Appendix C

LEGAL ASSESSMENT: LEGAL CONCERNS RAISED BY THE U.S. ARMY'S USE OF BIOMETRICS[1]

EXECUTIVE SUMMARY

From the legal perspective, the Army's use of biometrics raises concerns in three critical areas. These include statutory and administrative law concerns, constitutional law concerns, and international law concerns. The major statutory and administrative law structure that applies to Army use of biometrics is imposed by the Privacy Act of 1974, which regulates the collection, maintenance, use, and dissemination of personal information by federal government agencies. Accordingly, this Act is examined in great detail.

Army use of biometrics implicates constitutional rights involving informational privacy and physical privacy under the Bill of Rights as well as religious freedom under the First Amendment. To help the Army understand these rights, background information is presented and important cases dealing with these issues are discussed. *Whalen v. Roe*, the Supreme Court's leading case on informational privacy, is analyzed from the perspective of what the Army can learn from this case. To help the Army understand the real-world setting in which these rights operate in the context of biometric applications, this appendix includes discussion of two legal challenges raised on reli-

[1]The principal author of this Appendix, John D. Woodward, Jr., Esq., appreciates the helpful comments and insights provided by Stewart A. Baker, Esq., Robert R. Belair, Esq., Arthur S. Di Dio, M.D., J.D., Professor Steve Goldberg of the Georgetown University Law Center, Kristina Larson, Catherine A. Szilagyi, Esq., and Shirley C. Woodward, Esq. Their assistance in no way implies their endorsement of the views presented in this appendix or acquiescence in any mistakes contained herein.

gious grounds to state-mandated biometric applications in New York and Connecticut. To help the Army understand how other federal agencies view possible legal objections to biometric applications, recent experience of the Federal Bureau of Investigation (FBI) in this area is detailed.

As the Army increasingly operates in the international arena, Army use of biometrics could raise issues of international law. To help the Army understand how a major international law related to privacy can affect biometric applications, the possible impact of the European Union Data Protection Directive on U.S. Army biometric applications in European Union member states is assessed. Similarly, the possible impact of laws of other foreign nations is also addressed.

After surveying the legal landscape related to biometrics, this review concludes that Army use of biometric applications in the United States should not encounter any significant legal obstacles, provided the Army complies with the mandates of the Privacy Act and the teachings of the Supreme Court. To ensure this compliance, Army leadership can call on the many institutional assets within DoD and the Army who are experienced and skilled in dealing with privacy issues. These assets can do a case-by-case analysis of the biometric application and determine exactly what needs to be done legally to ensure compliance. In sum, while biometrics is a new technology, the Army has an existing framework that can accommodate legal requirements.

As Army biometric applications venture overseas, the Army leadership must consider international law issues raised by these applications on a case-by-case basis. The impact of the European Union Data Protection Directive on the U.S. Army as a data collector in EU member states is not entirely clear. The United States and the EU agreed in July 2001 on a "safe harbor" framework, which provides U.S. organizations a means of satisfying the directive's requirement that personal data is afforded an "adequate" level of privacy protection. This safe harbor framework is designed primarily for private sector entities, however, and it does not appear that the Army would currently be eligible to join the safe harbor. It appears likely, however, that the Army's use of biometrics will comply with the directive by virtue of falling within one of its exceptions, although continued attention is required because the various exceptions and exemptions

to compliance have yet to be definitively interpreted. Although the EU directive is a new and controversial privacy law, the Army has a framework in place to monitor the issues raised by the directive and to provide the Army with the necessary legal support to ensure compliance.

STATUTORY AND ADMINISTRATIVE LAW CONCERNS

The Privacy Act of 1974

Overview. The Privacy Act of 1974 regulates the collection, maintenance, use, and dissemination of personal information by federal government agencies, including DoD and the U.S. Army.[2] It serves as the basis for both the DoD Privacy Program and Army Privacy Program.[3] The Act requires the Office of Management and Budget (OMB) to prescribe guidelines and regulations for federal agencies to use in implementing the Privacy Act and provide continuing assistance for and oversight of the implementation of the Privacy Act by agencies.[4]

In broad terms, the Privacy Act gives certain rights to the "data subject"—or the individual who provides personal information—and places certain responsibilities on the "data collector"—the agency collecting the personal information. The Privacy Act balances a federal agency's need to collect, use, and disseminate information about individuals with the privacy rights of those individuals. In particular, the Act tries to protect the individual from unwarranted invasions of privacy stemming from a federal agency's collection, maintenance, use, and dissemination of personal information about the individual.[5]

---

[2]The Privacy Act of 1974, codified at 5 U.S.C. § 552a, as amended, went into effect on September 27, 1975. See Department of Justice (1998 and 1999).

[3]The DoD Privacy Program is issued under the authority of DoD Directive 5400.11, dated June 9, 1982. DoD 5400.11-R, dated August 31, 1982, establishes regulations for the implementation of the DoD Privacy Program. AR 340-21, dated July 5, 1985, establishes regulations for the implementation of the Army Privacy Program.

[4]5 U.S.C. § 552a(v)(1) and (2).

