

**A FOURTH AMENDMENT PRIVACY ANALYSIS OF THE
DEPARTMENT OF DEFENSE'S DNA REPOSITORY FOR
THE IDENTIFICATION OF HUMAN REMAINS: THE
LAW OF FINGERPRINTS CAN SHOW US THE WAY**

MAJOR STEVEN C. HENRICKS¹

I. Introduction

The Department of Defense (DOD), through the Armed Forces Institute of Pathology (AFIP), collects deoxyribonucleic acid (DNA) via blood samples from all service members.² The DOD collects the DNA samples for the sole purpose of identifying remains should a service member die while serving his or her country.³ The AFIP stores the collected samples at a single site in the Washington, D.C. area.⁴ From time to time, state, federal, and military law enforcement will seek to match DNA found at a crime scene or taken from a victim with the DNA samples stored at the AFIP site. Historically, the AFIP and the DOD honor such requests only when the request meets certain conditions, including that a "proper judicial order" accompanies the request.⁵ This article reviews whether the Fourth Amendment⁶ and recently enacted federal law⁷ require a warrant or search

1. Judge Advocate, U.S. Army. Presently assigned as the Group Judge Advocate, Fifth Special Forces Group, Fort Campbell, Kentucky. LL.M., 2003, The Judge Advocate General's Legal Center and School, U.S. Army, Charlottesville, Virginia; J.D., 1991, University of Kansas; B.A., 1988, Bethany College, Lindsborg, Kansas. Previous assignments include: Fort Monmouth, New Jersey, 1993-1996 (Legal Assistance Attorney, Administrative Law Attorney, Special Assistant U.S. Attorney, Trial Counsel, and Chief, Legal Assistance and Claims), Fort Riley, Kansas, 1996-1999 (Defense Counsel and Senior Defense Counsel), and Fort Hood, Texas, 2000-2002 (Chief, Legal Assistance, III Corps and Chief of Military Justice, 1st Cavalry Division). Member of the Kansas and Missouri bars.

2. See U.S. DEP'T OF DEFENSE, DIR. 5154.24, ARMED FORCES INSTITUTE OF PATHOLOGY 4 (20 Oct. 1996) [hereinafter DOD DIR. 5154.24].

3. See *id.*

4. See Interview with Mr. David Boyer, Director of Operations, Armed Forces Repository of Specimen Samples for the Identification of Human Remains, in Gaithersburg, Md. (Nov. 8, 2002) [hereinafter Boyer Interview].

5. See DOD DIR. 5154.24, *supra* note 2, at 6.

6. U.S. CONST amend. IV.

7. 10 U.S.C.S. § 1565a (LEXIS 2004).

authorization⁸ before the AFIP provides part of a service member's DNA sample to law enforcement.

A. Hypotheticals

To help understand the issues present in this topic, consider the following hypothetical scenarios.

1. Hypothetical 1

An unknown individual sneaks into barracks located on a large United States Army (Army) installation, home to over forty thousand troops. Once inside the barracks, the individual observes a female soldier enter her barracks room, notes the soldier does not have a roommate, and sees that she fails to lock her door. The individual checks that no one noticed him, dons a mask, and enters the female Soldier's barracks room. Once inside, the individual threatens the female with a knife, brutally rapes and sodomizes her, and then leaves the barracks unobserved.

Shortly thereafter, the female Soldier reports to military authorities that someone she could not identify raped her. Military health care officials immediately perform a rape kit analysis, which produces a semen sample from the unknown individual. When the military investigation does not immediately produce a suspect, the victim demands that the Army check its "DNA database" against DNA from the semen sample for a possible match. The Army responds that there is no way to know a Soldier committed this crime,⁹ and assuming a Soldier did rape the victim, Soldiers have a reasonable expectation of privacy in their respective DNA samples kept by the AFIP to identify human remains. A warrant or search authorization must therefore support any search done of an AFIP blood sample for a law enforcement purpose.

The victim, satisfied with neither that response nor the military investigation's progress, contacts local state law enforcement authorities and

8. A search authorization is the military equivalent of a warrant. A search authorization must be based on probable cause and can only be issued by a military judge, military magistrate, or a commander. See *MANUAL FOR COURTS-MARTIAL, UNITED STATES, MIL. R. EVID.* 315 (2002) [hereinafter *MCM*].

9. Assume the installation is an "open post," meaning that civilians can freely enter and leave the installation without any identification check.

inquires if they will investigate her rape. Local law enforcement decides to open an investigation into the rape after determining the crime occurred on concurrent federal and state jurisdiction.¹⁰ A local detective then submits a request, signed by the state agency head of law enforcement, to the AFIP requesting that they attempt a blind match of the suspect's DNA sample with the DNA samples under the AFIP's control. The AFIP's position remains unchanged, and a few months later the person who committed the rape, in fact a Soldier, kills a local civilian. The investigation of the killing conclusively establishes the Soldier as the rapist and the killer.

2. *Hypothetical 2*

Same facts as *Hypothetical 1*, but now military and state investigators both reasonably believe that the suspect is an unknown male Soldier who lives in some nearby barracks. There are approximately three hundred male soldiers who live in that barracks. The AFIP refuses to do a blind search of the three hundred Soldiers' DNA samples, in part because of no individualized probable cause.

3. *Hypothetical 3*

Same facts as *Hypothetical 1*, but now military and state investigators reasonably believe that the rapist is one of ten Soldiers seen around the barracks at the time of the rape. The investigation is in its early stages, and there has not yet been time to eliminate any of the ten Soldiers from suspicion. The AFIP's response is the same as in *Hypothetical 2*.

B. Article Overview

This article analyzes whether the DOD correctly requires a warrant or search authorization before releasing part of a service member's DNA or blood sample to law enforcement. First, the article reviews the DNA molecule, the DNA molecule's relationship to the human genome, and forensic testing of the DNA molecule. Second, the article discusses the AFIP's

10. Either the state or federal government has jurisdiction to prosecute crimes occurring in this area. There are four types of jurisdiction on military posts: exclusive federal legislative jurisdiction, concurrent legislative jurisdiction, partial jurisdiction, and proprietary federal interest. See U.S. DEP'T OF ARMY, REG. 405-20, FEDERAL LEGISLATIVE JURISDICTION 1 (1 Aug. 1973).

DNA sample collection protocol and then compares that process with the Federal Combined DNA Index System (CODIS) and fingerprint databanks. Within this section, the article addresses specific rules adopted by the DOD applicable to the release of the AFIP DNA samples.

Third, the article reviews federal statutory schemes that generally address whether and how federal executive agencies release information contained in records they possess. Fourth, the article examines whether service members have a reasonable expectation of privacy under the Fourth Amendment in the DNA samples they must give to the AFIP. Fifth, the article reviews and critiques recently enacted federal legislation that addresses the release of DNA samples to law enforcement. Sixth, based on the preceding review and analysis, the article addresses whether the AFIP's position in each hypothetical is correct.

The article then concludes that DNA's unique nature creates a reasonable expectation of privacy held by the service member in his AFIP DNA sample, which in almost all cases may be overcome only with consent to search or a search warrant or authorization. Moreover, the DOD's self-imposed rules concerning how and why the DOD and the AFIP collect service members' DNA separately creates a reasonable expectation of privacy by service members in their AFIP DNA sample, which again may only be overcome with consent or a search warrant or authorization.

II. DNA and the Human Genome

Most are by now familiar with three general DNA concepts: DNA is the building block of life; the double helix staircase model used to represent a DNA molecule; and matching DNA samples provide almost irrefutable identification of an individual. Any privacy analysis of an individual's DNA, however, must go deeper than this cursory knowledge. To know what privacy interests are at stake, one must understand what DNA is, what DNA can tell us about an individual, and what DNA may, in the future, tell us about that same individual.

A. The DNA Molecule

Deoxyribonucleic acid is present in every human cell.¹¹ Within each cell, DNA is a molecule made up of two strands of nucleotide acid.¹² Nucleotide acid subparts, called nucleotides, form the strands of the double

helix.¹³ Nucleotides, in turn, are made up of three components: a nitrogen base, a phosphate molecule, and a sugar molecule.¹⁴ The nitrogen base is further broken down to one of four organic bases: adenine (A), guanine (G), thymine (T), or cytosine (C).¹⁵ These nitrogen bases arrange themselves in two ways. First, on either strand of the double helix the nitrogen bases form linear, non-overlapping sequences known as the DNA sequence (for example, ATTCCGGA).¹⁶ Second, the nitrogen bases form base pairs between the two strands on the double helix.¹⁷ Adenine-thymine (AT) is one base pair, while GC (guanine-cytosine) forms the other base pair.¹⁸ Chemical bonds between these base pairs cause the nucleotide acid strands to come together as the double helix.¹⁹

The DNA sequence provides the code to life. Scientists have determined that the four nitrogen bases described in the preceding paragraph form code words, usually in groups of three letters.²⁰ Similar to a telegraph, a code phrase or message will begin with a start word, followed by a substantive message, and then followed with a code word saying the message is over.²¹ The substantive portion of the message instructs how to

11. See David H. Kaye & George F. Sensabaugh, Jr., *Reference Guide on DNA Evidence*, in REFERENCE MANUAL ON SCIENTIFIC EVIDENCE 485, 504 (Federal Judicial Center ed., 2d ed. 2000).

12. See *id.* at 560.

13. See Human Genome Project Information Web Site, *Dictionary of Genetic Terms*, at <http://www.ornl.gov/hgmis/publicat/primer2001/glossary.html> (last modified Mar. 12, 2004) [hereinafter *Dictionary of Genetic Terms*].

14. See *id.*

15. See David Berman, Online News Hour, *The Inside Is Out* (Feb. 12, 2001), at <http://www.pbs.org/newshour/extra/features/jan-june00/genome.html> (on file with author).

16. See JOHN BLAMIRE, *Genotype and Phenotype: The Genetic Code*, in SCIENCE AT A DISTANCE at <http://www.brooklyn.cuny.edu/bc/ahp/BioInfo/GP/GeneticCode.html> (last visited Nov. 16, 2004).

17. See Human Genome Project Information Website, *From the Genome to the Proteome*, at <http://www.ornl.gov/hgmis/project/info.html> (last modified Mar. 11, 2004) [hereinafter *From the Genome to the Proteome*].

18. See *Dictionary of Genetic Terms*, *supra* note 13.

19. See *id.*

20. See BLAMIRE, *supra* note 16. Sixty-four three-letter words are possible in a four-letter alphabet.

21. See *id.*

create a living organism and provides the organism with unique characteristics known as genetic traits.²²

A cell's cytoplasm is where a cell acts on DNA instructions necessary to produce a trait.²³ The DNA sends out its message by copying it onto a ribonucleic acid (RNA) molecule.²⁴ The RNA molecule then travels to the cell's cytoplasm where the cell converts the DNA instructions into a linear sequence of amino acids.²⁵ There are up to twenty classes of amino acids arranged in this sequence, and in the cytoplasm the amino acid sequence becomes a protein.²⁶ Often the protein takes the form of an enzyme catalyst that will cause or enhance a chemical reaction in the cell that then produces a genetic trait.²⁷ Eye color, blood type, skin pigmentation, and curly hair are all genetic traits caused by this process.²⁸ Deoxyribonucleic acid is therefore the molecule in the human body where our genetic traits reside in a nitrogen-based code.

