of the database's crime-solving power: "Later, when further expansions of CODIS are proposed, information from the

database will have been credited with solving hundreds or thousands of crimes, and we will have become inured to the idea that the government is entitled to hold large databases of DNA fingerprints" (873).

He called the plurality's opinion an "engraved invitation" to future expansions of the database, and predicted that each step may not seem like much until "the fishbowl will look like home" (*Kincade II*, 874). Accordingly, he declared that "the time to put the cork back in the brass bottle is now—before the genie escapes" (875). For Kozinski, technological advance, at least in surveillance, is a special source of risk to Fourth Amendment protections. Under the "reasonable expectations" standard in *Katz*, the scope of privacy protection depends on the subjective expectations of individuals, meaning that the government could eliminate privacy rights by accustoming the public to heightened levels of technological surveillance.

Reinhardt agreed with Kozinski that DNA profile technology exerts a sort of malignant gravitational pull toward the bottom of the slippery slope, noting with concern that some state statutes are already providing for the inclusion of arrestees and those convicted of misdemeanors. If "totality of the circumstances" should become the general rule, "we all have reason to fear that the nightmarish worlds depicted in films such as *Minority Report* and *Gattaca* will become realities" (*Kincade II*, 851). At the bottom of this slide lies the possibility that "the database could be used to repress dissent or, quite literally, to eliminate political opposition" (847).

Accordingly, Reinhardt and the other dissenters in *Kincade* cleaved to a bright line of individualized suspicion. All other doctrinal dispensations, they argue, "dismantle the structural protections that lie at the core of the Fourth Amendment" and simply ask us "to trust those in power" (845). Reinhardt identified a strong precautionary logic against the aggrandizement of power in the structural checks and balances of the Constitution. Whereas other judges managed the Fourth Amendment–technology interface by creating new kinds of suspect classes insulated from the innocent public, Reinhardt's approach would mean that––with respect to bodily intrusions for DNA databanks––felons, arrestees, and other classes would not be systematically downgraded. Instead, the individualized suspicion standard would continue to apply, maintaining the individual-state boundary as the crucial one for legal analysis. In other words, the arrestee is still one of "us" where civil liberties are at stake, and so too is the convict.

Conclusion

In this chapter, I have examined the play of imagination as different judges weigh the constitutionality of a new technology. We have seen how

different technological imaginaries form part of the interpretive framework of judging, conditioning and shaping doctrinal choice and legal reasoning. Some see a lurking dystopia in the new technological order; others see prospects for a safer society. These imaginaries entail not only visions, theories, and a priori characterizations of technological objects, but also models of how those objects interact with the social technology known as the law. Some judges recognize technologies to be problematic objects for legal analysis precisely because they develop and mutate; others consider them to be stable and predictable. These positions affect judicial calculations of the risks and benefits of selecting particular legal rules. Risk management strategies must address how new technological orders will engage the constitutional architecture in the long term. Thus, we see judges trying to manage the interoperability of two intersecting technological systems—one material, one normative.

As these Fourth Amendment cases demonstrate, legal adjudication can be a process and medium through which social and technological orders develop together and receive new articulation. In other words, it is site of coproduction, and an especially important one. These judicial imaginaries have stark consequences for different classes of citizens, who become unwitting players in the dynamics of bioconstitutionalism. The stakes are high. Even as these judicial imaginaries help bring new technological orders into full operation, they produce new kinds of subjects whose rights are reframed without their direct participation.

Notes

1. *Katz v. United States*, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).

2. *California v. Acevedo*, 500 U.S. 565, 580 (1991).

3. *Mincey v. Arizona*, 437 U.S. 385, 390 (1978), quoting *Katz*, 389 U.S. at 357 (footnotes omitted).

4. *Robbins v. California*, 453 U.S. 420, 438 (1981) (Rehnquist, J., dissenting).

5. *En banc*, French for "in the bench," signifies a decision by the full court of all the appellate judges on the court. This process is often invoked when there is a particularly significant issue at stake or when requested by a party to the case and agreed to by the court.

6. *Jones v. Murray*, 962 F.2d 302 (4th Cir. 1992).

7. See, for example, *Shaffer v. Saffle*, 148 F.3d 1180, 1181 (10th Cir. 1998); *Boling v. Romer*, 101 F.3d 1336, 1340 (10th Cir. 1996); *Schlicher v. Peters*, 103 F.3d 940, 943 (10th Cir. 1996); *Rise v. Oregon*, 59 F.3d 1556, 1560–1562 (9th Cir. 1995); *Kruger v. Erickson*, 875 F. Supp. 583, 588–589 (D.Minn. 1995); *Sanders v. Coman*, 864 F.Supp. 496, 499 (E.D.N.C. 1994); *Ryncarz v. Eikenberry*, 824 F. Supp. 1493, 1498–1499 (E.D.Wash. 1993).

8. *Roe v. Marcotte*, 193 F.3d 72, 81 (2nd Cir. 1999).

9. *Roe v. Marcotte* at 77, quoting and citing *Skinner v. Railway Labor Execs. Association*, 489 U.S. 602, 624 (1989).

10. *Griffin v. Wisconsin*, 483 U.S. 868 (1987).

11. *Griffin v. Wisconsin* at 79, citing *Skinner,* 489 U.S. at 625.

