BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT



**Biometrics**

**Defense Department**

Biometric data on suspected terrorist detainees can and should be routinely shared within the Defense Department and with federal and state agencies having a need for terrorism related information, writes Jeffrey L. Caddell. In this article, Caddell discusses the legal authority for DoD to collect and share biometrics information, the security protocols for biometrics data files, relevant privacy interests, and more.

# DoD Biometrics in the Age of Terrorism

By Jeffrey L. Caddell

## Introduction

In this age of terrorism, America is at a high risk of attack, and it will continue at such high risk unless it can decisively establish the identity of individuals and effectively link that identity to specific information for military operations. Recognizing this risk, the Department of Defense (DoD) is developing biometric capabilities[1] and is employing procedures to effectively share counter-terrorism information derived from those capabilities within DoD and with other federal agencies in order to determine the true identities of our adversaries and to verify the identities of our friends and allies.

DoD's goal is to make all Americans safer in this age of terrorism. The central issue is whether DoD's use of biometrics to identify a person, or verify their identity, is antithetical to that person's privacy interests in a post 9/11 world. DoD's goal is accomplished by balancing privacy interests using an effective, comprehensive, coordinated means of sharing terrorism information in a

*Jeffrey L. Caddell is Associate Deputy General Counsel (Acquisition, Information, & Technology) in the Department of the Army Office of the General Counsel. The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government.*

[1] Biometric capability means the ability to capture, compare and analyze measurable physical characteristics or personal behavior traits that can be used to recognize or identify a person.

 ISSN 1538-3423

way that safeguards an individual's legal rights and privacy expectations in accordance with applicable law.

This article will provide a general overview of biometrics, and briefly outline how unclassified biometric capabilities are being employed by the DoD in the Global War on Terrorism, while protecting the privacy interests associated with biometric data related to terrorism information.

## Biometrics Generally

The term ''biometrics'' is derived from the Greek words ''bio'' (life) and ''metrics'' (to measure).[2] In essence, the science of biometrics implemented by DoD is the capability to read the measurable biological characterization of an individual in order to identify or recognize that person through some computerized electronic analytical system. In order for an individual to be recognized or identified by a biometrics system, that person's biometric data must first be ''enrolled'' into the biometrics system. Enrollment is the end of the process that begins with collecting a biometric sample, conversion into a biometric reference, and storage in the biometric system's database for later analysis and comparison and association with an individual.[3] The two primary uses for Biometrics are: (1) to ''verify that people are who they say they are'' (verification), and (2) to ''identify unknown people'' (identification).[4] *Verification* is a ''one-to-one matching process where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates'' stored in the database.[5] *Identification*, on the other hand, ''is a one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the known identity of the individual whose template was matched.''[6]

## DoD Implementation of Biometrics

Most biometric systems operate by ''translating information relating specifically to a human feature or characteristic into a mathematical construction'' or a template.[7] DoD uses the science of Biometrics to create a unique identifier or template that can be electronically stored, retrieved, and compared with other information collected on an individual. The unique biometric identifier or template is associated with other information to assist operational decisions and to facilitate individual biometric file sharing. This ''associated information'' is the contextual information of the person's biographical data and the circumstances under which biometrics were gathered. For example, the fingerprints and facial photo biometrics gathered from a possible terrorist outside a village in Iraq are ''associated'' with the facts and circumstances of the encounter. This associated information can reveal the possible intent of the individual when U.S. forces encounter the same person months later in another part of Iraq. Usually, DoD will collect fingerprints, photographs and sometimes iris scans and DNA swabs. The information is stored and converted to a template for use in analysis suitable for either identification or verification comparisons.

The general scenario in which DoD might employ biometric capabilities in its efforts to defend U.S. interests include collecting biometrics from an unexploded Improvised Explosive Device (IED), or the collection from suspected insurgents or other persons of interest encountered during a military operation, for comparison against biometric data already in DoD's biometric database.

## Biometric Technologies – Modalities

There are many different types of biometric technologies, each of which focus on different physical-biological characteristics. Within the biometric community, these different characteristics are generally referred to as ''modalities''.[8] Generally, no single biometric modality is best suited for all biometric implementations.[9] Different modalities are selected and used based on such factors as the maturity and reliability of the technology, the costs of the sensors used to collect the biometrics, and the ease of collection under various environmental conditions. Fingerprint collection, for example, is one such type of biometric modality that is based on mature and reliable technology, is low in cost, and is easy to collect under most conditions. The following summations describe some of the more common biometric modalities:

*Fingerprint Recognition*. Fingerprinting has been in use as a biometric recognition technique since the late 19th century, and is based on comparing the graphical, flow-like ridges of the fingers.[10] This is perhaps the most well known of the biometrics modalities.[11]

*Iris/Retinal Recognition*. Eye recognition biometrics involves technologies that include either scanning the iris or scanning of the retinal area at the back of the eye. Images of the iris, or the pattern of veins at the rear of the eye in the case of retinal scans, are converted into a biometric template and stored for later comparison.[12]

*Face Recognition*. Facial imaging technology describes a group of different approaches designed to reduce facial qualities to mathematical abstractions that can be captured and evaluated electronically. The image of a face is captured using a scanner and then ana-

[2] National Science and Technology Council, Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, [hereinafter: NSTC], Biometrics History, at 56. (Document available at http://www.biometrics.gov/Documents/biofoundationdocs.pdf).