B. The Human Genome

Within a human cell, DNA molecules form the twenty-three pairs of chromosomes found in a cell's nuclei.²⁹ A genome is the DNA that makes up a complete set of chromosomes.³⁰ A single human chromosome on average is 100 million DNA base pairs long,³¹ and ranges from 50 million to 250 million DNA base pairs.³² A complete human genome contains approximately three billion DNA base pairs.³³ Chromosomes are made up

22. See BLAMIRE, *supra* note 16, at <http://www.Brooklyn.cuny.edu/bc/ahp/BioInfo/GP/FlowInfo.html>.

23. *See id.*

24. *See id.* The DNA coded sequence is redundant, meaning many of the same messages are sent out over and over again. Interestingly, computer programmers also often make their computer codes redundant to help ensure the program's vitality. *See id.*

25. Scientists believe that the substantive message sent to amino acids with three letter code words varies from one to four words. *See id.* at <http://www.Brooklyn.cuny.edu/bc/ahp/BioInfo/GP/GeneticCode.html> (last visited Mar. 31, 2004).

26. *See From the Genome to the Proteome, supra* note 17.

27. See BLAMIRE, *supra* note 16, at <http://www.Brooklyn.cuny.edu/bc/ahp/BioInfo/GP/GeneticTrait.html>.

28. *See Berman, supra* note 15.

29. *See From the Genome to the Proteome, supra* note 17.

30. *See id.*

31. *See id.*

32. *See id.*

33. *See id.*

of many genes,³⁴ but genes are nothing more than the strands of DNA sequence described in the proceeding two paragraphs that provide traits (that is, coding DNA sequence).³⁵ Just as every human cell contains DNA, almost every human cell contains a complete genome.³⁶

In the 1990s, scientists set out to map the human genome's entire DNA base pair sequence.³⁷ The task was daunting, but with continued advances in computer processing and other technology, scientists completed the mapping and now know the complete three billion DNA base pair sequence.³⁸ Knowing the entire human genetic sequence, however, is only a first step. Scientists must still "crack the code" of the DNA sequence.³⁹ That is, scientists do not yet know in every circumstance where substantive (*i.e.*, coding) DNA sequence ends and non-coding DNA sequence begins.⁴⁰ By understanding the human genome, scientists can better understand a cell's proteome: all proteins' structures and activities within a cell.⁴¹ The combined further study of the human genome and proteome will provide a molecular basis to understand and manipulate health, disease, and therefore life.⁴²

C. Forensic Testing of the DNA Molecule

The DNA sequence of base pairs is 99.9% the same in each human being.⁴³ That .1% difference, however, is what makes each of us individuals and not clones. Some of the unique aspects of an individual's DNA are non-coding DNA sequence, often referred to as "junk DNA."⁴⁴ Signif-

34. *See id.*

35. *See id.*

36. *See id.* All human cells except mature red blood cells contain a complete genome. *See id.*

37. *See* Human Genome Project Information Website, *U.S. Human Genome Project 5-Year Research Goal 1998-2003*, at http://www.ornl.gov/TechResources/Human_Genome/hg5yp/ (last modified Dec. 9, 2003).

38. *See* Berman, *supra* note 15.

39. The complete human genome has between thirty and forty thousand genes. *See From the Genome to the Proteome*, *supra* note 17.

40. *See* Berman, *supra* note 15.

41. *See From the Genome to the Proteome*, *supra* note 17.

42. *See id.*

43. *See* Berman, *supra* note 15.

44. Coding DNA is that part of the DNA sequence that provides instructions for protein action within the cell. That is, coding DNA constitutes a gene, and is usually made up of 1,000 to 10,000 base pairs. Non-coding DNA does not provide any known protein instruction. *See From the Genome to the Proteome*, *supra* note 17.

icant parts of the non-coding DNA sequence vary considerably between individuals.⁴⁵ Forensic scientists have seized on this difference to identify or exclude DNA from a known individual or to match or exclude DNA with another unidentified DNA sample.⁴⁶

Directly sequencing even a junk DNA sequence is time consuming and costly, and usually only research centers working on mapping the human genome have this capability.⁴⁷ Scientists, however, have developed techniques where they identify specific parts of a DNA sequence, called alleles, that vary between individuals.⁴⁸ Even these alleles are not directly sequenced to make a match or exclusion.⁴⁹ Instead, scientists identify the sequence of base pairs that makes the selected allele unique.⁵⁰ There are various methods to select the correct sequence⁵¹ of base pairs for this process. The two most common are variable number of tandem repeats (VNTRs) and short tandem repeats (STRs).⁵² The STRs are the shorter of the two, and average 50 to 350 base pairs long.⁵³

The restricted fragment length polymorphism testing (RFLP) usually tests the VNTRs and the polymerase chain reaction (PCR) technique tests the STRs.⁵⁴ The RFLP was the most common test used in the 1990s, and requires a relatively substantial amount of DNA to test effectively.⁵⁵ The PCR is the most common test used today, and requires a smaller amount of DNA because it uses an enzyme that copies and reproduces the relevant allele.⁵⁶ Both tests are effective on nuclear DNA only, and produce a “DNA fingerprint” that scientists can compare to other DNA samples.⁵⁷

45. See Kaye & Sensabaugh, *supra* note 11, at 493.

46. See *id.* at 522. The only exception is identical twins. See *id.*

47. See *id.* at 493.

48. Alleles are nothing more than a selected part of a DNA sequence. Some alleles are individually unique and some are not. For genetic or forensic typing, unique alleles are obviously used. See *id.* at 565.

49. See *id.* at 493.

50. See *id.*

51. Just like fingerprints, a person’s DNA sequence remains constant over time. See *id.*

52. See *id.* at 494.

53. See *id.*

54. See *id.* at 506.

55. See *id.*

56. See *id.* at 497.

Comparing DNA fingerprints to determine a match or exclusion usually involves statistics, probability, and population genetics.⁵⁸

D. Junk DNA?

The preceding background on DNA, DNA sequencing, and DNA testing helps clarify what scientists examine when matching or excluding DNA samples. Today, scientists obtain DNA fingerprints using the RFLP or PCR techniques on a person's junk DNA. As explained previously, junk DNA today tells us nothing about an individual the way a code sequence of DNA (that is, a gene) does. Thus, some argue that a person does not have the same privacy interests in junk DNA as he does in the complete DNA molecule or human genome.⁵⁹ Such an argument attempts to split a hair that should not be split.⁶⁰

Science cannot yet explain junk DNA's purpose. Sometime in the future, however, science will likely know the answer to this riddle. Two current theories are junk DNA shows the history of human and individual evolution (that is, some junk DNA sequences are "fossils" of extinct genes humans no longer need), and other junk DNA sequences affect in unknown ways our cellular protein synthesis.⁶¹ The potential to discover an individual's complete evolutionary history and know and understand a synthesis that affects our body's genetic traits is just as compelling a privacy interest as that which we have in code producing DNA sequences (that is, our genes).

Many people do not want public access to their genetic tendencies to be overweight or to develop cancer (what our genes can today tell about a person's possible future). Likewise, people may not want public access to how an individual's junk DNA sequences may help develop good (or bad)

57. *See id.* at 495. Nuclear DNA (nDNA) is DNA that originates from a cell's nucleus, and is the type of DNA discussed in this article. There is a different kind of DNA that comes from cell's mitochondria (mtDNA). nDNA and mtDNA have no relationship to each other. Comparing mtDNA samples for a match requires direct sequencing, and is done when nDNA is highly degraded. *See id.*

58. *See id.* at 488.

59. *See* David H. Kaye, *The Constitutionality of DNA Sampling on Arrest*, 10 CORNELL J.L. & PUB. POL'Y 455 (2001).

60. *See* discussion *infra* Part V.B.

61. *See* Bob Kuska, *Should Scientists Scrap the Notion of Junk DNA?*, 90 J. NAT'L CANCER INST. 1032 (1998).

proteins that help develop traits. Thus, the pejorative term junk DNA does not justify a lowered privacy interest in that part of a person's DNA sequence. Whatever privacy interest we have in our DNA, the continual advance of scientific inquiry to understand what we did not know yesterday justifies an across the board privacy interest in the entire DNA molecule, and indeed the entire human genome.⁶²

III. DNA and Fingerprint Repositories

While this article's purpose is to explore the Fourth Amendment and its applications to the DOD DNA repository, to better understand that repository, it must be compared to other similar federal repositories. For example, legislation controls how other federal repositories may use their stored information, and other federal repositories have litigated Fourth Amendment issues concerning the personal information they possess. Thus, this part in turn reviews the DOD's DNA Repository, the Combined DNA Index Center, and the National Criminal Information Center.

A. The Armed Forces Repository of Specimen Samples for the Identification of Remains

The DOD DNA Repository developed because of tragedy. On 12 December 1985, 237 members of the 3d Battalion, 502d Infantry Regiment of the 101st Airborne Division (3/502d Infantry) died in a plane crash near Gander, Newfoundland.⁶³ These troops had just completed a United Nations peacekeeping mission in the Sinai Desert and were en route to Fort Campbell, Kentucky, for the holidays.⁶⁴ At the time, experts used dental panorama x-rays to identify human remains from severely traumatic events, like aviation disasters, when fingerprint identification was not possible.⁶⁵ The 3/502d Infantry carried their troops' only dental panorama x-

62. It would be the rare case where DNA and the complete human genome would not both be present in a blood, semen, saliva, or hair sample. Certainly both are present in the blood samples at issue in this article.

63. See David Hoffman, *President Honors Soldiers Killed in Canadian Crash*, WASH. POST, Dec. 17, 1985, at A1. Eleven other soldiers died in the crash; ten from other Army Forces Command units, and one Army Criminal Investigative Division agent. 3/502d Infantry Regiment Homepage, *Tragedy at Gander*, at http://www.campbell.army.mil/3502/tragedy_at_gander.htm (last modified Oct. 15, 2002).

64. See *id.*

65. See Boyer Interview, *supra* note 4.

rays with them, and the crash destroyed the x-rays.⁶⁶ Neither the Army nor the DOD had copies of these x-rays, making identification of many remains from this tragedy problematic.⁶⁷

Following the Gander disaster, the DOD began to centralize the collection and storage of dental panorama x-rays.⁶⁸ The need for centralized records to identify deceased soldiers coincided with the rise of DNA forensic testing for identification. In 1991, the DOD began routinely using DNA to help identify human remains, and following the Gulf War, the DOD directed all servicemembers, active and reserve, to provide a DNA sample for this purpose.⁶⁹ Specifically, on 16 December 1991, the Deputy Secretary of Defense directed the Assistant Secretary of Defense for Health Affairs to formally implement DNA testing to identify servicemembers' remains.⁷⁰ This, in turn, caused the formation of a DNA specimen repository named the Armed Forces Repository of Specimen Samples for the Identification of Remains (AFRSSIR).⁷¹ The AFRSSIR was and is a part of the AFIP.⁷² A separate part of the AFIP, the Armed Forces DNA Identification Laboratory (AFDIL) performs DNA testing to compare samples for identification.⁷³

Today, the AFRSSIR has over four million DNA samples on file and is close to its goal of obtaining a DNA sample from every service member, active and reserve.⁷⁴ The collection procedure is simple and happens, among other times, on induction into the armed forces, reenlistment, and before a troop deployment.⁷⁵ A service member completes requested information on a bloodstain card, watches a technician stain the card with the service member's blood,⁷⁶ and then signs the card.⁷⁷ By signing the

66. *See id.*

67. *See id.*

68. *See id.*

69. *See* Mayfield v. Dalton, 901 F. Supp. 300, 302 (D. Haw. 1995), *vacated*, 109 F.3d 1423 (9th Cir. 1997).