12. *U.S. v. Kincade* (*Kincade I*), 345 F.3d 1095 (9th Cir. 2003).

13. *U.S. v. Kincade* (*Kincade II*), 379 F.3d 813 (9th Cir. 2004) (*en banc*).

14. *Kincade I*, 345 F.3d at 1095.

15. *Kincade I* at 1099–1100, citing Nelkin 1999, 110.

16. *Association for Molecular Pathology v. United States Patent and Trademark Office*, No. 09 Civ. 4515 (S.D.N.Y., Mar. 29, 2010).

17. *Anderson v. Commonwealth*, 274 Va. 469 (Va. 2007) and *U.S. v. Pool*, 645 F. Supp. 2d 903 (E.D. Cal. 2009). In contrast, a Minnesota court of appeal has held that arrestee inclusion is unconstitutional for lack of probable cause. *In re Welfare of C.T.L.,* 722 N.W. 2d 484 (Minn. Ct. App. 2006).

18. The reports cited in the opinion were Beck and Shipley 1989 and Virginia Division of Justice and Crime Prevention 1989.

19. *Kyllo v. United States*, 533 U.S. 27 (2001).

20. *Silverman v. United States*, 365 U.S. 505, 509 (1961).

References

Aronson, Jay. 2006. *The Introduction, Contestation, and Regulation of Forensic DNA Analysis in the American Legal System (1984–1994)*. Minneapolis, Minn.: University of Minnesota Press.

Beck, Allen J., and Bernard E. Shipley. 1989. "Recidivism of Prisoners Released in 1983." Bureau of Justice Statistics Special Report: 1–13.

Biancamano, John D. 2009. Arresting DNA: The Evolving Nature of DNA Collection Statutes and Their Fourth Amendment Justifications. *Ohio State Law Journal* 70:613–660.

Bieber, Frederick. 2004. Science and Technology of Forensic DNA Profiling: Current Use and Future Directions. In *DNA and the Criminal Justice System*, ed. David Lazer, 23–62. Cambridge, Mass.: MIT Press.

Bradley, Craig M. 1993. The Court's "Two Model" Approach to the Fourth Amendment: Carpe Diem! *Journal of Criminal Law & Criminology* 84:429–461.

Callon, Michael. 1987. Society in the Making: The Study of Technology as a Tool for Sociological Analysis. In *The Social Construction of Technological Systems*, ed. Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, 83–103. Cambridge, Mass.: MIT Press.

Carnahan, S. J. 2004. The Supreme Court's Primary Purpose Test: A Roadblock to the National Law Enforcement Database. *Nebraska Law Review* 83:1–37.

Hughes, Thomas. 2004. *Human-Built World: How to Think About Technology and Culture*. Chicago, Ill.: University of Chicago Press.

Jasanoff, Sheila. 2008. Making Order: Law and Science in Action. In *New Handbook of Science and Technology Studies*, ed. Ed Hackett et al., 761–786. Cambridge, Mass.: MIT Press.

Jasanoff, Sheila, and Sang-Hyun Kim. 2009. Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in the United States and South Korea. *Minerva* 47 (2): 119–146.

Kaye, David H. 2006. Who Needs Special Needs? On the Constitutionality of Collecting DNA and Other Biometric Data from Arrestees. *Journal of Law, Medicine & Ethics* 34:188–198.

Kaye, David H., and Michael E. Smith. 2003. DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage. *Wisconsin Law Review* 2003:413–459.

Lynch, Michael, Simon A. Cole, Ruth McNally, and Kathleen Jordan. 2008. *Truth Machine: The Contentious History of DNA Fingerprinting*. Chicago, Ill.: Chicago University Press.

Maclin, Tracey. 1994. When the Cure for the Fourth Amendment Is Worse than the Disease. *Southern California Law Review* 68:1–72.

Maclin, Tracey. 2005. 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 & Ethics* 33 (1): 102–124.

Murphy, Erin. 2008. Paradigms of Restraint. *Duke Law Journal* 57:1321–1411.

Nakashima, Ellen, and Spencer Hsu. "U.S to Expand Collection of Crime Suspects' DNA—Policy Adds People Arrested But Not Convicted." *Washington Post*, April 17, 2008, A1.

Nelkin, Dorothy. 1999. Cultural Perspectives on Blood. In *Blood Feuds: AIDS, Blood, and the Politics of Medical Disaster*, ed. Eric A. Feldman and Ronald Bayer, 273–292. New York: Oxford University Press.

Power, Robert C. 1989. Technology and the Fourth Amendment: A Proposed Formulation for Visual Searches. *Journal of Criminal Law & Criminology* 80:1.

Virginia Division of Justice and Crime Prevention. 1989. *Violent Crime in Virginia*. Richmond: Commonwealth of Virginia, Department of Criminal Justice Statistics.

Virginia Joint Subcommittee Studying Creation of a DNA Test Data Exchange. 1990. Report of the Joint Subcommittee Studying Creation of a DNA Test Data Exchange to the Governor and the General Assembly of Virginia. Richmond: Commonwealth of Virginia.

Winner, Langdon. 1986. Do Artifacts Have Politics? In *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, ed. Langdon Winner, 19–39. Chicago, Ill.: University of Chicago Press.

Wynne, Brian. 1988. Unruly Technology: Practical Rules, Impractical Discourses and Public Understanding. *Social Studies of Science* 18 (1): 147–167.