[3] NSTC, Privacy & Biometrics: Building a Conceptual Foundation, p. 6, (September 15, 2006), [hereinafter Foundation], available at http://www.biometrics.gov/docs/privacy.pdf.

[4] Robin Feldman, Considerations On The Emerging Implementation Of Biometric Technology, 25 Hastings Comm. & Ent. L.J. 653, 655 (2003).

[5] Foundation, supra note 3, at 8.

[6] Definition, http://www.biometrics.dod.mil/Bio101/5.aspx

[7] Feldman, at 656. In and of itself, the template has no ''physiological meaning;'' rather, the information developed by the computer is only indirectly related to physiological features.

[8] NSTC, Foundation, supra note 3, at 12.

[9] Id.

[10] Id. at 13; Feldman, supra note 4, at 657.

[11] NSTC, Fingerprint Recognition, at 100; See also: NSTC, Biometrics Overview, at 80. (Documents available at: http://www.biometrics.gov/Documents/biofoundationdocs.pdf).

[12] NSTC, Iris Recognition, at 114; NSTC, Biometrics Overview, at 81. (Documents available at: http://www.biometrics.gov/Documents/biofoundationdocs.pdf).

  PVLR ISSN 1538-3423

lyzed in order to obtain a biometric ''signature'' through the use of different algorithms.[13]

*Voice recognition*. Also known as ''speaker recognition,'' this biometric modality uses an individual's voice for verification and/or identification.[14]

*Dynamic Signature*. Dynamic signature measures the speed and pressure an individual uses when signing his or her name—not what the signature itself looks like.[15]

*Vascular Pattern Recognition*. This modality is based on research suggesting that the pattern of blood vessels within a human body is individual-specific and does not change over time. Similar in concept to a retinal scan, a person's vein pattern, as seen with near-infrared light, is converted into a template for analysis by means of a pattern-matching technique.[16]

*DNA Matching*. DNA (deoxyribonucleic acid) biometric modality is based on the well-known double helix structure.[17] A DNA sample is used to produce either a DNA fingerprint or a DNA profile. The premise is that DNA is unique for each individual and does not change throughout a person's life.[18] One significant problem with using DNA biometrics is that while comparison tests are difficult to circumvent, extreme care must be taken to avoid contamination of the sample collected.[19] Additionally, privacy issues with DNA analysis arise from the fact that DNA may reveal sensitive information related to genetic and medical aspects of individuals and disclose information about hereditary factors and medical disorders.[20]

There are other biometric modalities and methods, each having different levels of accuracy. These include: Odor Recognition;[21] Gait Recognition;[22] and Facial Thermography.[23] DoD has the capability to employ photography, fingerprinting, iris scanning, and DNA sampling modalities.

There has been recent discussion about the benefits of using multiple modalities, based on the idea that several modalities can be used together in order to improve the efficiency of the biometric system and enhance flexibility by using different modalities in parallel.[24] More flexibility is possible in a biometric system built for multiple modalities, (e.g., fingerprint and face recognition). In situations where a user for example, seeking access to a system protected by a biometric log-in process, has difficulty registering or enrolling a fingerprint, due to excessive wear or injury, the user could use a face scan in verification mode instead.[25]

## Legal Authority to Collect Biometrics

The legal authority for DoD to collect and use biometrics is derived from the Constitutional authority of the President, as Commander in Chief of the Armed Forces, in the exercise of his war powers (that reasonably includes directing the military to collect and use biometrics);[26] and from Title 10 of the United States Code, section 3062(a), regarding the general purpose of the Armed Forces,[27] (which largely depends on DoD's responsibility for effectively prosecuting war, and protecting enduring national interests);[28] and in the plenary powers of the Secretary of Defense, 10 U.S.C. § 113; Secretary of the Army, 10 U.S.C. § 3013; Secretary of the Navy, 10 U.S.C. § 5013; and Secretary of the Air Force; and 10 U.S.C. § 8013.[29] More recently, Congress provided additional legal authority when it designated the Secretary of the Army as the Executive Agent for DoD Biometrics programs.[30] DoD Directive 8521.01E establishes policy and assigns responsibilities and describes general procedures for DoD Biometrics efforts. Together, these sources provide the domestic legal authority for DoD to obtain the biometrics of suspected terrorists detained as a result of a military operation.