70. *See* Memorandum, The Deputy Secretary of Defense, to Secretaries of the Military Departments et al., subject: Establishment of a Repository of Specimen Samples to Aid in Remains Identification Using Genetic Deoxyribonucleic Acid (DNA) Analysis (16 Dec. 1991).

71. *See* Armed Forces Repository of Specimen Samples for the Identification of Remains Homepage, *Repository History*, at <http://www.afip.org/Departments/oafme/dna/afrssir/index.html> (last visited Nov. 16, 2004).

72. *See id.*

73. *See* Boyer Interview, *supra* note 4.

74. *See id.*

75. *See id.*

card, an individual acknowledges that the blood sample on the card came from him or her, and that the individual read the attached Privacy Act Statement.⁷⁸ The back of the card contains the following Privacy Act Statement:

1. Authority: 10 U.S.C. 131 (Secretary of Defense), 10 U.S.C. 3013 (Secretary of the Army) 10 U.S.C. 5013 (Secretary of the Navy), 10 U.S.C. 8013 (Secretary of the Air Force), and 5 U.S.C. 301 (Departmental Regulations). A response is mandatory for DOD personnel, and possible consequences for failing to respond include adverse administrative actions and punitive disciplinary actions under the Uniform Code of Military Justice. A response is voluntary for DOD civilian personnel selected for the program, but possible consequences for failing to respond include ineligibility for deployment with U.S. Armed Forces, which, if a condition of employment, may result in adverse administrative action up to and including separation from the federal service. A response is voluntary for non-DOD personnel selected for the program, but possible consequences for failing to respond include exclusion from areas under the control of U.S. Armed Forces and hindrance of remains identification efforts.
2. Principal Purpose: Information in this system of records will be used for the identification of human remains. The principal purpose of the information is to identify reference specimen samples that will routinely be stored and not analyzed until needed for remains identification program purposes.
3. Routine Uses: Routine uses include notification to federal, state, local, and foreign authorities of the identification of human remains. Blanket routine uses do not apply to this system.
4. Destruction Notice: Specimen samples not used for identification of remains will be maintained for 50 years, and then destroyed. Samples will be destroyed prior to the scheduled destruction date upon donor request submitted following the conclusion of the donor's complete military service obligation or

76. In 1997, the DOD stopped also collecting oral swabs for a DNA sample. *See* Memorandum, Assistant Secretary of Defense Health Affairs, to DNA Collection Site Personnel, subject: Elimination of Oral Swab Reference Specimen (28 Aug. 1997).

77. *See* Armed Forces Repository of Specimen Samples for the Identification of Remains Homepage, *DNA Specimen Collection Instructions*, at http://www.afip.org/Departments/oafme/dna/afrssir/dnapolicies/coll_instr.pdf (last visited Nov. 16, 2004).

78. U.S. Dep't of Defense, Armed Forces Institute of Pathology, DNA Bloodstain Card (08120) (Jan. 1997).

other applicable relationship to DOD. (Complete military service is not limited to active duty service; it includes all service as a member of the Selected Reserves, Individual Ready Reserves, Standby Reserves, or Retired Reserves.) Requests for early destruction may be sent to Repository Administer, Armed Forces Institute of Pathology, Armed Forces Repository of Specimen Samples for the Identification of Remains, 16050 Industrial Drive, Suite 100, Gaithersburg, MD 20877.⁷⁹

Not surprisingly, the collection of service members' DNA samples has at times been controversial, mainly over a fear of a sample's misuse— notwithstanding that AFRSSIR merely stores the DNA samples and AFIP does not produce a DNA fingerprint until identification of remains becomes an issue. At least three service members, two marines and one airman, have been court-martialed because they each refused to provide a DNA sample.⁸⁰ Each was convicted at their court-martial for failing to obey a lawful order.⁸¹ The two marines then challenged the DOD's collection of DNA samples in federal court.⁸² To address the fear of misuse, the Department of Justice informed the court of the following (as recounted in the court's opinion):

Except for a limited number of "quality assurance" tests in which the DNA is typed to ensure that the repository's storage and analytical mechanisms are working properly, DNA is not extracted from the samples unless and until there is a need for it to assist in the identification of human remains; and [A]ccess to the repository facility, computer system and the samples themselves is strictly limited. Specimens stored in the repository are not to be used for a purpose other than remains identification unless a request, routed through the civilian secretary of the appropriate military service, is approved by the assistant secretary of defense for health affairs. The government notes that no such request from this program has ever been approved, though it is unclear how many, if any, such requests have been made.⁸³

79. *Id.*

80. See Sarah Gill, *The Military's DNA Registry: An Analysis of Current Law and a Proposal for Safeguards*, 44 *NAVAL L. REV.* 175, 175 (1997).

81. *See id.*

82. See *Mayfield v. Dalton*, 901 F. Supp. 300 (D. Haw. 1995), *vacated*, 109 F.3d 1423 (9th Cir. 1997) (stating that both marines had been honorably discharged after their courts-martial, and after the district court entered its decision, mooting the case on appeal).

Department of Defense Directive 5154.24 implements, *inter alia*, the DOD's concern to protect an individual's privacy interest in his AFRSSIR DNA sample.⁸⁴ It mandates that the AFRSSIR will "[I]mplement special rules and procedures to assure the protection of privacy interests in the specimen samples and any DNA analysis of those samples in accordance with subsection 3.5."⁸⁵

Paragraph 3.5.1, *DOD Dir. 5154.24* limits DNA sample uses to the following: identification of human remains, internal quality assurance tests, any use of which the donor (or surviving next of kin) consents, and a criminal investigation or prosecution in which all of the following conditions are present:

1. The responsible DOD official has received a proper judicial order or judicial authorization;
2. The specimen sample is needed for the investigation or prosecution (sic) of a crime punishable by one year or more of confinement;
3. No reasonable alternative means for obtaining a specimen for DNA profile analysis is available; and
4. The use is approved by the Assistant Secretary of Defense for Human Affairs after consultation with the General Counsel of the Department of Defense.⁸⁶

Thus, when a service member provides a mandatory DNA sample, he or she may, in part, determine their continuing privacy interest in that sample by: science's continual study and understanding of DNA, the human genome, and the human proteome; the executive branch's statements to a federal court concerning the AFRSSIR DNA samples; the Privacy Act statement on the back of a bloodstain card; and *DOD Dir. 5154.24*. In other words, based on these sources, do servicemembers continue to have a privacy interest in their AFRSSIR DNA samples, and if yes, what is the extent of that interest? To help answer those questions, this article compares the AFRSSIR identification databank with other identification databanks.

83. *Id.* at 302.

84. *See* DOD DIR. 5154.24, *supra* note 2.

85. *Id.* at 4.

86. *Id.* at 6-7.

B. The Combined DNA Index System

Given the rise and reliability of DNA forensic testing, Congress directed the Federal Bureau of Investigation (FBI), via the DNA Identification Act of 1994 and the DNA Analysis Backlog Elimination Act of 2000, to create and implement a Combined DNA Index System (CODIS).⁸⁷ The CODIS's mandates are to gather DNA samples from certain persons, profile those samples using the techniques described in Part II.C, and then enter the resulting DNA fingerprint into a searchable computer databank.⁸⁸ Some of Congress's stated purposes in implementing this Act were to exonerate the wrongly accused and convicted, help identify suspects, and convict the rightly accused.⁸⁹

Deoxyribonucleic acid samples for the CODIS databank come from the following sources: (a) convicted state,⁹⁰ federal,⁹¹ and military⁹² offenders of "qualifying offenses"⁹³ who are currently incarcerated or are on release, parole, or probation; (b) unidentified DNA samples discovered at crime scenes or on crime victims; (c) unidentified human remains; and (d) family members of missing persons who voluntarily donate a sample.⁹⁴ For those individuals who are currently incarcerated or on release, parole, or probation for a qualifying offense, providing a DNA sample is mandatory. Refusing to provide a mandatory sample or even failure to cooperate can result in forcible retraction of a sample, administrative sanctions, revo-

87. 42 U.S.C. §§ 14131-14135e (2000).

88. *See id.* § 14135a.

89. *See id.* § 14134 (congressional findings).

90. States make up their own list of qualifying offenses. Thus, qualifying crimes are similar, but usually differ, between state jurisdictions. *See id.* § 14132.

91. *See id.* § 14135b (including the District of Columbia).

92. Each service secretary is responsible for collecting DNA samples from their service's qualifying offenders, and then forwarding those samples to the Secretary of Defense. The Secretary of Defense is then responsible for analyzing the DNA sample to produce a DNA fingerprint for inclusion in the CODIS databank. The author understands this process as the various military confinement centers take samples from qualifying offenders, and then send the samples to the AFIDIL for analysis. The AFIDIL then forwards the resulting DNA fingerprint to the FBI for inclusion in CODIS. 10 U.S.C.S. § 1565 (LEXIS 2003).

93. Qualifying offenses usually include all sexual offenses and most felony offenses. *See, e.g.*, 42 U.S.C § 14135a.

94. *See id.* § 14132.

cation of release, parole, or probation, a separate criminal charge, or some combination thereof.⁹⁵

Congress placed statutory limits on the CODIS databank's use, the violation of which authorizes a criminal penalty.⁹⁶ Specifically, the results of CODIS DNA analysis may be disclosed to criminal justice agencies for law enforcement identification purposes, in judicial proceedings, and to assist criminal defendants.⁹⁷ Exceptions to these "privacy protection standards" (as the statute names them) are tests and results that assist in protocol development and quality control.⁹⁸ Another exception allows use of the CODIS DNA analysis for a population statistics database and for identification research.⁹⁹ Before any exception can apply, however, CODIS personnel must remove all personally identifiable information from the DNA analysis.¹⁰⁰ Neither the statute nor implementing regulations¹⁰¹ define the term "personally identifiable information," but the term likely means that, for an exception to apply, there must be no way to link a DNA fingerprint stored in the CODIS databank with an individual's name.

The different purposes between the CODIS databank and the AFRS-SIR databank result in a fundamental difference between the databanks. For CODIS to work, a technician must analyze and profile each DNA sample resulting in a DNA fingerprint that the technician can then place in a searchable computer database. The AFRSSIR, however, does not initially profile the DNA samples it receives. Instead, the AFRSSIR merely stores the blood samples for possible later use in identifying remains. Thus, consistent with CODIS's purpose to help solve crimes, CODIS can conduct a blind search of an unknown DNA sample taken from a crime scene for any matches in their computer database. The AFRSSIR does not profile its samples on receipt, and therefore cannot conduct a blind computer database search upon request.¹⁰²

C. The National Crime Information Center

95. *See id.* § 14135a.