[5]There are several things the Privacy Act does not do. For example, the Privacy Act does not regulate the collection, maintenance, use, and dissemination of personal information by state and local government agencies. See *Ortez v. Washington County,*

Along these same lines, the DoD Privacy Program "is intended to provide a comprehensive framework regulating how and when the Department collects, maintains, uses, or disseminates personal information on individuals. The purpose of the Program is to balance the information requirements and needs of the Department against the privacy interests and concerns of the individual" (DoD, 2000c). Similarly, the Army Privacy Program sets out "the privacy rights of individuals and the Army's responsibilities for compliance with operational requirements established by the Privacy Act."[6]

The Privacy Act's basic provisions, reflected in both the DoD Privacy Program and the Army Privacy Program,[7] include

- restricting federal agencies from disclosing personally identifiable records maintained by the agencies;
- requiring federal agencies to maintain records with accuracy and diligence;
- granting individuals increased rights to access records about them maintained by federal agencies and to amend their records, provided they show that the records are not accurate, relevant, timely, or complete; and
- requiring federal agencies to establish administrative, technical, and policy safeguards to protect record security.[8]

As these basic provisions suggest, the Privacy Act sets forth a so-called "code of fair information practices" requiring federal agencies, as data collectors, to adopt minimum standards for collection, use, maintenance, and dissemination of records. It also requires that

---

Oregon, 88 F.3d 804, 811 (9th Cir. 1996). The Privacy Act does not regulate personal information held by private sector entities. See 5 U.S.C. § 552a; 5 U.S.C. § 552f (definition of "agency"). See also *Gilbreath v. Guadalupe Hosp. Found.*, 5 F.3d 785, 791 (5th Cir. 1993). The Privacy Act does not apply when the individual, or data subject, is not a U.S. citizen or an alien lawfully admitted for permanent residence. See 5 U.S.C. § 552a(a)(4).

[6]AR 340-21 at ¶ 1-5.

[7]Unless otherwise indicated, the Privacy Act provisions discussed in this RAND Report apply to DoD and the U.S. Army.

[8]See, e.g., Cate (1997, p. 77) and Department of Justice (1998) at "Individual's Right of Access," "Individual's Right of Amendment," and "Agency Requirements."

agencies publish detailed descriptions of these standards and the procedures used to implement them. Data collector responsibilities are discussed below.

Applicability to Biometrics. Although the Privacy Act does not specifically mention "biometrics," our analysis strongly suggests that the Act can include Army biometric applications. As the Act applies to a "record" that is "contained in a system of records," the threshold issue to resolve is whether biometric identification information, whether in the form of an image file or a template file, falls within the Act's broad definition of record. The Act defines "record" as:

> [A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or *other identifying particular assigned to the individual, such as a finger or voice print or a photograph. . . .*[9]

The OMB *Guidelines* explain that "record" means "any item of information about an individual that includes an individual identifier" and "can include as little as one descriptive item about an individual."[10] The Court of Appeals for the Third Circuit has affirmed the *Guidelines*' definition, finding that "record" includes "any information about an individual that is linked to that individual through an identifying particular."[11] The Court of Appeals for the District of Columbia has stressed that the Privacy Act only protects "information that actually describes the individual in some way."[12]

As explained in the main body of this report, biometrics are distinctive individual identifiers. They are "identifying" and they are "particular" to an individual. Moreover, fingerprint and voiceprint, two of the examples cited in the Act's definition of "record," are physical characteristics. As such, they fall within the definition of

---

[9]See 5 U.S.C. § 552a(a)(4) (emphasis added).

[10]See OMB (1987) (quotations omitted). See also Department of Justice (1998) at "Definitions: D. Record."

[11]*Quinn v. Stone*, 978 F.2d 126, 133 (3d Cir. 1992).

[12]*Tobey v. N.L.R.B.*, 40 F.3d 469, 471-73 (D.C. Cir. 1994).

biometrics. Accordingly, biometrics satisfy the Privacy Act's definition of "record."

To fall within the Privacy Act, the record must be "contained in a system of records." The Act defines "system of record" as:

> [A] group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. . . .[13]

OMB's *Guidelines* explain that a system of records exists when two conditions are met. First, there must be an "indexing or retrieval capability using identifying particulars [that is] built into the system." Second, the agency must "in fact, retrieve records about individuals by reference to some personal identifier" (OMB, 1987, and Department of Justice, 1998, at "Definitions: E. System of Records"). Commenting on these OMB *Guidelines*, the Court of Appeals for the District of Columbia has explained that a federal agency must not only have "the capability to retrieve information indexed under a person's name, but the agency must in fact retrieve records in this way in order for a system of records to exist."[14]

To determine if an Army biometric application is a record contained in a system of records, the Army must do a case-by-case analysis of each application examining how the biometric is used. For some applications, it is possible that the Privacy Act would not be implicated because the record is not contained in a system of records. For example, the Army's Fort Sill pilot program did not implicate the Privacy Act because, while the biometrically protected digital cash card provided to Army basic trainees was arguably a record, the fingerprint template was stored only on the card. It was not contained in any system of records, such as a central database. On the other hand, some applications will implicate the Act. Such an application would include biometric identification information combined with information about an individual that can be retrieved by an identifying particular, like a biometric.

---

[13]See 5 U.S.C. § 552a(a)(5).

[14]*Henke v. United States Dep't of Commerce*, 83 F.3d 1453, 1460 n.12 (D.C. Cir. 1996).

In cases where an Army biometric application implicates the Privacy Act, the Army must make certain that it complies fully with the Act's provisions. In ensuring this compliance, the Army can draw on many existing institutional assets who have extensive experience in Privacy Act matters. These assets include the Defense Privacy Board,[15] the Assistant Secretary of Defense (Comptroller), the Defense Privacy Office, the DoD General Counsel, the Army Assistant Chief of Staff for Information Management, the Army General Counsel, the Army Judge Advocate General, the Army Office of the Deputy Chief of Staff for Personnel, OMB, and many others.

The Privacy Act's major requirements are explained below.