While DoD's collection and use of biometrics is authorized under U.S. law, it is also consistent with international law. Under international law, the treatment of lawful and unlawful combatants is governed by the Geneva Conventions, particularly the Convention on the Treatment of Prisoners of War.[31] As a general matter, ''terrorists'' are not lawful combatants protected under the Law of War because terrorists generally do not meet the legal classification as lawful combatants under the Geneva Convention.[32] Consequently, unlawful combatants may be captured, detained, and tried by military

---

[13] Biometrics at the Frontiers: Assessing the impact on Society, European Commission, Joint Research Centre (DG JRC), Institute for Prospective Technological Studies, [hereinafter Frontiers], http://www.statewatch.org/news/2005/mar/Report-IPTS-Biometrics-for-LIBE.pdf, p. 54, 2005.

[14] NSTC, Speaker Recognition, at 128; See also: NSTC, Biometrics Overview, at 82. (Documents available at http://www.biometrics.gov/Documents/biofoundationdocs.pdf).

[15] NSTC, Dynamic Signature, at 87, available at: http://www.biometrics.gov/Documents/biofoundationdocs.pdf).

[16] See NSTC, Vascular Pattern Recognition, at 134, available at: http://www.biometrics.gov/Documents/biofoundationdocs.pdf).

[17] Frontiers, supra note 13 at 62.

[18] Id. at 63.

[19] Id.

[20] Id.

[21] The use of an individual's odor to determine identity.

[22] The use of an individual's walking style or gait to determine identity.

[23] The measure of how heat dissipates off the face of an individual.

[24] Frontiers, supra note 13, at 98. See John D. Woodward, Jr., Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism, Military Review, p. 30, September-October 2005.

[25] Id., Frontiers, at 98.

[26] U.S. Const. art II, § 2.

[27] 10 U.S.C. § 3062(a). ''It is the intent of Congress to provide an Army that is capable, in conjunction with the other armed forces, of preserving the peace and security, and providing for the defense, of the United States, the Territories, Commonwealths, and possessions, and any areas occupied by the United States; supporting the national policies; implementing the national objectives; and overcoming any nations responsible for aggressive acts that imperil the peace and security of the United States.''

[28] Army Field Manual 1, paragraphs 2-25-26.

[29] For example, the Secretary of Defense has statutory authority to perform any of his functions or duties, or exercise any of his powers as he may designate – unless specifically prohibited by law. See 10 U.S.C. § 113.

[30] Emergency Supplemental Appropriations Act, 2000, Pub. L. No. 106-246, § 112, 114 Stat. 511, 531-532.

[31] Geneva Convention Relative to the Treatment of Prisoners of War, opened for signature August 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135, (ratified 1955) [hereinafter GPW].

[32] Lawful Combatants are: members of a nations armed forces; persons who accompany armed forces but are not members thereof; members of a merchant marine or civilian air crew; or individuals who, on the approach of the enemy, take up arms to resist invading forces. GPW.

tribunals for acts that render their belligerency unlawful.[33]

Nonetheless, unlawful combatants are still entitled to humane treatment under General Article 3 of the Geneva Convention.[34] This is often referred to as Common Article 3, and is so named because it is contained in all four Geneva Conventions of 1949. The 2006 U.S. Supreme Court decision in *Hamdan v. Rumsfeld*,[35] applied Common Article 3 to a global conflict with a non-state actor, al-Qaeda, taking place within the territory of a country that is a party to the Geneva Conventions, Afghanistan. The ruling in *Hamdan* implies that Common Article 3 applies to the Global War on Terrorism anywhere in the world that is within the territory of a party to the Geneva Conventions.[36]

The relevant elements of Common Article 3 are the requirement for humane treatment; the proscriptions against mutilation, torture, and cruel treatment; and the proscriptions against outrages upon personal dignity, including humiliating and degrading treatment. The Geneva Conventions do not mention ''biometrics;'' and so collecting and using biometrics are not addressed as a specific matter. The area where Common Article 3 might apply in the context of biometrics is in the prohibition of humiliating or degrading treatment. The reason for focusing discussion on humiliating and degrading treatment is that merely collecting biometrics in a manner that inflicts no harm or injury would not constitute mutilation, torture, or cruel treatment, as those terms are commonly defined.