96. The statute explicitly authorizes the imposition of a fine of not more than \$100,000. *See id.* § 14135e.

97. *See id.* § 14132(a)(3).

98. *See id.* § 14133(b)(2).

99. *See id.*

100. *See id.*

101. *See* Collection and Use of DNA Information, 28 C.F.R. subpt. 812.4 (LEXIS 2004).

Federal law charges the FBI to manage the National Crime Information Center (NCIC).¹⁰³ The NCIC links, by computer and telecommunications, local, state, tribal, federal, foreign, and international criminal justice agencies.¹⁰⁴ The NCIC's purpose is to identify first time offenders of qualifying offenses (including arrests for those offenses and protection orders)¹⁰⁵ and to identify previously unknown or unidentified suspects via information already entered in the NCIC.¹⁰⁶

The following systems make up the NCIC: the Fingerprint Identification Records System (FIRS); Interstate Identification Index System (III System); and criminal history record repositories of participating criminal justice agencies.¹⁰⁷ Fingerprint records submitted by participating criminal justice agencies, individuals' criminal histories (that is, rap sheets), and a list of all names included in the fingerprint and rap sheet records make up FIRS.¹⁰⁸ The III System also contains fingerprint data, but includes other identifying data like tattoos and social security numbers as well.¹⁰⁹

The NCIC mostly consists of information submitted at the state level and below. A typical scenario follows: A local jurisdiction arrests a suspect. Within twenty-four hours, that local jurisdiction submits the individual's "name, date of birth, fingerprints, tattoos, aliases, sex and race" in the NCIC computer system using a NCIC control terminal agency.¹¹⁰ The

102. The AFRSSIR Internet home page does discuss a database search, but this is merely a database containing the names of individuals who have given a sample. This type of search is necessary so multiple DNA samples from the same individual do not clog the system. For those who have served in the military, it is easy to imagine that a first sergeant may not take a Private's word that the private previously gave a DNA sample. Thus, units can verify with the AFRSSIR which of their service members needs to donate a DNA sample. See Armed Forces Repository of Specimen Samples for the Identification of Remains Homepage, *Database Query*, at <http://www.afip.org/Departments/oafme/dna/afrssir/database.html> (last visited Nov. 16, 2004). Also note that the AFRSSIR system assumes that the military will have a good idea of the identity of human remains that require conclusive identification, thus eliminating the need for a blind computer database search. For example, flight manifests or troop rosters coupled with already identified remains will narrow the possibilities in most cases to just a few persons.

103. See 28 U.S.C. § 534 (2000). The Attorney General delegated this responsibility to the Federal Bureau of Investigation. See Criminal Justice Information Systems, 28 C.F.R. § 20.31(a).

104. See 28 C.F.R. § 20.3(n).

105. See 28 U.S.C. § 534(e).

106. See *United States v. Walker*, 92 F.3d 714, 716 (8th Cir. 1996).

107. See 28 C.F.R. subpt. 20.3.

108. See *id.* § 20.3(l).

109. See *id.* § 20.3(m).

NCIC enters that information into its databanks, then compares that information against its databanks to ensure both that the individual gave his or her correct identification and also that another jurisdiction does not have charges pending.¹¹¹ Should another jurisdiction want the individual, the FBI sends an immediate notice of the NCIC “hit” to both the retaining and seeking jurisdictions.¹¹² The local jurisdiction assumes responsibility for the correctness of its entries, and has a duty to update its entries as any particular case progresses through the criminal justice system.¹¹³

Both federal statute¹¹⁴ and regulation¹¹⁵ govern privacy concerns raised by the NCIC’s databanks. Generally, these provisions make it unlawful to access or distribute the information contained in the NCIC’s databanks if not done for an official purpose. Absent a state law limiting such a disclosure, however, federal law does not prohibit release of arrest or conviction data to the public.¹¹⁶ Thus, under this scheme, the federal government protects from disclosure only something called “non-conviction data.”¹¹⁷

IV. Statutory Schemes That Address When the Executive Branch Can Release Records

The Privacy Act of 1974¹¹⁸ and the Freedom of Information Act (FOIA)¹¹⁹ are two federal statutory schemes that address how the federal government releases information it possesses. The Privacy Act recognizes that the federal government acquires immense quantities of information about individuals.¹²⁰ Concern for the privacy of this information produced the Privacy Act and its general rule of not releasing personal information to third parties without a subject’s consent.¹²¹ There are, however, twelve

110. *Walker*, 92 F.3d at 716.

111. *See id.*

112. *See id.*

113. An acquittal or dismissal is not a reason to remove an existing record from the NCIC. *See* 28 C.F.R. § 20.37.

114. 5 U.S.C. § 534(b) (2000).

115. 28 C.F.R. § 20.21(b).

116. *See id.* pt. 20 app.

117. Non-conviction data is defined at *id.* § 20.3(q). The distinction between conviction and non-conviction data attempts to strike a balance between not allowing certain information to employers versus the constitutional right of the freedom of the press. *See id.*

118. 5 U.S.C. § 552a.

119. *Id.* § 552.

120. *See Cardamone v. Cohen*, 241 F.3d 520, 524 (6th Cir. 2001).

exceptions to the Privacy Act's general rule.¹²² The FOIA's purpose, on the other hand, is to help ensure the public understands government operation.¹²³ The FOIA's general rule is federal agencies should provide information about how the agency works to the public, but there are also several exceptions and exemptions to the FOIA's general rule of disclosure.¹²⁴

Oftentimes, requests to federal agencies for information will cite both the Privacy Act and the FOIA as independent justification for the release of the requested information. In such cases, the agency must analyze the request under both statutes to determine if information is releasable. Federal agencies in receipt of requests for information will often conduct this dual analysis even when the request does not cite both statutes.¹²⁵ Thus, to help answer the questions posed in this article's hypotheticals, this article will review both statutes as they apply to the AFRSSIR DNA samples.

A. The Privacy Act

To ensure citizens have some control over personal information collected by the federal government, the Privacy Act, *inter alia*, requires executive agencies to give public notice¹²⁶ of any "system of records," and limits disclosure of records based on who is requesting the records the subject or a third person.¹²⁷ A system of records is records under agency control about an individual and that can be retrieved by an individual's name or identifying particular.¹²⁸ The AFRSSIR DNA samples probably fall

121. *See id.*

122. *See id.*

123. *See Doe Agency v. Doe Corp.*, 493 U.S. 146, 152 (1989).

124. *See id.*

125. *But see Bartel v. Fed. Aviation Admin.*, 725 F.2d 1403 (D.C. Cir. 1984).

126. The purpose of the public notice is to give the public an opportunity to comment on the use of a system of records before an agency implements such use. *See* 5 U.S.C. § 552a(e)(11).

127. *See id.* § 552a(b).

128. *See id.* § 552a(a)(4) & (5).

within the definition of a system of records,¹²⁹ and the DOD accordingly gave public notice in the *Federal Register*.¹³⁰

The public notice requires inclusion of several topics of disclosure, including the routine uses of the records, the purpose of the users, and blanket routine uses. In pertinent part, the AFRSSIR's public notice states as follows:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DOD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

....

To a proper authority, as compelled by other applicable law, in a case in which all of the following conditions are present:

[same language as contained in paragraph 3.5.1 of DODD 5154.24, at Part III.A];

The Army's Blanket Routine Uses do not apply to this system.¹³¹

Thus, the AFRSSIR publicly states its intent that a routine use of its blood samples is to assist law enforcement if, and only if, law enforcement has a judicial order.¹³² That does not end the inquiry under the Privacy Act, however, for one must next consider if any statutory exception allows disclosure of the AFRSSIR DNA samples.

There are twelve exceptions to the Privacy Act's general rule that an agency cannot disclose a record to a third person without the subject's consent, three of which are relevant to our inquiry.¹³³ First, 5 U.S.C. §

129. A system of records includes "any item, collection, or grouping of information about an individual that is maintained by an agency, including . . . other identifying particular assigned to the individual, such as a finger or voice print . . ." *Id.* § 552a(a)(4). Arguably, the AFRSSIR blood samples are not records under this definition because the AFIP has not done a DNA fingerprint for each sample. Nevertheless, the DOD's public notice lists "specimen collections" as a category of records. *See* Notice to Amend System of Records, 63 Fed. Reg. 10,205 (Mar. 2, 1998).

130. 63 Fed. Reg. at 10,205.

131. *Id.* Federal agencies, including the DOD and the Army underneath it, can and do list blanket routine uses that all of their systems of records are subject to, unless a particular system opts out of these blanket uses. The Army's blanket use contains a law enforcement routine use, but the AFRSSIR opts out of that use for its samples. *See* Notice to Amend Preamble to System of Records Notice, 66 Fed. Reg. 7745 (Jan. 21, 2001), *available at* http://www.defenselink.mil/privacy/notices/army/army_preamble.html (last modified Oct. 9, 2002).

552a(b)(3) allows disclosure pursuant to a published routine use.¹³⁴ As just shown, the AFRSSIR's routine use incorporates *DOD Dir. 5154.24*'s restrictive language. Second, 5 U.S.C. § 552a(b)(2) requires disclosure when the FOIA requires release of the record.¹³⁵ The next subheading will discuss the FOIA and if that statute requires release of the AFRSSIR DNA samples. Third, 5 U.S.C. § 552a(b)(7) (Exception 7) provides, under certain conditions, for disclosure of records to law enforcement with no warrant requirement.¹³⁶ Given that DOD, by its own directive, requires a warrant before releasing an AFRSSIR DNA sample, does *DOD Dir. 5154.24*, and the principle behind it, trump Exception 7?

As a general rule, a federal statute trumps an executive agency's directive to the degree they conflict.¹³⁷ A inquiry, however, must go deeper than that. If a statute produces an unconstitutional result, courts will stop or reverse such effects. Thus, if service members maintain a reasonable expectation of privacy in their AFRSSIR blood samples, then providing those samples to law enforcement without a warrant presumptively

132. Although *DOD Dir. 5154.24* requires, *inter alia*, a judicial order, this term should be interpreted to mean a warrant or search authorization and not a subpoena. Usually, any party to a civil or criminal trial may issue a subpoena, but a judge can quash subpoenas issued in violation of the law. See *United States v. Scaduto*, No. 94Cr.311(WK), 1995 U.S. Dist. LEXIS 3715 (S.D.N.Y. Mar. 24, 1995). Importantly, the Supreme Court held in *United States v. Miller*, 425 U.S. 435 (1976) that if an individual holds a reasonable expectation of privacy in a record held by a third-party, this requires a court, upon proper motion, to quash a subpoena duces tecum to the third-party holding that record.

133. 5 U.S.C. § 552a(b)(1)-(12) (2000).

134. See *id.* § 552a(b)(3).

135. See *id.* § 552a(b)(2).

136. Exception 7 provides that disclosure:

[T]o another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.