The "No Disclosure Without Consent Rule." The Privacy Act prohibits a federal agency from "disclos[ing] 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 certain exceptions discussed below]."[16] This provision is known as the "No Disclosure Without Consent Rule."

While the "No Disclosure Without Consent Rule" applies, the Act contains twelve enumerated exceptions to this rule.[17] The exceptions to the "No Disclosure Without Consent" Rule are as follows:

(1) The "Intra-Agency Need to Know" Exception

(2) The "Required Freedom of Information Act (FOIA) Disclosure" Exception

(3) The "Routine Use" Exception

(4) The "Bureau of the Census" Exception

---

[15]Membership of the Defense Privacy Board consists of the Director of the Defense Privacy Office, who sits as Executive Secretary, and Representatives designated by the Secretaries of the Military Departments, the Assistant Secretary of Defense (Comptroller) (whose designee serves as Chairperson), the Assistant Secretary of Defense (Manpower, Reserve Affairs, and Logistics), the DoD General Counsel, and the Director of the Defense Logistics Agency. See DoD 5400.11-R, ¶ 6.1.

[16]See 5 U.S.C. § 552a(b).

[17]See 5 U.S.C. § 552a(b)(1)-(12).

(5) The "Statistical Research" Exception

(6) The "National Archives" Exception

(7) The "Law Enforcement Request" Exception

(8) The "Individual Health or Safety" Exception

(9) The "Congressional" Exception

(10) The "General Accounting Office" Exception

(11) The "Judicial" Exception

(12) The "Debt Collection Act" Exception.

These broadly structured exceptions are discussed below.

The "Intra-Agency Need to Know" exception. This applies when officers and employees of the federal agency maintaining the record have a need for the record in the performance of their duties.[18] In the case of medical records, the Army construes this exception somewhat narrowly by restricting what is disclosed. For example, the applicable Army regulation provides that when "medical information is officially requested for a use other than patient care, only enough information will be provided to satisfy the request."[19]

The "Required Freedom of Information Act ("FOIA") Disclosure" exception. This exception provides that the Privacy Act cannot be used to prohibit a disclosure that the FOIA requires.[20]

The "Routine Use" exception. As for disclosure of a record, a "routine use" means "the use of such record for a purpose which is compati-

---

[18]See 5 U.S.C. § 552a(b)(1). See, e.g., *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 549 n.2 (3d Cir. 1989) (approving, as "intra-agency need to know" exception, disclosure of investigative report to Britt's Marine Corps Reserve commanding officer "since the Reserves might need to reevaluate Britt's access to sensitive information or the level of responsibility he was accorded"); *Beller v. Middendorf*, 632 F.2d 788, 798 n.6 (9th Cir. 1980) (approving disclosure of record revealing servicemember's homosexuality by Naval Investigative Service to commanding officer for purpose of reporting "a ground for discharging someone under his command").

[19]AR 40-66, ¶ 2.2(e), dated May 3, 1999.

[20]See 5 U.S.C. § 552a(b)(2). See also *Greentree v. United States Customs Serv.*, 674 F.2d 74, 79 (D.C. Cir. 1982) (Privacy Act is not to "be used as a barrier to FOIA access").

ble with the purpose for which it was collected."[21] The Privacy Act requires that the federal agency publish in the *Federal Register* "each routine use of the records contained in the system, including the categories of users and the purpose of such use."[22] Thus, the federal government agency must satisfy two requirements for a proper routine use disclosure: The routine use must be "compatible" and constructive notice must be given by publication of the agency's routine use in the *Federal Register*.[23]

According to OMB, compatibility encompasses functionally equivalent uses and other uses that are necessary and proper.[24] The federal judiciary has not settled on a uniform interpretation of compatibility. For example, the Court of Appeals for the District of Columbia has adopted a broadly construed "common usage" requiring only that "a proposed disclosure would not actually frustrate the purposes for which the information was gathered."[25] On the other hand, the Court of Appeals for the Third Circuit put forth a narrower construction: a "concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and its disclosure."[26] In cases where the federal judiciary must determine the legality of a federal agency's routine use, the judiciary gives deference to the federal government agency's construction of its routine use.[27]

---

[21]See 5 U.S.C. §§ 552a(b)(3); 552a(a)(7) (definition of "routine use").

[22]See 5 U.S.C. § 552a(e)(4)(D).

[23]Some federal courts have determined that a third requirement exists: Actual notice of the routine use must be given to the individual at the time the information is collected from him. See *United States Postal Service v. National Ass'n of Letter Carriers*, 9 F.3d 138, 146 (D.C. Cir. 1993) (stating that "[a]lthough the statute itself does not provide, in so many terms, that an agency's failure to provide employees with actual notice of its routine uses would prevent a disclosure from qualifying as a 'routine use,' that conclusion seems implicit in the structure and purpose of the Act"); *Covert v. Harrington*, 876 F.2d 751, 754-56 (9th Cir. 1989).

[24]See OMB (1987), 52 Fed. Reg. 12,990, 12,993.

[25]*United States Postal Service v. National Ass'n of Letter Carriers*, 9 F.3d 138, 144 (D.C. Cir. 1993).

[26]*Britt v. Naval Investigative Service*, 886 F.2d 544, 555 (3d Cir. 1989).

[27]See, e.g., *Department of the Air Force, Scott Air Force Base, Ill. v. FLRA*, 104 F.3d 1396, 1402 (D.C. Cir. 1997); *FLRA v. U.S. Dep't of Treasury*, 884 F.2d 1446, 1451 (D.C. Cir. 1989).