Given the omission of ''biometrics'' in the conventions, it is appropriate to review existing U.S. military and domestic criminal law and regulation to determine if the taking of biometrics in a detainee-custodial setting might constitute cruel or degrading treatment in contravention of Common Article 3. Collecting the biometrics of a person's face via photographs is a long standing practice acceptable under U.S. criminal law, (and most other nations), premised on the reasoning that the law does not prohibit the observation of acts or property in public view—such as a detainee's face.[37] Further, U.S. law generally permits the taking of photographs and fingerprints from arrestees/detainees as a normal identification process consistent with constitutional protections.[38] In a similar vein, the 5th Amendment privilege against self-incrimination offers no safe haven against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, or even to make a particular gesture.[39] Moreover, Army Regulation 190-8, implementing the obligations and proscriptions of the Geneva Conventions, specifically authorizes the fingerprinting and photographing of Enemy Prisoners of War (EPWs), retained personnel, and other detainees.[40]

Using principles of U.S. criminal law by analogy, and Army regulation specifically implementing international law, it is apparent that taking biometric measurements via photographs, fingerprints, and other non-intrusive measurement of physical characteristics are lawful and appropriate treatment for terrorists or suspected terrorists held in U.S. custody, and therefore does not constitute cruel or inhumane treatment. The remaining concern is whether the practice of obtaining DNA from detainees constitutes cruel or inhumane treatment, or an outrage against personal dignity.

The DoD currently obtains DNA samples by taking buccal swabs from a detainee's mouth for storage and subsequent analysis.[41] Buccal swabs are used in military operations instead of blood samples because they are far easier to obtain and store in military operational environments and avoid the risk of disease associated with exposure to blood. The question here is whether the practice of taking DNA via buccal swabs amounts to cruel or inhumane treatment, or an outrage against personal dignity sufficient to violate Common Article 3.

There is a distinction between invasive and non-invasive procedures under U.S. criminal law. Invasive procedures that ''shock the conscience'' are typically prohibited, and could therefore be seen as cruel or inhumane treatment, or an outrage against personal dignity under Common Article 3.[42] U.S. law has long recognized that taking blood samples to collect evidence is lawful. A recent court decision reached the same con-

[33] See, Ex parte Quirin, 317 U.S. 1, 31 (1942); Hamdi v. Rumsfeld, 542 U.S. 507 (2004).

[34] GPW, Article 3: ''In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each party to the conflict shall be bound to apply, as a minimum, the following provisions: 1. Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria. To this end the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons: (a) Violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture; (b) Taking of hostages; (c) Outrages upon personal dignity, in particular, humiliating and degrading treatment; (d) The passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized peoples. The wounded and sick shall be collected and cared for. 2. An impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict. The Parties to the conflict should further endeavor to bring into force, by means of special agreements, all or part of the other provisions of the present Convention. The application of the preceding provisions shall not affect the legal status of the Parties to the conflict.''

[35] 548 U.S. 557 (2006).

[36] See, John Bellinger, The Meaning of Common Article Three, http://www.opiniojuris.org/posts/1168814555.shtml.

[37] Katz v. U.S., 389 U.S. 347 (1967), holding that police may photograph public events during routine investigations.

[38] See e.g., Davis v. Mississippi, 394 U.S. 721,727 (1969); Schmerber v. California, 384 U.S. 757, 764 (1966); United States v. Dionisio, 410 U.S. 1 (1973); Smith v. U.S., 324 F.2d. 879 (D.C. Cir. 1963).

[39] Schmerber v. California, 384 U.S. 757 (1966).

[40] AR 190-8, ENEMY PRISONERS OF WAR, RETAINED PERSONNEL, CIVILIAN INTERNEES AND OTHER DETAINEES, October 1, 1997. This regulation implements international law, both customary and codified, relating to EPW, RP, CI, and ODs, which includes those persons held during military operations other than war.

[41] A buccal smear (pronounced ''buckle'') is the painless removal of a sample of cells from the lining of the mouth (inside of the cheek) for study. (U.S. National Library of Medicine and the National Institutes of Health): http://www.nlm.nih.gov/medlineplus/print/ency/article/003414.htm.

[42] Rochin v. California, 324 U.S. 165 (1957), (forcing a drug suspect to have his stomach pumped out, in order to recover evidence, violated the 4th Amendment).

  PVLR ISSN 1538-3423

clusion for the collection of DNA samples. In 2006, the U.S. Court of Appeals for the Seventh Circuit specifically held that taking blood samples for DNA collection from a person on probation was not a violation of the Eighth Amendment prohibition against cruel and unusual punishment.[43] The court reasoned that the government's need to collect identifying information, along with the minimal pain and discomfort accompanying a blood draw serves to take the DNA Identification Act collection requirements outside the ambit of cruel and unusual punishment. Arguably, taking DNA samples via buccal swabs is a less intrusive means of collecting a sample than the physical act of taking blood samples.[44]

DoD collects biometric information pursuant to law in order to protect the United States against international terrorism and other threats. For the use of biometrics to be an effective tool against terrorism, the data must be accessible by many different federal agencies to perform homeland security, diplomatic, defense, foreign intelligence, and law enforcement functions.