Id. § 552a(b)(7).

137. See *Int'l Ass'n of Machinists & Aerospace Workers v. Wisconsin Employment Relations Comm.*, 427 U.S. 132 (1976).

violates service members' Fourth Amendment protections.¹³⁸ The article addresses this issue in Part V.

B. The Freedom of Information Act

Unlike the Privacy Act, the FOIA's general rule is to disclose requested agency records unless one of three exceptions or nine exemptions applies.¹³⁹ Only one exemption is relevant to this article's inquiry, the FOIA's Exemption 6.¹⁴⁰ Exemption 6 permits an agency to withhold records that are "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."¹⁴¹ The Supreme Court has defined similar files as information of a personal nature.¹⁴² Clearly, if service members maintain a reasonable expectation of privacy in their AFRSSIR DNA samples, then those samples contain information of a personal nature.¹⁴³

Freedom of Information Act Exemption 6 also requires a balancing between the privacy interest at stake and the public's interest in disclosure. In *Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court held that the only public interest in this balancing test is FOIA's core purpose: will the requested information shed light on how an agency performs its duties?¹⁴⁴ If not, even a minimal privacy interest authorizes withholding the requested agency records.¹⁴⁵

138. See *Kiraly v. FBI*, 728 F.2d 273, 275 (6th Cir. 1984) (saying that an unwarranted invasion of privacy precludes disclosure under both the Privacy Act and the FOIA).

139. 5 U.S.C. § 552. Note that neither FOIA nor the Privacy Act requires an agency to create records. See *Flight Safety Serv. Corp. v. Dep't of Labor*, No. 3:00-CV-1285-P, 2002 US Dist. LEXIS 8811 (N.D. Tex. May 16, 2002). Because the AFRSSIR does not make or keep DNA fingerprints, the law may not require the AFRSSIR to make such records upon a request to do a blind search of their samples. *But see supra* note 130.

140. See 5 U.S.C. § 552(b)(6).

141. *Id.*

142. See *Dep't of State v. Washington Post*, 456 U.S. 595 (1986).

143. Outside a Fourth Amendment analysis, the legal community is beginning to consider whether DNA should fall under the penumbra of constitutional rights that, taken together, protect an individual's right to privacy. See Jeffrey S. Grand, Note, *The Bleeding of America: Privacy and the DNA Dragnet*, 23 *CARDOZO L. REV.* 2277 (2002). Freedom of Information Act Exemption 6 does not set the bar so high, however, that a constitutional right must be at stake to justify withholding. See *infra* text accompanying notes 146-47.

144. 489 U.S. 749 (1989).

145. See *Nat'l Ass'n of Retired Fed. Employees v. Horner*, 879 F.2d 873, 879 (D.C. Cir. 1989).

V. The Fourth Amendment

The Fourth Amendment paradigm, developed by Supreme Court precedent, provides a framework to analyze search and seizure issues. Courts continue to resolve fact patterns within the framework, but individual cases sometimes do not fit neatly within the borders of existing precedent. Thus, a change in circumstances may call into question whether the rationale for a particular precedent applies to a new case. If those changed circumstances are compelling, the court may distinguish a case or set aside the precedent.

The rapid rise of DNA use and our collective knowledge of the human genome represent a vast escalation of what cells and molecules from our bodies can tell others about us. Prosecutors and defense counsel alike appreciate DNA and the underlying science because such samples often establish guilt or innocence. Yet, as discussed in Part II, the DNA molecule is much more than a fingerprint, because it can tell others about our genetic history and genetic future. Thus, this article next considers existing Fourth Amendment precedent and determines how DNA, and specifically the AFRSSIR DNA samples, best fit within the paradigm.

A. The Fourth Amendment Paradigm

Criminal lawyers know the Fourth Amendment mantra by heart. The Fourth Amendment protects against unreasonable government searches and seizures.¹⁴⁶ Courts presume a law enforcement search unreasonable when done without a warrant or search authorization based on probable cause unless certain court-created exceptions apply.¹⁴⁷ A warrantless government search, however, is reasonable when the person objecting to the search does not have a reasonable expectation of privacy in the thing

146. The Fourth Amendment states in its entirety that

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend IV. The Fourteenth Amendment to the Constitution makes the Fourth Amendment applicable to the States. *See* *Schmerber v. California*, 384 U.S. 757, 766 (1966).

147. *See* *Preston v. United States*, 376 U.S. 364 (1964).

searched.¹⁴⁸ Courts consider both an objective and subjective prong to determine whether a person enjoys a reasonable expectation of privacy: does the person, based on her conduct, have a subjective expectation of privacy in the thing searched?; and is society willing to recognize a privacy interest in the thing searched?¹⁴⁹ A court must say yes to both prongs before the Fourth Amendment applies, presumptively requiring the government to obtain a search warrant or authorization to search.¹⁵⁰

1. The Supreme Court Addresses Bodily Intrusions and Chemical Analysis

The Supreme Court considered *Schmerber v. California*,¹⁵¹ a driving while intoxicated case, in 1966. In *Schmerber*, the defendant consumed alcohol at a bowling alley before he and a friend left in a vehicle driven by the defendant.¹⁵² Shortly after leaving, the defendant's car skidded off the road and hit a tree.¹⁵³ While the defendant received medical treatment, the police ordered medical personnel to also withdraw a blood sample from the defendant to determine the defendant's blood-alcohol content.¹⁵⁴ The defendant objected at the time the sample was drawn and again at his trial when the prosecution offered into evidence his blood-alcohol content.¹⁵⁵

First, the Court ruled that although the police obtained no warrant to extract the defendant's blood to test it for alcohol content, they clearly had probable cause to do so.¹⁵⁶ Second, the Court found that any intrusion of the body to withdraw blood squarely implicated Fourth Amendment concerns.¹⁵⁷ Indeed, the Court noted it was the first time they had considered bodily intrusions under the Fourth Amendment, that their prior precedents

148. See *Katz v. United States*, 389 U.S. 347 (1967).

149. See *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

150. See *id.*

151. 384 U.S. 757 (1966).

152. See *id.* at 758.

153. See *id.*

154. See *id.*

155. See *id.* at 759.

156. Both at the scene of the accident and at the hospital, the defendant showed signs of drunkenness. See *id.* at 768.

157. See *id.* at 767.

concerning government searches of property were not helpful, and that they therefore were writing on a “clean slate.”¹⁵⁸

The Court went on to note the important policy of protecting “personal privacy and dignity” which the Fourth Amendment represents.¹⁵⁹ On these facts, however, the Court found the police acted reasonably without getting a search warrant because there was probable cause to believe the defendant had committed a crime, and it was reasonable for the police to believe exigent circumstances existed because of diminishing blood-alcohol content over time.¹⁶⁰ The Court therefore recognized a bodily intrusion exception to the Fourth Amendment’s warrant requirement, provided trained medical personnel perform the extraction and exigent circumstances exist.¹⁶¹ Before this emergency exception applies, however, law enforcement must have probable cause to believe that the body fluid sought will contain evidence of a crime.

The Supreme Court’s next important case addressing the Fourth Amendment and bodily intrusions to test body fluids came in *Skinner v. Railway Labor Executives’ Association*.¹⁶² In *Skinner*, various groups representing railroad workers sought injunctive relief against compelled blood, urine, and breath tests performed by the railroads on their workers to detect and deter alcohol and drug use.¹⁶³ The workers sought injunctive relief based partly on the premise that the compelled tests violated their Fourth Amendment rights.¹⁶⁴ *Skinner* upheld the federal regulations authorizing the compelled tests, and in doing so provided a Fourth Amendment analysis applicable to issues presented in this article.

The Court explained that a governmental intrusion into a body to take blood usually invokes the Fourth Amendment at two levels: the detention of the person necessary to make the extraction, and the subsequent chemical analysis of the sample.¹⁶⁵ The Court also held that chemical analysis of a urine or breath sample similarly invokes Fourth Amendment privacy concerns.¹⁶⁶ Important for any subsequently considered DNA analysis, the Court said a chemical analysis of urine was a Fourth Amendment

158. *See id.* at 768.

159. *See id.* at 767.

160. *See id.* at 772.

161. *See id.*

162. 489 U.S. 602 (1989).

163. *See id.* at 612.

164. *See id.*

165. *See id.* at 616.

search because the analysis could “reveal a host of private medical facts about an employee, including whether he is epileptic, pregnant, or diabetic.”¹⁶⁷

The Court then stated that determining the Fourth Amendment applies (that is, that railroad workers have a reasonable expectation of privacy in their blood, urine, and breath when the government seeks to chemically analyze those samples) is only the beginning of the inquiry, for it must next determine if the government acted reasonably in doing the search (that is, chemical analysis) without a warrant.¹⁶⁸ To determine if the government acted reasonably, the Court announced it must weigh the privacy interests at stake against the legitimate governmental interest promoted by the search.¹⁶⁹ Within this balancing test, the Court also put forth a “special needs” test for the government: a special need beyond law enforcement that makes obtaining a warrant impracticable.¹⁷⁰

The Court articulated the government’s special need to adequately regulate the railroad industry as the need to prevent accidents, especially when studies showed that industry had a drug and alcohol problem.¹⁷¹ Locomotives and railcars could become lethal when operated by those under the influence of drugs or alcohol.¹⁷² The Court then balanced the government’s public safety concern against the privacy interests at stake by focusing on the manner used to gain the blood, breath, or urine.¹⁷³ The Court held that the bodily intrusions to get a blood or breath sample were insignificant when weighed against the need for public safety.¹⁷⁴ The Court also upheld the search of the urine samples using the same rationale,

166. *See id.* at 616-18. The Court stated that a chemical analysis by the government of blood, breath, or urine was a search under the Fourth Amendment. The Court also noted that obtaining blood and urine samples might also be a seizure under the Fourth Amendment, but that its analysis protected the privacy interest regardless whether the facts presented a search or seizure of bodily fluids. *See id.*

167. *Id.* at 617.

168. *See id.* at 619.

169. The Court restated that a search without a warrant presumptively violates the Fourth Amendment, but would consider a balancing test or special needs test to overcome the presumption. *See id.*

170. *See id.* at 619-20.

171. *See id.*

172. *See id.*

173. *See id.*

174. *See id.* at 625. The Railroad did not test its employees randomly, but tested entire crews after an accident. *See id.*

but hinted it may have reached a different conclusion if an observer directly watched an employee urinate.¹⁷⁵

Finally, finding the public need for safety so great, the Court held that the government could obtain the samples to test for drug or alcohol use even when probable cause was not present.¹⁷⁶ Given the public safety need, the government still acted reasonably conducting a search of blood, breath, or urine samples even when there was no individualized suspicion of wrongdoing.¹⁷⁷ *Skinner*, however, does not overrule *Schmerber* and its holding that law enforcement must generally have probable cause to test for drug or alcohol use. In *Skinner*, the railroads did the search to protect public safety, and not for a law enforcement purpose. Given that *Schmerber* and *Skinner* are reconcilable, how have courts squared these holdings with challenges to the CODIS system? The Supreme Court has not yet addressed the issue, but several federal appellate courts have.