Two important types of "compatible" routine uses frequently occur with respect to law enforcement. First, in the context of investigations and prosecutions, law enforcement agencies routinely share law enforcement records with each other.[28] Second, agencies may routinely disclose any records indicating a possible violation of law, regardless of the purpose for collection, to law enforcement agencies for purposes of investigation and prosecution.[29] For example, the Army has published a so-called "law enforcement blanket routine use" which applies to every record system maintained within the Army, unless a specific exception is made. One such exception is that the "law enforcement blanket routine use" does not apply to the "Armed Forces Repository of Specimen Samples for the Identification of Remains" system of records, which includes "specimen collections from which a DNA typing can be obtained."[30]

The "law enforcement blanket routine use" provides that:

> In the event that a system of records maintained by [the Army] to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.[31]

---

[28]See, e.g., OMB (1987, 40 Fed. Reg. 28,955) (proper routine use is "transfer by a law enforcement agency of protective intelligence information to the Secret Service"); see also 28 U.S.C. § 534 (authorizing Attorney General to exchange criminal records with "authorized officials of the Federal Government, the States, cities, and penal and other institutions").

[29]See OMB (1987, 40 Fed. Reg. 28,953); see also 28 U.S.C. § 535(b) (1994) (requiring agencies of the Executive Branch to expeditiously report "[a]ny information, allegation, or complaint" relating to crimes involving government officers and employees to United States Attorney General).

[30]See 63 Fed. Reg. 10,205, March 2, 1998. See also Armed Forces (2000). See also Appendix B, Program Reports, DoD DNA Specimen Repository for Remains Identification.

[31]*Preamble to the Department of Army Privacy Act Systems of Records Notice*, available at http://www.defenselink.mil/privacy/notices/army/army_preamble.html. Additional Army blanket routine uses are published at this site.

Because of its "potential breadth," the routine use exception is a controversial provision of the Privacy Act.[32] For example, it has been called "a huge loophole"[33] that has been used by federal agencies to justify almost any use of the data (Cate, 1997, p. 78, footnote omitted). The two law enforcement routine use exceptions discussed above have been criticized on the ground that they circumvent the more restrictive requirements of the routine use exception.[34]

Moreover, Congress can always mandate additional new "routine uses" for agencies, which the affected agencies must establish as "routine uses" (OMB, 1987, 40 Fed. Reg. 28,954). For example, Congress has mandated the establishment of a federal "Parent Locator Service" within the Department of Health and Human Services and requires federal agencies to comply with requests from the Secretary of HHS for addresses and places of employment of absent parents.[35]

The "Bureau of the Census" exception. This exception is for disclosure of information made to the U.S. Bureau of the Census for purposes of planning or carrying out a census or related activity pursuant to statute.[36]

The "Statistical Research" exception. This exception permits disclosure of information to entities that will use the information for statistical research or a reporting record. The information must be transferred to the entity in a form that is not individually identifiable.[37]

---

[32]See Department of Justice (1998), "Conditions of Disclosure to Third Parties: B. Twelve Exceptions to the 'No Disclosure Without Consent' Rule: 3. 5 U.S.C. § 552a(b)3 (routine uses)."

[33]See Cate (1997, p. 78), citing David Flaherty, the former British Columbia Data Protection Commissioner (footnote omitted).

[34]See Department of Justice (1998) (citing *Privacy Commission Report* at 517–518; Britt, 886 F.2d at 548 n.1 (dictum); *Covert*, 667 F. Supp. at 739, 742 (dictum)). See also Privacy International, *Privacy and Human Rights 1999* (asserting that the Privacy Act's effectiveness is "significantly weakened by administrative interpretations [of the routine use exception]").

[35]See 42 U.S.C. § 653.

[36]See 5 U.S.C. § 552a(b)(4).

[37]See 5 U.S.C. § 552a(b)(5).

The "National Archives" exception. This limited exception permits disclosure of records that have sufficient historical or other value to warrant consideration for their preservation by the U.S. government.[38]

The "Law Enforcement" exception. This exception provides for disclosure of information to federal law enforcement agencies and allows an agency, "upon receipt of a written request, [to] disclose a record to another agency or unit of State or local government for a civil or criminal law enforcement activity."[39]

The "Individual Health or Safety" exception. This exception permits disclosure of information pursuant to a showing of compelling circumstances affecting the health or safety of an individual.[40] For example, dental records on several individuals could be released to identify an individual injured in an accident.

The "Congressional" exception. This exception applies to disclosure of information to the House of Representatives and the Senate or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee.[41]

The "General Accounting Office" exception. This exception applies to disclosure of information to the Comptroller General in the course of the performance of the duties of the General Accounting Office.[42]

The "Judicial" exception. This exception applies to court orders requiring disclosure.[43] It prevents the Privacy Act from "be[ing] used to block the normal course of court proceedings, including court-ordered discovery."[44] Some disagreement exists as to what exactly constitutes a "court order." The issue centers on whether a subpoena issued by a court clerk, as opposed to the court itself,

---

[38]See 5 U.S.C. § 552a(b)(6).

[39]See OMB (1987, 40 Fed. Reg. 28,948, 28,955); 5 U.S.C. § 552a(b)(7).

[40]See 5 U.S.C. § 552a(b)(8).

[41]See 5 U.S.C. § 552a(b)(9).

[42]See 5 U.S.C. § 552a(b)(10).

[43]See 5 U.S.C. § 552a(b)(10).