## Legal Authority to Share Biometrics

Legal authority for the sharing of biometric data related to terrorism information was recently established in two statutes; the Homeland Security Act of 2002,[45] which directed federal agencies to promptly provide terrorism information to the Secretary of Homeland Security; and by Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, (IRTPA),[46] which directed the creation of an ''Information Sharing Environment'' to provide for federal, state, local, and tribal access as appropriate to terrorism information.''[47] Prior to these statutes, the Patriot Act had required the federal government to devise a method to verify the identity of anyone entering the United States to confirm their identities and facilitate background checks.[48]

Additional sharing authority can be found in the Homeland Security Presidential Directive-6 (HSPD-6) released Sept. 16, 2003, which focused on the integration and use of screening information to protect the nation against terrorism.[49] In Aug. 27, 2004, the President signed Homeland Security Presidential Directive 11 (HSPD-11) regarding Comprehensive Terrorist-Related Screening Procedures. The HSPD-11 focused squarely on terrorism information and the need to implement a coordinated and comprehensive approach to terrorist-related screening.[50] The combined effect of these documents was to direct federal agencies to implement comprehensive and coordinated procedures for collecting and integrating information on terrorists and to use that information to the full extent permitted by law.

## Protecting Biometric Data Files

The current security protocols governing the central repository for DoD's Biometric detainee database calls for the files to be marked ''For Official Use Only'' (FOUO), and requires that they be stored on a secure server, in a secured remote area, under strictly controlled access. This FOUO designation is used by DoD and a number of other federal agencies to identify information or material, which, although unclassified, may not be appropriate for public release.[51] The term FOUO is defined as ''unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA).''[52] FOUO information may be disseminated within the DoD components and between officials of the DoD components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO information may also be released to officials in other departments and agencies of the executive and judicial branches in performance of a valid government function. The restrictive markings, the secured data storage requirements, and the controlled sharing of terrorism information provide considerable protection of all biometric data files.

## Privacy

The central issue is whether DoD's use of biometrics to identify a person, or verify their identity, is antithetical to that person's privacy interests in a post 9/11 world.

The concept of privacy arises under various bodies of law, and is generally not seen as an absolute right. It is ultimately a balance between the privacy interests of the individual, and the privacy interests accepted by the society in which the individual resides. Privacy interests are liberties resulting from the social deference to those liberties. ''The liberty does not reside in the conduct; it resides in the social deference extended to it.''[53] Three of the four areas of privacy interests discussed here represent the different facets of social deference extended to privacy interests within the United States.

## Common Law Privacy Interests

The common law concept of privacy law developed during the 1890s when Samuel Warner and Louis Brandeis, reacting to the recent advent of photography and gossip newspapers, argued for the recognition of a new

[43] United States v. Hook, 471 F.3d 766 (7th Cir. 2006).

[44] This is not to suggest that taking blood samples would be illegal under the Common Article, only that buccal swabs are less intrusive than taking blood samples.

[45] 6 U.S.C. § 122, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[46] 6 U.S.C. § 485, Pub. L. No. 108-458, 118 Stat. 3638, 3825-3832 (2004).

[47] Section 1016 supplements section 892 of the Homeland Security Act of 2002 (Public Law 107-296), and Executive Orders 13311 of July 29, 2003, and 13388 of Oct. 25, 2005, and other Presidential guidance, which address various aspects of information access.

[48] 8 U.S.C. § 1105(c), as amended by USA Patriot Act § 403 (2001).

[49] http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html

[50] http://www.whitehouse.gov/news/releases/2004/08/20040827-7.html.

[51] See DoD Regulations 5400.7-R and 5200.1-R. Note: FOUO marking designation may eventually change to ''Controlled Unclassified Information'' (CUI), under a plan to start using common document markings across the federal government.

[52] 5 U.S.C. § 552 (2002). The U.S. Freedom of Information Act (FOIA) is a law ensuring public access to U.S. government records. See: http://www.usdoj.gov/oip/foiastat.htm. The fact that information is marked FOUO does not mean it is automatically exempt from public release under FOIA. If a request for the information is received, it must be reviewed to see if it meets the FOIA dual test: (1) It fits into one of the nine FOIA exemption categories, and (2) There is a legitimate government purpose served by withholding the information.