2. *Federal Courts and CODIS*

Recall that CODIS requires state or federal governments to extract a DNA sample from those convicted of certain crimes who are incarcerated or on release, parole, or probation.¹⁷⁸ No current probable cause supports this governmental extraction of DNA. Indeed, there is usually no known crime under investigation when the government obtains the sample. Every federal appellate court to date that has considered the issue, however, has held that CODIS does not violate the Fourth Amendment, using either a balancing test or a special needs test. Two recent Supreme Court decisions, however, call into question the continuing validity of these past precedents, as explained in a recent federal district court decision.

a. *The Balancing Test*

Most federal appellate courts that have considered the constitutionality of CODIS under the Fourth Amendment rely on a balancing test between an individual's privacy interests and the governmental interest at stake.¹⁷⁹ For example, in *Jones v. Murray*, a Fourth Circuit case reviewing

175. *See id.* at 626.

176. *See id.* at 629.

177. *See id.*

178. *See supra* text accompanying note 88.

Virginia's version of CODIS,¹⁸⁰ the court found governmental interests in CODIS included obtaining an accurate way to identify felons (because felons possess a motive to change or alter their identities), helping solve past and future crimes, and acting as a deterrent to recidivism.¹⁸¹ These interests outweighed the minimal intrusion of drawing blood by medical personnel.¹⁸²

Jones recognized that the CODIS required no probable cause or suspicion to conduct a search, but, in a clever juxtaposition, piggybacked on the probable cause that brings a convict into the criminal justice system.¹⁸³ The court said:

We have not been made aware of any case, however, establishing a per se Fourth Amendment requirement of probable cause, or even a lesser degree of individualized suspicion, when government officials conduct a limited search for the purpose of ascertaining and recording the identity of a person who is lawfully confined to prison. This is not surprising when we consider that probable cause had already supplied the basis for bringing the person within the criminal justice system. 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.¹⁸⁴

Partially relying on *Jones*, the Ninth Circuit in *Rise v. Oregon*¹⁸⁵ also upheld Oregon's version of CODIS.¹⁸⁶ *Rise* found that the minimal intrusion to draw blood did not outweigh the significant public interest in accu-

179. See, e.g., *Shaffer v. Saffle*, 148 F.3d 1180, 1181 (10th Cir.), cert. denied, 525 U.S. 1005 (1998); *Boling v. Romer*, 101 F.3d 1336, 1340 (10th Cir. 1996); *Rise v. Oregon*, 59 F.3d 1556 (9th Cir. 1995), cert. denied, 517 U.S. 1160 (1996); *Jones v. Murray*, 962 F.2d 302, 306 (4th Cir.), cert. denied, 506 U.S. 977 (1992). None of these cases considers the constitutionality of CODIS, but rather the constitutionality of state DNA databanks similar to CODIS.

180. 962 F.2d 302, 304 (4th Cir.), cert. denied, 506 U.S. 977 (1992). Virginia's version of CODIS required anyone convicted of a felony after a certain date to provide a DNA sample. See *id.*

181. See *id.* at 307.

182. See *id.*

183. See *id.* at 306.

184. *Id.*

185. 59 F.3d 1556 (9th Cir. 1995), cert. denied, 517 U.S. 1160 (1996).

186. See *id.* at 1558. Oregon's version of CODIS required only sexual offenders and those convicted of certain violent crimes to provide DNA samples. See *id.*

rately identifying certain felons.¹⁸⁷ Unlike *Jones*, however, *Rise* coupled the drawing of blood with a convicted felon's diminished privacy interest in his or her identification: holding a convicted felon does not have a reasonable expectation of privacy in his identification, including DNA identification from a drawn blood sample.¹⁸⁸ While the court went on to perform a Fourth Amendment balancing test, under the court's logic, the weighing of state and individual interests was not relevant. A balancing test is only necessary if the Fourth Amendment applies, and if there is no expectation of privacy, then the Fourth Amendment does not apply.¹⁸⁹

b. The Special Needs Test

The Second Circuit, in *Roe v. Marcotte*,¹⁹⁰ also upheld the constitutionality of Connecticut's version of CODIS,¹⁹¹ but went to lengths to distinguish their reasoning from other federal circuits that used a Fourth Amendment balancing test.¹⁹² In *Marcotte*, convicted sexual offenders sought an injunction prohibiting the state's attorney general from forcibly obtaining a DNA sample.¹⁹³ The Court made quick work of the plaintiffs' Fourth Amendment arguments, acknowledging that the analysis of blood constituted a search, but that the government's special needs allowed the government to proceed without a search warrant.¹⁹⁴

Marcotte articulated the government's special needs as follows:

[D]efendants 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 testing. Defendants argue that the existence of state and national DNA data banks will serve an important governmental interest

187. *See id.* at 1562.

188. *See id.* at 1560.

189. *See Skinner, Sec'y of Transp. v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 619 (1989).

190. 193 F.3d 72 (2d Cir. 1999).

191. Connecticut's version of CODIS in place at time of the court's decision only required sexual offenders to provide DNA samples. *See id.* at 74.

192. *See id.* at 81.

193. *See id.* at 74.

194. *See id.* at 80.

in solving both past and future crimes. More importantly, they contend that the statute's requirement that imprisoned sexual offenders provide a DNA sample will deter these individuals from committing future offenses of a similar nature. Balanced against this significant interest is the drawing of a blood sample for testing, an intrusion that the Supreme Court has characterized as minimal.¹⁹⁵

The *Marcotte* Court felt it important to justify its holding under the special needs test, because as the Supreme Court explained in *Skinner*, if the government has a special need separate from its law enforcement role, it may proceed to search without probable cause.¹⁹⁶ Thus, the *Marcotte* Court believed that if it applied a Fourth Amendment balancing test to Connecticut's version of CODIS, it must first have concluded that Connecticut was acting for a law enforcement purpose and that any search would require probable cause or "at the very least some quantum of individualized suspicion."¹⁹⁷ Because obtaining CODIS DNA samples never entails individualized suspicion, the Court determined it was intellectually dishonest to justify CODIS under a Fourth Amendment balancing test.

c. The Supreme Court Reasserts The Paradigm

Some might argue that the Fourth Amendment's balancing test and special needs test create exceptions that swallow the Fourth Amendment's mandate that the government must obtain a warrant to search. Two Supreme Court cases cut against this argument, however. First, the Court, in *City of Indianapolis v. Edmond*,¹⁹⁸ reaffirmed the general rule that if a search or seizure's primary purpose is for general law enforcement, then the police must honor the Fourth Amendment's warrant requirement.¹⁹⁹

In *Edmond*, the city of Indianapolis conducted roadblocks to temporarily detain vehicles so drug-sniffing canines could sniff a vehicle's exterior and police could observe the vehicle's occupants.²⁰⁰ If a dog made a "hit" or if police officers on the scene had reason to believe drugs were in

195. *Id.* at 79.

196. *O'Connor v. Ortega*, 480 U.S. 709 (1987) and *Griffin v. Wisconsin*, 483 U.S. 868 (1987), also concluded that special needs other than the needs of normal law enforcement will make a search unsupported by either a warrant or probable cause reasonable.

197. *Marcotte*, 193 F.3d at 77 (internal citations and quotations omitted).

198. 531 U.S. 32 (2000).

199. *See id.*

a vehicle, they would then search the vehicle.²⁰¹ The Court ruled the primary purpose of looking for drugs was nothing more than a general law enforcement stop, and it distinguished this case from previous decisions where the Court allowed police roadblocks to check for valid licenses and registrations or drunk drivers.²⁰² In those cases, the Court said the primary purpose of the roadblocks was a general safety concern: only qualified, unimpaired drivers should operate motor vehicles.²⁰³

Second, the Court, in *Ferguson v. City of Charleston*,²⁰⁴ struck down a state hospital's regulation that required the hospital to give prosecutors positive drug tests done on urine samples from pregnant women.²⁰⁵ The hospital justified its actions, because its employees had noticed many expectant mothers that came to the hospital for state provided pre-natal care also abused drugs.²⁰⁶ To deter this drug use, the state hospital announced its plan to test expectant mothers for drug use and provide positive test results to local prosecutors.²⁰⁷

The Court applauded the social goal of reducing drug use, but found the hospital's plan violated the Fourth Amendment. In essence, the state hospital conducted warrantless and suspicionless searches of urine and used the results of the search for a law enforcement purpose, even though the eventual goal was to deter drug use.²⁰⁸ Such a result could not qualify as a special need because of the plan's entanglement with law enforcement.²⁰⁹ The Court then paradoxically said the state hospital's plan could also not meet the Fourth Amendment reasonableness standard under a bal-

200. The Court stated the roadblock stop amounted to a seizure, but that the drug-sniffing canine on a vehicle's exterior did not amount to a search. *See id.* at 40 (internal citations omitted).

201. *See id.*

202. The Court said it was not ruling on roadblocks where a secondary purpose of the stop may be to search for drugs. Thus, for police to avoid the Court's holding, a roadblock's primary purpose could be to permissibly check a license and registration, and its secondary purpose could be to detect drugs. The Court mentioned this possibility when it noted courts decide a roadblock's primary purpose. *See id.* at 46-7.

203. *See id.*

204. 532 U.S. 67 (2001).

205. *See id.*

206. *See id.* at 69.

207. The Court assumed the tested women did not provide informed consent to this practice. *See id.* at 76.

208. *See id.* at 82.

ancing test because the Court had used that test to uphold only the road-block seizures.²¹⁰

d. The General Prohibition Against Law Enforcement Searches Without a Warrant and CODIS

Given the reemergence in Supreme Court cases prohibiting general law enforcement searches without a warrant, convicted felons continue to challenge CODIS. Three separate federal district courts reviewed CODIS in published decisions after *Ferguson* and *Edmond*.²¹¹ The district courts split their decisions, one court ruling that the federal version of CODIS was unconstitutional, while the other two courts continued to find CODIS constitutional.

In *United States v. Miles*, the court considered the various purposes of CODIS and determined its primary purpose was for law enforcement (that is, to accurately solve crimes).²¹² Accordingly, *Miles* (a Ninth Circuit district court decision) found *Edmonds* and *Ferguson* overruled *Rise*, and found CODIS unconstitutional, because it required an individual to submit to a warrantless and suspicionless search for a general law enforcement purpose.²¹³ In *United States v. Reynard*, however, another court agreed

209. The Court distinguished why this drug case did not qualify under the special needs test as had other drug cases as follows:

This case differs from the four previous cases in which we have considered whether comparable drug tests “fit within the closely guarded category of constitutionally permissible suspicionless searches.” In three of those cases, we sustained drug tests for railway employees involved in train accidents, for United States Customs Service employees seeking promotion to certain sensitive positions, and for high school students participating in interscholastic sports. In the fourth case, we struck down such testing for candidates for designated state offices as unreasonable.

Id. at 87 (internal citations omitted).

210. *See id.* at 84. This statement must surely come as a surprise to all courts that use the balancing test to determine government reasonableness in the absence of a warrant, but when probable cause is nonetheless present.