[44]See *Clavir v. United States*, 84 F.R.D. 612, 614 (S.D.N.Y. 1979).

should qualify under this exception. A Defense Privacy Board Advisory Opinion has concluded that, "[a] subpoena signed by a clerk of a Federal or State court, without specific approval of the court itself, does not comprise an 'order of a court of competent jurisdiction' for purposes of nonconsensual disclosures [under the judicial exception]. . . . [D]isclosure of records [under this exception] requires that the court specifically order disclosure" (DoD, 2000b). Similarly, the Court of Appeals for the District of Columbia has held that a subpoena routinely issued by a court clerk—such as a federal grand jury subpoena—is not a "court order" within the meaning of this exception because it is not "specifically approved" by a judge.[45]

The "Debt Collection Act" exception. The Debt Collection Act of 1982 authorized this disclosure exception. It permits agencies to disclose bad debt information to credit bureaus. Before disclosing this information, however, agencies must complete a series of due process steps designed to validate the debt and to offer the individual an opportunity to repay it.[46]

Under the Privacy Act, rights are personal to the individual who is the subject of the federal agency record. These rights cannot be asserted by others on behalf of the aggrieved individual.[47]

Agency Responsibilities. *Overview:* The Privacy Act places certain responsibilities on the data collector. These responsibilities include publishing information about the systems of records in the data collector's charge, giving notice to data subjects of the uses to which the data will be put, and safeguarding data.

Publication: Among the responsibilities the Privacy Act places on the data collector, it requires an "agency that maintains a system of records" to "publish in the *Federal Register* upon establishment or revision a notice of the existence and character of the system of

---

[45]See *Doe v. DiGenova*, 779 F.2d 74, 77-85 (D.C. Cir. 1985).

[46]See 5 U.S.C. § 552a(b)(11); OMB (1987, 48 Fed. Reg. 15,556-60).

[47]See, e.g., *Parks v. IRS*, 618 F.2d 677, 684-85 (10th Cir. 1980) (which holds that a union lacks standing to litigate its members' Privacy Act claims); *Word v. United States*, 604 F.2d 1127, 1129 (8th Cir. 1979) (which holds that a criminal defendant lacks standing to allege Privacy Act violations regarding use at trial of medical records concerning third party); *Dresser Indus. v. United States*, 596 F.2d 1231, 1238 (5th Cir. 1991) (which holds that a company lacks standing to litigate employees' Privacy Act claims).

records."[48] This notice, which is known as a "Privacy Act Systems of Records Notice," must include

- the name and location of the system;
- the categories of individuals about whom records are maintained in the system;
- the categories of records maintained in the system;
- each routine use of the records contained in the system, including the categories of users and the purpose of such use;
- the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
- the title and business address of the agency official responsible for the system of records;
- the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
- the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
- the categories of sources of records in the system.[49]

The Army has 249 systems of records for which such notice must be published (DoD, 2000a). These range from "Official Personnel Folders and General Personnel Files" (AAFES 0401.04) to "Individual Health" (AAFES 0405.11) to "Carpool Information/Registration System" (A0001SAIS) and many others (DoD, 2000a).

The Privacy Act permits a federal agency to promulgate rules to exempt systems of records from certain parts of the Privacy Act if certain conditions are met. One such condition is if the system of records is maintained as a principal function by a law enforcement

[48]See 5 U.S.C. § 552a(e)(4).

[49]See 5 U.S.C. § 552a(e)(4)(A)-(I).

agency and the records were compiled for law enforcement purposes.[50] Other conditions include if the system of records contains classified information;[51] investigatory material compiled for law enforcement purposes;[52] material maintained and used solely as statistical records;[53] investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service federal contracts or access to classified information;[54] and other conditions.[55]

As Army use of biometrics will likely lead to the establishment of new systems of records and revisions to old systems, the Army must comply with this Privacy Act Systems of Records Notice requirement. As its 249 systems of records suggest, the Army has ample experience in doing so.

Notice: The Privacy Act requires the data collector to give notice[56] to the data subject informing him of four factors:

- The authority that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary.
- The principal purpose or purposes for which the information is intended to be used.
- The routine uses that may be made of the information.
- The effects on the data subject if any, of not providing all or any part of the requested information.[57]

---

[50] 5 U.S.C. § 552a(j)(2).

[51] 5 U.S.C. § 552a(k)(1).

[52] 5 U.S.C. § 552a(k)(2).

[53] 5 U.S.C. § 552a(k)(4).

[54] 5 U.S.C. § 552a(k)(5).

[55] See, e.g., 5 U.S.C. § 552a(k)(4) ("U.S. Secret Service" exception); 5 U.S.C. § 552a(k)(6) ("testing materials" exception).

[56] This notice may be given (1) on the actual form which the data collector uses to collect the information desired or (2) on a separate form that can be retained by the individual. See 5 U.S.C. § 552a(e)(3).

[57] See 5 U.S.C. § 552a(e)(3)(A)-(D). The authority may be granted by statute or executive order of the President. See 5 U.S.C. § 552a(e)(3)(A).

In its biometric applications, the Army will likely comply with the Privacy Act's notice requirement during the biometric enrollment process, when it first collects the biometric identification information from the data subject. As an institution that collects much information from many individuals, the Army has extensive experience in satisfying the notice requirement.