[53] Professor Robert Parks, Lectures, Privacy Law Seminar, George Washington University School of Law. Fall Semester 1995.

concept of a Privacy Tort.[54] Some seventy years later, William Prosser summarized the evolving Law of Privacy and defined four distinct areas of privacy:[55] (1) Intrusion into one's seclusion or private affairs; (2) Publication of embarrassing private facts of the individual; (3) Publication of information that places one in a false light but does not arise to defamation; and, (4) Appropriation of one's name or image for another's commercial gain. Prosser's organizational scheme (later adopted by the American Law Institute, Restatement of Torts), established that the Law of Privacy relates, in a collective sense, to the ''interference with the interest of the individual in leading, to some reasonable extent, a secluded and private life, free from the prying eyes, ears, and publications of others.''[56]

## Constitutionally Derived Privacy Interests

The privacy interests derived from various provisions of the U.S. Constitution are distinct from common-law privacy interests. Although the term ''privacy'' doesn't expressly appear in the U.S. Constitution, that document is commonly interpreted to contain a few protections and privileges that address privacy interests of individuals.[57] These protections are often based on the concept of a ''reasonable expectation of privacy'' on the part of the individual affected.[58] The Fourth Amendment, for example, provides for a privacy interest, or ''right'' of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.[59] Over the years, American jurisprudence has carved out many distinct areas of invaluable privacy interests, as recognized by the Supreme Court: certain intimate information protected from disclosure;[60] certain personal decisions shielded from government intrusions;[61] certain forms of communication protected;[62] Physical body protected;[63] certain personal spaces protected;[64] and generally, the right to be left alone.[65] For some, the right to privacy is seen as having three components: (1) a right to be left alone; (2) a right to autonomous choice regarding intimate matters; and (3) a right to autonomous choice regarding other personal matters.[66] To those three, some might add a privacy interest in Informational Privacy, defined as the ''ability to maintain control over the use and dissemination of one's personal information.''[67] Terrorists understandably seek to obscure their real identity and deny DoD any access or control over their informational privacy.

## Statutory Privacy Interests

While common law privacy interests and those derived from various Constitutional provisions might apply broadly, the statutorily codified privacy interests embodied in the Privacy Act of 1974 provide specific requirements for U.S. federal agencies and are applicable only to the privacy interests of U.S. citizens and persons admitted into the U.S. for lawful permanent residence, (hereafter referred to as ''U.S. Persons'').[68] This statutory component of privacy law impacts DoD's use of biometrics as far as U.S. citizens or lawful U.S. residents are concerned. The Privacy Act governs how federal agencies collect, maintain, use, and share or disseminate ''records'' of personal information. The Privacy Act defines a ''record'' to include the person's name, or the identifying number, symbol, or other identifying particular, assigned to the individual such as a finger or voice print or a photograph.[69] Consequently, a Privacy Act protected record in this case includes any biometrics data information about a U.S. person, within a system of records, to include a fingerprint, voice print, photograph, iris scan, etc., which is associated or linked to the individual U.S. person. It does not directly apply to non-U.S. persons, whose numbers comprise the bulk of persons from whom DoD collects biometric data records in the Global War On Terrorism. It is important to note the distinction between collecting biometrics from suspected terrorists for the purposes of combating terrorism, and collecting biometrics from DoD employees for the purposes of controlling access to DoD buildings or the DoD information network. Biometric data files collected from DoD employees for access purposes are stored separate and apart from those collected from persons detained as a result of military operations.

The Privacy Act provides for a balancing of interests; e.g., a federal agency's need for collection, use, and dissemination of information about individuals, balanced against the privacy interests of those individuals. The Act provides covered individuals, (U.S. Persons), with rights of access, amendment or correction, and accounting. More precisely, the Privacy Act permits only

[54] See Samuel Warner & Louis Brandeis, In the Right of Privacy, 4 Harv. L. Rev. 193 (1890).

[55] See Prosser, Privacy, 48 Cal. L. Rev. 383 (1960).

[56] See Restatement of Torts, § 652A (1976).

[57] Bert-Jaap Koops and Ronald Leenes, 'Code' and the Slow Erosion of Privacy, 12 Mich. Telecomm. Tech. L. Rev. 115, 125 (2005), available at http://www.mttlr.org/voltwelve/koops&leenes.pdf

[58] Id. at 128.

[59] U.S. Const. amend. IV.

[60] Whalen v. Roe, 429 U.S. 589 (1974), (access to database of prescription drug information).

[61] Carey v. Population Services Int'l, 431 U.S. 678 (1977), (distributing contraceptives to minors); Whalen v. Roe, 429 U.S. 589 (1979); Roe v. Wade, 410 U.S. 113 (1973), (abortion); Loving v. Virginia, 388 U.S. 1 (1967), (ban on interracial marriage).

[62] Katz v. United States, 389 U.S. 347 (1967), (listening device in a public phone booth)

[63] Rochin v. California, 342 U.S. 165, 173-174 (1952) (pumping a suspect's stomach); Cf. Schmerber v. California, 384 U.S. 757, 766-772 (1966) (compulsory blood test).

[64] United States v. Karo, 468 U.S. 705 (1984), (school official searching students purse); Payton v. New York, 445 U.S. 573 (1980), (warrantless entry into the home); see also Bowers v. Hardwick, 106 S. Ct. 2841, 2850-51 (1986) (Blackmun, J., dissenting) (privacy right did not extend to homosexual conduct in the home).