211. *See, e.g.*, *United States v. Miles*, 228 F. Supp. 2d 1130 (E.D. Cal. 2002); *United States v. Reynard*, 220 F. Supp. 2d 1142 (S.D. Cal. 2002); *Groceman v. United States*, No. 3:01-CV-1619-G, 2002 U.S. Dist. LEXIS 11491 (N.D. Tex. 2002); and *Pardue v. Johnson*, No. 2:00-CV-0424, 2002 U.S. Dist. LEXIS 14699 (N.D. Tex. 2002).

212. 228 F. Supp. 2d 1130 (E.D. Cal. 2002).

213. *See id.*

with *Miles* that the Supreme Court had effectively overruled *Rise*, but found that the government nevertheless met the special needs test by relying on *Marcotte*.²¹⁴ Specifically, *Reynard* found CODIS's purposes go beyond normal law enforcement by, *inter alia*, having probationary officers or prison personnel draw the blood samples instead of police, and that trying to exonerate the innocent was not a normal law enforcement function.²¹⁵

3. *The Supreme Court and Fingerprints*

Today, most in American society recognize that on arrest, law enforcement takes an arrestee's fingerprints and a "mug shot." Law enforcement then enters this information into various searchable databases using the NCIC.²¹⁶ It was not until 1969, however, that the Supreme Court held that taking an arrestee's fingerprints did not violate the Fourth Amendment's prohibition against unreasonable searches.²¹⁷ Specifically, *Davis v. Mississippi* held that a person does not enjoy a reasonable expectation of privacy in the oily residue left by a fingerprint.

A person does not reasonably enjoy this expectation of privacy, the Court explained, because "fingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search."²¹⁸ Thus, to the extent an individual goes about daily affairs and leaves traces of his or her fingerprints behind, law enforcement can seize those fingerprints. Fourth Amendment jurisprudence, however, is seldom so straightforward. *Davis* also held that even though there is no reasonable expectation of privacy in a fingerprint, the police must not violate the Constitution or the law when getting the print.²¹⁹ For example, if the police illegally detain a suspect in violation of the Fourth Amendment, then a

214. 220 F. Supp. 2d 1142 (S.D. Cal. 2002).

215. *See id.* The author's opinion is *Reynard* and *Marcotte* use strained logic under the special needs test so that the governmental interest outweighs the individual's privacy interest. For example, most agree that law enforcement's function is to convict the guilty and clear the innocent. To split this dual purpose by saying exonerating the innocent goes beyond normal law enforcement appears contrary to *Ferguson*, *Edmonds*, and common sense.

216. *See text at infra* Part II.C.

217. *See Davis v. Mississippi*, 394 U.S. 721 (1969).

218. *See id.* at 727.

219. *See id.*

defendant can successfully exclude from evidence fingerprints taken during the illegal detention.²²⁰

Davis went on in dicta to suggest that a detention done solely to obtain a person's fingerprints when there was less than probable cause to support the detention was not unlawful in every case (although there was a constitutionally deficient detention in *Davis*).²²¹ *Davis* explained that if law enforcement adopted "narrowly circumscribed procedures" to obtain fingerprints during a criminal investigation, it could detain individuals at convenient times for a short period to obtain fingerprints.²²² Some jurisdictions have in fact implemented such procedures upon a showing of reasonable suspicion.²²³

B. The Fourth Amendment Paradigm Applied to the DOD's DNA Database

The compulsory taking of a service member's blood by the government clearly implicates the Fourth Amendment.²²⁴ The government's purpose in taking the blood sample for the DNA database is to identify human remains when, because of severe trauma or degradation, more traditional identification methods cannot provide conclusive identification.²²⁵ Because the taking is wholly unrelated to any crime, the government's purpose must satisfy the special needs test before the taking of blood is reasonable under the Fourth Amendment.²²⁶

The government's purpose meets this high standard. The Supreme Court repeatedly has said the taking of blood is a minor intrusion of the person.²²⁷ Weighed against the legitimate government interest in accurately identifying the remains of those who die serving their country, the taking of blood is reasonable under the Fourth Amendment.²²⁸ That, however, cannot end our inquiry, because as the Supreme Court noted in *Skin-*

220. *See id.*

221. *See id.*

222. *See id.*

223. *See, e.g.,* ARIZ. REV. STAT. § 13-3905(A) (West 1999).

224. *See* *Schmerber v. California*, 384 U.S. 757 (1966).

225. *See supra* Part III.A.

226. *See* *Roe v. Marcotte*, 193 F.3d 72 (2d Cir. 1999).

227. *See* *Skinner, Sec'y of Transp. v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 625 (1989).

ner, the chemical analysis of a body fluid sample also implicates the Fourth Amendment.²²⁹

The DNA molecule makes up genes, chromosomes, and the human genome. The mapping of the human genome and the eventual cracking of the DNA code coupled with scientists' study of human proteome will reveal almost everything there is to know about an individual on a biological level.²³⁰ Thus, the Supreme Court's observation in *Skinner* that a urine sample can tell others if the donor is pregnant, epileptic, or diabetic, which consequently raises a reasonable expectation of privacy in that sample, is exponentially true regarding a DNA sample from blood.²³¹ Thus, the DOD's taking of the service member's blood is a classic example of a seizure,²³² but the subsequent DNA analysis of the blood sample requires a distinct Fourth Amendment analysis because of an individual's retained privacy interest in a bodily fluid sample that "reveal[s] a host of medical facts"²³³ This result is true to *Davis*'s reasoning, because DNA analysis probes into a person's private, albeit genetic, life.

If the DOD eventually does a DNA analysis of an AFRSSIR blood sample to identify remains, the special needs test would find that search reasonable under the Fourth Amendment, as explained above. The special needs test, however, would also necessarily find unreasonable a warrantless DNA analysis of an AFRSSIR blood sample done by law enforcement to help solve a crime. As *Ferguson* and *Marcotte* explain, the special needs test only justifies a search whose primary purpose is not law enforcement.²³⁴ Helping to solve a crime squarely meets the definition of a gen-

228. See *Mayfield v. Dalton*, 901 F. Supp. 300 (D. Haw. 1995), *vacated*, 109 F.3d 1423 (9th Cir. 1997) (to the authors' knowledge this is the sole case that has considered the issue. The Ninth Circuit, however, vacated the decision because the case was moot). See *supra* note 70.

229. See *Skinner*, 489 U.S. at 616.

230. See *supra* Part II.

231. See *Skinner*, 489 U.S. at 616.

232. See *supra* note 167, where the Supreme Court explained it did not need to distinguish between a search and seizure of a bodily fluid sample because the government was taking the sample to immediately search it. The DOD initially takes the sample, however, to store it, not search it. See *supra* Part III.A.

233. See *Skinner*, 489 U.S. at 617.

234. See *supra* Parts V.A.1 and V.A.2.b-d.

eral law enforcement purpose, and therefore, a governmental search based on that purpose done without a warrant violates the Fourth Amendment.²³⁵

A balancing test approach applied to a law enforcement search of an AFRSSIR blood sample would likewise violate the Fourth Amendment unless done pursuant to informed consent to search or a valid search warrant or authorization. The Fourth Amendment's balancing test requires probable cause, or at least individualized suspicion, coupled with circumstances that would defeat the purpose of securing a warrant.²³⁶ In almost every case, law enforcement could obtain a search warrant for a specific service member's AFRSSIR blood sample without time degrading the DNA sample already in law enforcement's possession. Moreover, if a court applied a Fourth Amendment balancing test outside the bounds of a roadblock or exigent circumstances, the individual's privacy interest in his or her DNA sample must trump law enforcement's "solve a crime" purpose pursuant to *Edmonds* and *Ferguson*.²³⁷

Finally, courts determine a reasonable expectation of privacy based on a totality of the circumstances.²³⁸ A court should therefore consider the involved steps the DOD has taken to assure service members they have a reasonable expectation of privacy in their stored blood samples at AFRSSIR: the DOD has promulgated a directive requiring, *inter alia*, a court order before law enforcement may seize an AFRSSIR sample;²³⁹ and the DOD opted out of the "blanket uses" of systems of records under the Privacy Act, including a law enforcement use.²⁴⁰ Under the Supreme Court's

235. This conclusion implicitly criticizes the reasoning, but not necessarily the result, of the cases cited in Parts V.A.2.a, b, and d because each of those courts stopped their analysis of an individual's privacy concerns with the minimal intrusiveness of taking a blood sample. *Skinner* teaches, however, that when the body fluid sample reveals medical information about an individual, the privacy analysis should not stop at how the government gained the sample. *See Skinner*, 489 U.S. at 617.

236. *See Schmerber v. California*, 384 U.S. 757 (1966).

237. *See supra* Part V.A.2.c.

238. *See Katz v. United States*, 389 U.S. 347 (1967).

239. *See supra* Part III.A. The DOD authorized the release of a former service member's DNA sample to Pennsylvania state and local investigators pursuant to a federal grand jury subpoena. Based on the author's conclusion that service members retain a reasonable expectation of privacy in their AFRSSIR DNA samples, the DOD should have moved to quash the subpoena. *See supra* note 133. By not challenging the subpoena, the DOD may have inadvertently undercut one factor on which service members could rely when forming a subjective expectation of privacy. For the other reasons cited in this article, however, service members still reasonably hold a subjective expectation of privacy in their AFRSSIR DNA samples.

240. *See supra* note 133 and accompanying text.

subjective prong, a service member could reasonably believe, based on the steps taken by the DOD, that he has an expectation of privacy in his AFRS-SIR blood sample.

A court may also properly infer from the DOD's actions that the executive branch's position is that society should recognize this privacy interest. Under the objective prong, some may argue, however, that because forensic DNA analysis involves junk DNA only, this makes the sample more like a fingerprint, and thus, society should not recognize a privacy interest.²⁴¹ *Skinner*, however, did not make this distinction when considering the privacy interests in a urine sample,²⁴² and the evolving knowledge of junk DNA may soon moot this argument.²⁴³ Supreme Court precedent therefore strongly suggests a servicemember has both a subjective and objective expectation of privacy in the AFRSSIR blood sample.

C. The Application of Military Rules of Evidence (MRE) 312(f) to the DOD's DNA Databank Military

Military Rule of Evidence 312(f) provides:

Nothing in this rule shall be deemed to interfere with the lawful authority of the armed forces to take whatever action may be necessary to preserve the health of a servicemember. Evidence or contraband obtained from an examination or intrusion conducted for a valid medical purpose may be seized and is not evidence obtained from an unlawful search or seizure²⁴⁴

A plain reading of this rule authorizes law enforcement access to an AFRSSIR DNA sample if the drawing of blood for the DNA sample was done for a "valid medical purpose." The Court of Appeals for the Armed Forces couples the phrase "valid medical purpose" with "necessary to preserve the health of the servicemember" to trigger a lawful search or seizure under MRE 312(f).²⁴⁵ Obviously, the AFRSSIR blood samples are not taken to preserve a service member's health since their purpose is to identify remains; therefore, they are not taken for a valid medical purpose. Thus, neither MRE 312(f) nor any other military rule of evidence provides

241. *See supra* note 59 and accompanying text.