Data Safeguarding: The Privacy Act requires the data collector to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records." Similarly, the Act requires the data collector "to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained."[58]

As this provision of the Act makes clear, the data collector must put in place appropriate safeguards to protect information in its databases. However, as a federal district court has explained, "[t]he Privacy Act does not make administrative agencies guarantors of the integrity and security of materials which they generate."[59] Instead, "the agencies are to decide for themselves how to manage their record security problems, within the broad parameters set out by the Act."[60] Accordingly, the data collectors "have broad discretion to choose among alternative methods of securing their records commensurate with their needs, objectives, procedures, and resources."[61]

The Senate Report accompanying the Privacy Act supports this judicial view:

> The Committee recognizes the variety of technical security needs of the many different agency systems and files containing personal information as well as the cost and range of possible technological

---

[58]See 5 U.S.C. § 552a(e)(10).

[59]*Kostyu v. United States*, 742 F.Supp. 413, 417 (E.D. Mich. 1990) (which holds that alleged lapses in IRS security resulting in disclosure of information to public were not willful and intentional as required to establish Privacy Act violation).

[60]*Id.*

[61]*Id.*

> methods of meeting those needs. The Committee, therefore, has not required [ ] in this Act a general set of technical standards for security of systems. Rather, the agency is merely required to establish those administrative and technical safeguards which it determines appropriate and finds technologically feasible for the adequate protection of the confidentiality of the particular information it keeps against purloining, unauthorized access, and political pressures to yield the information to persons with no formal need for it.[62]

The Senate Report stressed that data collectors have flexibility in deciding appropriate safeguards:

> The [Privacy] Act . . . provides reasonable leeway for agency allotment of resources to implement this subsection. At the agency level, it allows for a certain amount of "risk management" whereby administrators weigh the importance and likelihood of the threats against the availability of security measures and consideration of cost.[63]

While a breach of database security and confidentiality can be harmful or embarrassing to the data collector, both the agency and the employee responsible for the breach can be found legally liable for a Privacy Act violation. This legal liability can include civil liability for the agency and criminal liability for an agency official. Civil liability for such a breach attaches when "the agency has acted in a manner which was intentional or willful."[64] The federal judiciary has interpreted this phrase "to require a showing of fault 'somewhat greater than gross negligence.' "[65]

Similarly, criminal liability, in the form of a misdemeanor, attaches for such a breach when an "officer or employee of an agency, who by virtue of his employment or official position, has possession of, or

---

[62]*Id.* (citing S.Rep. No. 93-1183, reprinted in 1974 U.S. Code Cong. & Admin. News 6916, 6969).

[63]*Id.* (citing S.Rep. No. 93-1183, reprinted in 1974 U.S. Code Cong. & Admin. News 6916, 6969).

[64]See 5 U.S.C. § 552a(g)(4); *Pilon v. United States Department of Justice*, 796 F.Supp. 7, 12 (D.D.C. 1992); *Kostyu*, 742 F.Supp. at 416.

[65]*Kostyu*, 742 F.Supp. at 416.

access to, agency records [covered by the Privacy Act], and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it."[66] Likewise, criminal liability can attach when an "officer or employee of any agency [ ] willfully maintains a system of records without meeting the notice requirements of [the Privacy Act]."[67]

In implementing its biometric applications that fall under the Privacy Act, the Army must meet all of the Act's many requirements. Successfully meeting these requirements will require a comprehensive, coordinated effort drawing on DoD's Privacy Act institutional assets as well as the Army's appropriate technical, security, law enforcement, and administrative assets. However, the Army has complied with the Privacy Act in the past, is complying now, and should continue to comply in the future. Fortunately, the Army has a seasoned and experienced structure already in place to ensure Privacy Act compliance.

Additional Safeguards. *The Computer Matching and Privacy Act of 1988*: The Computer Matching and Privacy Act of 1988 ("The Computer Matching Act") amended the Privacy Act by adding new provisions regulating federal agencies' computer matching practices and placing requirements on the agencies.[68] A computer match is done by using a computer program to search an agency's files for infor-

---

[66]See 5 U.S.C. § 552a(i)(1). Certain exemptions apply. See, e.g., 5 U.S.C. § 552a(j).

[67]See 5 U.S.C. § 552a(i)(2). Certain exemptions apply. See, e.g., 5 U.S.C. § 552a(j).

[68]See 5 U.S.C. § 552a(o) (1988). See also Turkington and Allen (1999, pp. 362–363), from which this section is largely drawn. The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act to add several new provisions. These include 5 U.S.C. § 552a(a)(8)-(13), (e)(12), (o), (p), (q), (r), and (u). These provisions add procedural requirements for agencies to follow when engaging in computer matching activities; provide matching subjects with opportunities to receive notice and to refute adverse information before having a benefit denied or terminated; and require that agencies engaged in matching activities establish Data Integrity Boards to oversee those activities. These provisions became effective on December 31, 1989. OMB's guidelines on computer matching should be consulted in this area. See 54 Fed. Reg. 25,818-29 (1989). Subsequently, Congress enacted the Computer Matching and Privacy Protection Amendments of 1990, which further clarify the due process provisions found in subsection (p). OMB's proposed guidelines on these amendments appear at 56 Fed. Reg. 18,599-601 (proposed April 23, 1991). See Department of Justice (1998) at "Computer Matching."

mation associated with or indexed by a personal identifier, such as a name or SSN. The information thus obtained can then be compared with information in the databases of another federal agency. In this way, discrepancies and inconsistencies might be discovered that point to fraud in government benefits, for example.

DoD participates in approximately 25 computer matching programs with various different government agencies (DoD, 2000d). For example, DoD has a "Debt Collection" matching program in effect with the Department of Education. The purpose of this program is to identify and locate federal personnel who are delinquent on payments to certain programs administered by the Department of Education.