[65] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), (warrantless wiretap of home phone lines, majority opinion later reversed by Katz).

[66] See Laurence H. Tribe, American Constitutional Law, § 15- 1 (2d ed. 1988); Ken Gormley, One Hundred Years of Privacy, 1992 Wis. L. Rev. 1335, 1340.

[67] Dr. Ann Cavoukian, Privacy & Biometrics, Abstract, at 2, (undated), available at http://www.pcpd.org.hk/english/infocentre/files/cakoukian-paper.doc. See also, Bert-Jaap Koops and Ronald Leenes, 'Code' and the Slow Erosion of Privacy, supra note 57, at 127

[68] The Privacy Act, 5 U.S.C. § 552a (2000). See, http://www.usdoj.gov/oip/1974polobj.htm.

[69] Id.

  PVLR ISSN 1538-3423

a U.S. person to seek access to his or her own ''record,'' and only if that record is maintained by the agency within a ''system of records''—that is a record actually retrieved by that individual requester's name or personal identifier.[70] A U.S. person can request access to an agency record about themselves. The request can be granted or denied, in whole or in part. Access granted can be subject to a payment of a fee. Denials of access can be appealed. A person can also request to amend or correct the record on them, which can be granted or denied, in whole or in part. Some types of records require the agency to keep a log detailing the instances where the record was disclosed to (shared with) others. The Act provides a means for a person to request an accounting of any such disclosures made by the agency to another person, organization, or agency of the record on the requestor.

One significant rule under the Privacy Act is the ''No Disclosure Without Consent'' rule. This means ''no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to ten exceptions].''[71] The two exceptions relevant in this context are: (1) the ''need to know within agency,'' exception,[72] and the ''routine use'' exception.[73]

The ''need to know'' within the agency exception applies to ''those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.''[74] The second applicable exception is for routine agency uses, which must have been previously published in the *Federal Register*.[75] The Act defines ''routine use'' to mean ''with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.''[76] This routine use exception sets forth two requirements for a proper routine use disclosure: (1) *Federal Register* publication, thereby providing constructive notice; and (2) compatibility.[77] The routine use exception's notice provision requires agencies to plan in advance what uses the agencies will make of information.[78] The requirement for ''compatibility'' includes uses that are the functional equivalent to the published uses, and those necessary to the exercise of the published uses.[79]

The DoD has published a routine use Systems of Records Notice (SORN), in the *Federal Register* for biometrics collected from detainees, and can be found under the reference of A0025-2c SAIS DoD.[80] The detainee SORN is applicable to U.S. persons who are suspected terrorists or otherwise detained through military operations. As previously noted, under the provisions of the Privacy Act, federal agencies are prohibited from sharing U.S. person biometric information without that individual's written consent, unless an exception applies. The sharing of DoD's biometric information data on U.S. person detainees is accomplished using both of the above noted exceptions. In the first instance, biometric data is disclosed to another DoD entity with a need to know. In the second instance, biometric data is disclosed consistent with the listed routine uses published in the applicable SORN in the *Federal Register*. The SORN for the Army Biometrics program includes a routine use specifically providing for sharing terrorism related information. That routine use provides for sharing:

*To Federal, State, tribal, local, or foreign agencies for the purposes of law enforcement, counterterrorism, immigration management and control, and homeland security, or for purposes of protecting the territory, people, and interests of the United States of America against breaches of security related to DoD controlled information or facilities, and against terrorist activity.*[81]

A key point is that most of DoD's biometric data files in the detainee database are of non-U.S. persons; and, the Privacy Act expressly does not apply to non-U.S. persons.

## International Privacy Interests

The recognition and protection of privacy interests is not unique to American jurisprudence. One of the first international documents to reference a privacy interest was the *Universal Declaration of Human Rights, 1948,* where in Article 12 it was proclaimed that: ''No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.''[82] More specific protections were incorporated in the Council of Europe: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, in 1981.[83]

The more recent European Union Data Protection Directive, Council Directive 95/46 of the European Parliament, and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995,[84] is a fairly