242. *See supra* notes 228-32 and accompanying text.

243. *See supra* note 61 and accompanying text.

244. MCM, *supra* note 8, MIL. R. EVID. 312(f).

245. *See United States v. Stevenson*, 53 M.J. 257, 260 (2000).

law enforcement a basis to seize or search an AFRSSIR DNA sample without a warrant, search authorization, or consent.²⁴⁶

VI. Recently Enacted Federal Legislation

On 2 December 2002, President Bush signed Public Law 107-314 into law. Section 1063(a) of that law, now at 10 U.S.C.S. § 1565a, reads as follows:

DNA samples maintained for identification of human remains:
use for law enforcement purposes.

(a) Compliance with court order.

(1) Subject to paragraph (2), if a valid order of a Federal court (or military judge) so requires, an element of the Department of Defense that maintains a repository of DNA samples for the purpose of identification of human remains shall make available, for the purpose specified in subsection (b), such DNA samples on such terms and conditions as such court (or military judge) directs.

(2) A DNA sample with respect to an individual shall be provided under paragraph (1) in a manner that does not compromise the ability of the Department of Defense to maintain a sample with respect to that individual for the purpose of identification of human remains.

(b) Covered purpose. The purpose referred to in subsection (a) is the purpose of an investigation or prosecution of a felony, or any sexual offense, for which no other source of DNA information is reasonably available.

(c) Definition. In this section, the term "DNA sample" has the meaning given such term in section 1565(c) of this title.²⁴⁷

246. See MCM, *supra* note 8, MIL. R. EVID. 312(d).

247. 10 U.S.C.S. § 1565a (LEXIS 2004).

This statute fails to address any Fourth Amendment privacy issues raised by the AFRSSIR DNA samples. Before critiquing the statute, however, one should understand how this legislation came about.

This article's first hypothetical is based on a rape and murder case from Fort Hood, Texas. The case received national attention, including the victim's mother going public with her daughter's name and photograph a few weeks before the accused's court-martial.²⁴⁸ The Army's investigation did not satisfy the victim's mother, and she and her daughter eventually complained to their congressman, John Culberson of Houston, Texas.²⁴⁹ Congressman Culberson then proposed the above statute in the Bob Stump National Defense Authorization Act Year 2003.²⁵⁰ Neither the House of Representatives nor the Senate debated the above statute, and President Bush signed it into law unchanged from what Congressman Culberson initially submitted.²⁵¹

A careful reading of 10 U.S.C.S. § 1565a leaves one with many questions and few if any answers. The statute states that the DOD must honor a warrant or search authorization from a federal court or military judge²⁵² if for a felony or sexual offense, and the AFRSSIR can maintain the sample's integrity. This language is almost identical to that found in paragraph 3.5.1, *DOD Dir. 5154.24*, discussed at Part III.A. Thus, 10 U.S.C.S. § 1565a merely states what has always been the law: the AFRSSIR DNA samples are subject to search and seizure by law enforcement possessing a properly obtained warrant.²⁵³ Neither lawyers nor law enforcement need

248. See *A Child Who Is 'Not the Same,'* ARMY TIMES, Dec. 16, 2002, at 15-16. At the accused's court-martial for those crimes described in the first hypothetical and other crimes not mentioned, the military judge sentenced the accused to be imprisoned for the term of the accused's natural life without the possibility of parole.

249. See John M. Gonzalez, *Victim Assails Army For Not Matching DNA Sooner,* HOUS. CHRON., May 5, 2002, at A37.

250. H.R. 4546, 107 Cong. § 1566 (2002).

251. See Tranette Ledford, *Law Expands Access to Military DNA,* ARMY TIMES, Dec. 16, 2002, at 8.

252. The statute does not define "military judge." Giving the term its plain meaning, the DOD may not have to honor search authorizations done by commanders or military magistrates, who generally have the power to order a search or seizure of or on military property based on probable cause. See *supra* note 8.

253. A subpoena should be insufficient. See *supra* note 238.

a statute to tell them a judicial search and seize warrant trumps a reasonably held privacy interest.

The statute fails to address the key issue that brought the rape victim and her mother to Congressman Culberson's office. Can law enforcement get to the AFRSSIR DNA samples without a warrant? One can make arguments on either side of what the statute intended, but the statute, on its face, explicitly fails to say a warrant or court order is the sole way law enforcement may gain access to the AFRSSIR DNA samples.²⁵⁴ The statute is also silent on its interaction with the Privacy Act and FOIA. If the statute meant to act on the rape victim and her mother's complaint that the Army should have matched the DNA to the suspect or accused via the AFRSSIR DNA samples, it fails to take any steps in that direction.²⁵⁵ If the statute meant to answer what privacy interests a service member has in his AFRSSIR DNA sample, it also fails to do that. The statute is therefore a "push,"[not a generally recognized term] and we are left analyzing the Privacy Act, FOIA, and the Fourth Amendment to answer the privacy question.

VII. Hypotheticals Revisited

In *Hypothetical 1*, the victim requests the DOD to search its DNA databanks for the forty thousand soldiers stationed at the Army post against the DNA sample taken from the victim's body. In this hypothetical, there is no probable cause or individualized suspicion to justify a search warrant or authorization. Moreover, as explained in Part V.B, service members maintain a reasonable expectation of privacy in their DNA

254. The legislative and executive branch would clearly invade the power of the court if they passed a law that said an individual did not enjoy a reasonable expectation of privacy in a given area or thing. The converse, however, is not necessarily true. The legislature and executive branch could enact a law that said, for example, individuals possess a reasonable expectation of privacy in their garbage no matter the location of such garbage. There is no reason why such a statute would not pass constitutional muster in that legislatures and the executives are free to empower the people with more rights than the constitution provides.

255. A first step would appropriate funds to analyze, "fingerprint," and place in a searchable computer database the over four million DNA samples currently stored by the AFRSSIR. The next step might be to authorize by statute and implementing regulations the placing of a copy of such a database in CODIS or the NCIC, with accompanying Privacy Act legislation and implementing regulations.

samples stored at the AFRSSIR. The state agency's Privacy Act/FOIA request, however, slightly complicates the analysis.

As a practical matter, honoring the request would overwhelm AFDIL, because they could not timely produce a DNA fingerprint from forty thousand blood samples and continue their other work. Second, neither the Privacy Act nor FOIA require an agency to create records in response to a request, and producing the DNA fingerprint from existing blood samples arguably makes a new record.²⁵⁶ Third, as discussed in Parts IV.A and B, if a service member maintains a reasonable expectation of privacy in a government record, then neither the Privacy Act nor FOIA authorizes that record's release.²⁵⁷

Hypotheticals 2 and 3 are questions of degree based on *Hypothetical 1*. *Hypothetical 2* limits the pool of possible suspects to three hundred soldiers, but law enforcement still has no individualized suspicion against any soldier. While three hundred DNA samples for AFDIL analysis and DNA fingerprinting may be manageable, that is not the crux of a Fourth Amendment analysis. Thus, for *Hypothetical 2*, the analysis is the same as *Hypothetical 1*.

Hypothetical 3 is problematic under the Fourth Amendment because it gives the power of foresight. We know there are ten suspects, and one of them will kill in the future if not stopped now. Implicit in constitutional criminal law is a trade off: for the good of the system some guilty go free. Thus, when police illegally seize evidence or illegally obtain a confession, courts generally do not allow the admission of that evidence at trial to deter future police misconduct.²⁵⁸ Generally, therefore, *Hypothetical 3's* answer is the same as *Hypotheticals 1 and 2*. *Hypothetical 1's* answer is not, however, a blanket solution.

Law enforcement has ten suspects in *Hypothetical 3*, and it is reasonable to assume that in a few days their investigation will establish alibis for most of the ten suspects. Police would then have individualized suspicion against one or two soldiers, and most likely in the near future could obtain a search warrant for the relevant AFRSSIR blood sample. What if, however, some exigent circumstance presented itself at this point (for example, one of the two primary suspects was about to leave the United States to a

256. See *supra* note 141.

257. See *supra* note 140 and accompanying text.

258. See *Mapp v. Ohio*, 367 U.S. 643 (1961).

country with whom the United States did not have an extradition treaty).²⁵⁹ Not every law enforcement search of an AFRSSIR blood sample is unreasonable without a warrant, for as Justice Jackson said in dissent:

But if we are to make judicial exceptions to the Fourth Amendment for these reasons, it seems to me they should depend somewhat upon the gravity of the offense. If we assume, for example, that a child is kidnaped [sic] and the officers throw a roadblock about the neighborhood and search every outgoing car, it would be a drastic and indiscriminating use of the search. The officers might be unable to show probable cause for searching any particular car. However, I should candidly strive hard to sustain such an action, executed fairly and in good faith, because it might be reasonable to subject travelers to that indignity if it was the only way to save a threatened life and detect a vicious crime. But I should not strain to sustain such a roadblock and universal search to salvage a few bottles of bourbon and catch a bootlegger.²⁶⁰

Thus, in almost every case, law enforcement should obtain a warrant to perform a DNA analysis of a service member's AFRSSIR blood sample. Exigent circumstances coupled with individualized suspicion, however, could make a warrantless law enforcement search reasonable under the Fourth Amendment. That being said, *Hypothetical 3* does not present facts that trigger this exception to the general rule.

VIII. Conclusion

Our knowledge of the DNA molecule evolves and expands. Today, and even more so in the foreseeable future, the DNA molecule will reveal many medical and biological facts about the individual from whom the molecule came. Supreme Court precedent shows that individuals have a reasonable expectation of privacy in their bodily fluids when the chemical analysis of those fluids may reveal personal facts about the individual, even when the specific chemical analysis done does not reveal those facts. Moreover, steps taken by the DOD lead service members to believe they have a privacy interest in their DNA blood samples. Thus, service mem-

259. Assume for the sake of argument that the soldier could freely leave. Obviously, a commander would likely order the soldier not to leave post.

260. *Brinegar v. United States*, 338 U.S. 160, 183 (1949).

bers retain a reasonable expectation of privacy in their blood samples given to the AFRSSIR for possible future DNA analysis to identify their remains.

This conclusion is important, for it precludes release of the AFRSSIR samples under the Privacy Act and FOIA, provides a basis to quash a subpoena seeking a AFRSSIR blood sample, triggers a Fourth Amendment analysis when law enforcement wants to obtain a DNA fingerprint from an AFRSSIR blood sample, and precludes a *Davis* reasonable suspicion standard to get at the AFRSSIR blood samples. In almost every case, the Fourth Amendment requires law enforcement to obtain a warrant or search authorization before they may perform a DNA analysis on an AFRSSIR blood sample. Unfortunately, existing federal legislation to protect a service member's privacy interest in his or her AFRSSIR blood sample is inadequate. To protect this interest, Congress and the President should enact legislation making the misuse of the AFRSSIR blood samples criminal, as they have done with DNA samples in CODIS and NCIC identification information. Finally, Congress and the DOD, respectively, should amend 10 U.S.C.S. § 1565a and *DOD Dir. 5154.24* to clearly state that only a search authorization by a military judge or search warrant by a federal judge or magistrate satisfies the requirement of a court order.