For all of its matching programs, DoD must meet the Computer Matching Act's requirements, which basically involve entering into formal agreements with the exchanging agencies,[69] verifying independently the accuracy of data received before any official action is taken,[70] providing notice in the *Federal Register* prior to conducting or revising a computer matching program,[71] and establishing a Data Integrity Board to monitor implementation and compliance with the Act.[72]

Because a personal identifier in the form of a biometric could implicate the Computer Matching Act, the Army will need to study the Act closely to determine whether the Army's specific biometric application is implicated. As with the Privacy Act, the Army can call on many existing institutional assets with experience in matters pertaining to the Computer Matching Act.

Administrative Regulation: From the administrative regulatory perspective, Congress can follow two well-worn policy paths when dealing with a public policy issue involving a new technology, such as biometrics. It can take the direct route and pass legislation regulating Army use of the technology or it can delegate its authority to

---

[69]See 5 U.S.C. § 552a(o)(1)(A-D).

[70]See 5 U.S.C. § 552a(o)(1)(E).

[71]See 5 U.S.C. § 552a(o)(1)(D).

[72]See 5 U.S.C. § 552a(u)(1).

the appropriate administrative agencies within DoD. The delegation route is the road most frequently traveled. However, even though the Army, specifically, and DoD, in general, are well-equipped with expertise, experience, and institutional memory, they still face enormous challenges in designing, formulating, and implementing government policy for biometric applications. In addition, numerous competing groups (many well-organized and some politically influential) will want to press their claims in this public policy process.[73]

The Army should bear in mind that Congress, through the legislative process, can require the Army to satisfy additional conditions related to its biometric applications. For example, Congress could go beyond the Privacy Act and place additional prohibitions on disclosure of biometric identification information and further restrict sharing.

The Uniform Code of Military Justice (UCMJ) and Privacy Protections. Historically, the Supreme Court has long recognized that differences between the civilian and military criminal law systems exist. The Court has stated that "[m]ilitary law, like state law, is a jurisprudence which exists separate and apart from the law which governs in our federal establishment."[74] Most important, the Court has acknowledged that the military criminal law system, embodied by the UCMJ, can impose restrictions on a servicemember's rights. However, the UCMJ does not strip a servicemember of his or her constitutional rights. As the Court of Military Appeals has observed: "[I]t is apparent that the protections in the Bill of Rights, except those which are expressly or by necessary implication inapplicable, are available to members of our armed forces."[75] For example, the Supreme Court has explained that the special demands of "military life do not, of course, render nugatory in the military context the guarantees of the First Amendment."[76] In the context of Army biometric applications, however, the UCMJ does not seem to provide

---

[73]See generally Goldberg (1994).

[74]*Burns v. Wilson*, 346 U.S. 137, 140 (1953).

[75]*United States v. Jacoby*, 29 C.M.R. 244 (C.M.A. 1960) (*citing Burns v. Wilson*, 346 U.S. 137 (1953); *Shapiro v. United States*, 69 F.Supp. 205 (Ct. Cl. 1947); *United States v. Hiatt*, 141 F.2d 664 (3d Cir. 1944).

[76]*Goldman v. Weinberger*, 475 U.S. 503 (1986).

servicemembers with any greater privacy rights beyond what is in the U.S. Constitution.

CONSTITUTIONAL LAW CONCERNS

Introduction

Beyond the specific individual rights provided by statutory and regulatory regimes, the Constitution, through its Bill of Rights, protects individual privacy rights. These constitutionally protected privacy rights consist of physical, decisional, and informational privacy rights. These privacy rights do not pose a constitutional barrier to Army biometric applications, provided that the Army follows the guidance of the Supreme Court as explained in this section.

Overview. As the Army expands its biometric applications and requires more and more members of the Army community to provide biometric identification information, it is likely that someone required to participate will refuse and (1) face disciplinary action within the military justice system, if the refuser is under its jurisdiction, and/or (2) file a federal lawsuit, claiming his constitutional rights are violated. The military is no stranger to such litigation.[77] This section of the appendix begins by examining how the federal judiciary views the military. It then explores the major bases of any legal challenges that might be brought on constitutional grounds.

Judicial Deference to Military. Several Supreme Court decisions have established that the federal judiciary views the nation's military as uniquely different from civilian society. For example, then-Justice William H. Rehnquist explained that the Supreme Court "ha[s] repeatedly held that 'the military is, by necessity, a specialized society separate from civilian society.' "[78] In the preparation and performance of its duties, "the military must insist upon a respect for duty

---

[77] *Id*. (involving Air Force officer who brought lawsuit against the Secretary of Defense claiming that the uniform regulation that prevented him from wearing his yarmulke infringed on his constitutional rights).

[78] *Id*. at 507 (citing *Parker v. Levy*, 417 U.S. 733, 743 (1974); *Chappell v. Wallace*, 462 U.S. 296, 300 (1983); *Schlesinger v. Councilman*, 420 U.S. 738, 757 (1975); *Orloff v. Willoughby*, 345 U.S. 83, 94 (1953)). See also *Burns v. Wilson*, 346 U.S. at 140.

and a discipline without counterpart in civilian life."[79] "[W]ithin the military community, there is simply not the same [individual] autonomy as there is in the larger civilian community."[80]