[70] 5 U.S.C. § 552a(d)(1) (2000).
[71] 5 U.S.C. § 552a(b) (2000).
[72] 5 U.S.C. § 552a(b)(1) (2000).
[73] 5 U.S.C. § 552a(b)(3) (2000).
[74] See OMB Guidelines, 40 Fed. Reg. 28,948, 28,950-01, 28,954 (July 9, 1975). This ''need to know'' exception authorizes the intra-agency disclosure of a record for necessary, official purposes. See, http://www.usdoj.gov/oip/1974condis.htm#exceptions.
[75] 552a(e)(4)(D) requires *Federal Register* publication of ''each routine use of the records contained in the system, including the categories of users and the purpose of such use.''
[76] 552a(a)(7).
[77] See, e.g., Britt v. Naval Investigative Serv., 886 F.2d 544, 547-50 (3d Cir. 1989); Shannon v. Gen. Elec. Co., 812 F. Supp. 308, 316 (N.D.N.Y. 1993).
[78] 120 Cong. Rec. 40,881 (1974).
[79] See OMB Guidelines, 52 Fed. Reg. 12,990, 12,993 (Apr. 20, 1987).
[80] See http://www.dod.mil/privacy/notices/army/A0025-2c_SAIS-DoD.html.
[81] *Id.*
[82] Adopted and proclaimed by U.N. General Assembly resolution 217 A (III) of 10 December 1948. The same language was repeated in Article 17 of the International Covenant Civil Political Rights, 1966, International Covenant on Civil and Political Rights, G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976. See also, Article 8, European Convention on Human Rights & Fundamental Freedoms, available at http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.
[83] COE, ETS No. 108, January 28, 1981, entered into force on Oct. 1, 1985. See, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.
[84] The EU Data Protection Directive 95/46, O.J. (L 281), Nov. 23, 1995 p. 31, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

comprehensive attempt to protect information privacy. Article 6 of Directive 95/46, (somewhat similar to the U.S. Privacy Act), requires that personal data be: processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; accurate and, where necessary, kept up to date; and, every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. Articles 10 through 12 of Directive 95/46 require notice to the individual regarding the collection of the personal information, notice of the purpose for the collection, and, aside from statistical or historical purposes, provides for a right of the individual to access and potentially correct inaccurate information. There are some notable security exceptions to these privacy interests as well; specifically, Article 13 provides that Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in certain listed Articles, when such a restriction constitutes necessary measures to safeguard national security, defense, or public security; the prevention, investigation, detection and prosecution of criminal offenses; or of breaches of ethics for regulated professions. In short, this recent expression of the European concept of privacy expressly allows for ''exceptions'' necessary for national security and public safety that are similar to the routine use exception of the U.S. Privacy Act, as employed by the DoD biometrics routine use notice.

While these international documents do not directly impact the privacy protections of the DoD Biometrics program, they could affect the exchange (sharing) of biometric data collected on EU citizens provided from the EU to the United States. Articles 25 and 26 of the EU Directive restrict the transfer of ''personal data'' to countries outside the EU that do not offer a sufficient level of data protection.[85] Such data transfers from the EU to non-EU countries that lack an ''adequate level of protection'' are only permitted in certain defined situations, which include transfer based on important public interest grounds. Arguably, the prevention of terrorism is one such important public interest. But since the Privacy Act only provides the full scope of protections or access rights to U.S. persons, the EU members might be reluctant to exchange biometric files with DoD unless DoD applies full Privacy Act protections to biometrics files obtained on EU citizens.

[85] Id.

## DoD Biometric Privacy Protections

In compliance with U.S. law and regulation, DoD provides several layers of privacy protection for its detainee biometric information data files. All unclassified detainee biometric information files, whether of U.S. Persons or non-U.S. Persons, should be marked FOUO information and marked as information that may be exempt from mandatory release to the public under FOIA. As FOUO data files, detainee biometric information may be disseminated within the DoD components and between officials of the DoD components as necessary in the conduct of official business related to sharing terrorism information. All FOUO detainee biometric information may also be released to officials in other departments and agencies of the executive and judicial branches in performance of a valid government function related to terrorism information. U.S. person detainee biometric data information is subject to the protections of the Privacy Act, and is disclosed to those officers and employees of the agency who maintains the record who have a need for the record in the performance of their duties, and is released to other government agencies as a routine use exception, under the terrorism information data sharing authorities noted previously. The only significant difference in how DoD treats U.S. person detainee biometric data and non-U.S. person detainee biometric data is that the later group does not have the rights of access, amendment and correction, and accounting that U.S. persons have under the Privacy Act.

## Conclusion

DoD is employing biometrics capabilities and procedures to effectively collect, employ, and share counterterrorism information derived from those capabilities within DoD and with other federal agencies to reveal the identities of our terrorist adversaries and to verify the identities of our friends and allies. Biometric data on suspected terrorist detainees can and should be routinely shared within DoD and with federal and state agencies having a need for terrorism related information in such areas as: immigration, law enforcement, intelligence, counter-intelligence, border protections, and military operations. DoD's biometrics efforts have thus far resulted in the capture of hundreds of terrorists, arguably greatly enhancing the safety and security of Americans at home and overseas. Providing for the protection of privacy interests embodies society's attempt to accommodate the individual's exercise of socially acceptable liberties and freedoms. DoD is balancing privacy interests by using an effective, comprehensive, coordinated means of sharing terrorism information in a manner that safeguards an individual's legal rights and privacy expectations in accordance with applicable law, with the goal of making all Americans safer in this age of terrorism.

  PVLR ISSN 1538-3423