The Supreme Court recognizes that "the military authorities have been charged by the Executive and Legislative Branches with carrying out our Nation's military policy."[81] Moreover, the Supreme Court has observed that the "courts [are] 'ill-equipped to determine the impact upon discipline that any particular intrusion upon military authority might have.' "[82] Therefore, "[j]udicial deference . . . is at its apogee when legislative action under the congressional authority to raise and support armies and make rules and regulations for their governance is challenged."[83] The Court has determined that "[j]udges are not given the task of running the Army."[84] Rather, "[t]he responsibility for setting up channels through which . . . grievances can be considered and fairly settled rests upon the Congress and upon the President of the United States and his subordinates. The military constitutes a specialized community governed by a separate discipline from that of the civilian."[85] Because the military is so different from the civilian community, "[o]rderly government requires that the judiciary be as scrupulous not to interfere with legitimate Army matters as the Army must be scrupulous not to intervene in judicial matters."[86]

This judicial deference that the federal judiciary gives to the military suggests that the federal courts may be somewhat reluctant to intrude into proper Army concerns related to biometrics. However, the federal courts will not hesitate to protect the constitutional rights of an individual. To help ensure that it receives this deference, the

---

[79]*Schlesinger v. Councilman*, 420 U.S. at 757. See also *Brown v. Glines*, 444 U.S. 348, 354 (1980).

[80]*Goldman v. Weinberger*, 475 U.S. at 507 (citing *Parker v. Levy*, 417 U.S. at 751).

[81]*Id.*

[82]*Id.* (citing *Chappell v. Wallace*, 462 U.S. at 305, quoting Warren, 1962).

[83]*Goldman v. Weinberger*, 475 U.S. at 508 (quoting *Rostker v. Goldberg*, 453 U.S. 57, 70 (1981)).

[84]*Orloff v. Willoughby*, 345 U.S. at 93-94.

[85]*Id.*

[86]*Id.*

Army should be prepared to demonstrate that each of its biometric applications serves a worthwhile and useful military purpose.

What Privacy Rights Does the U.S. Constitution Recognize?

Survey of Privacy Scholarship. Jurists and scholars have long grappled with defining what privacy is and explaining what privacy should be (Cate, 1997, pp. 19–31).[87] In 1879, Judge Thomas M. Cooley, in his classic treatise on torts, included "the right to be let alone" as a class of tort rights, asserting that "[t]he right to one's person may be said to be a right of complete immunity" (Hixson, 1987, p. 30, and Goldberg, 1994, p. 114). Echoing and popularizing Cooley's phrase, Samuel D. Warren and Louis D. Brandeis (1890), in their landmark law review article, *The Right to Privacy*, voiced their view of privacy as a "right to be let alone." Brandeis, as a Supreme Court Justice, used this phrase in his famous dissent in *Olmstead v. United States*, declaring that the Founding Fathers "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[88] Privacy as the "right to be let alone" has a positive appeal and commendable simplicity, but the phrase has been criticized in that "legally, it offers no guidance at all. Coveting an indefinable right is one thing; enforcing it in a court of law is another" (Alderman and Kennedy, 1995, p. xiv).

More recent scholarship also offers insight into privacy. For example, Ruth Gavison (1980, pp. 421, 428) offers what is perhaps the extreme privacy model: "[P]rivacy is a limitation of others' access to an individual . . . [I]n perfect privacy no one has any information about X, no one pays any attention to X, and no one has physical access to X." Privacy includes a control aspect—"control we have over information about ourselves" (Fried, 1970, p. 140), "control over who can sense us" (Parker, 1974, pp. 275, 281, internal quotation marks omitted), or "control over the intimacies of personal identity" (Gerety, 1977, pp. 233, 236) Based on her survey of the extensive privacy literature, Professor Lillian R. Bevier (1995, pp. 455, 458, foot-

---

[87]While a detailed discussion of the many facets of privacy is beyond the scope of this report, an excellent starting point is Turkington and Allen (1999).

[88]277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); see also Cate (1997, p. 57) and Goldberg (1994, p. 114).

note omitted) concluded, "[p]rivacy is a chameleon-like word, used denotatively to designate a range of wildly disparate interests—from confidentiality of personal information to reproductive autonomy—and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name."[89]

Constitutional Background. The word "privacy," like the word "biometrics," is nowhere to be found in the text of the U.S. Constitution. However, without making explicit reference to privacy, the Constitution nonetheless protects certain privacy interests.[90] The Bill of Rights contains these protections in the First Amendment rights of freedom of speech, press, religion and association; the Third Amendment prohibition against the quartering of soldiers in one's home; the Fourth Amendment right to be free from unreasonable searches and seizures; the Fifth Amendment right against self-incrimination; the Ninth Amendment's provision that "[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people"; and the Tenth Amendment's provision that "[t]he powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."

What then is the constitutional right to privacy and how does it affect biometrics used in U.S. Army applications? The answer to the first part of the question is legally fuzzy. As a federal appellate court has recently observed, "[w]hile the Supreme Court has expressed uncertainty regarding the precise bounds of the constitutional 'zone of privacy,' its existence is firmly established."[91]

Most modern constitutional privacy interests have their roots in the Due Process Clause of the Fourteenth Amendment. This clause says that no state shall "deprive any person of life, liberty, or property, without due process of law." For more than 100 years, these words have been interpreted by the Supreme Court to contain a substantive

---

[89]See also Murphy (1996, p. 2381).

[90]Or "zones of privacy," to use Justice Douglas's term. *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965) (holding unconstitutional a state statute that criminalized the sale of contraceptives to married couples).

[91]*In re Crawford*, 1999 U.S. App. LEXIS 24941, *7 (9th Cir. 1999) (citing *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977); *Griswold v. Connecticut*, 381 U.S. at 483).

protection that "bar[s] certain government actions regardless of the fairness of the procedures used to implement them."[92]

Three Forms of Privacy. The Supreme Court has stressed that "there is a realm of personal liberty which the government may not enter."[93] This realm, or zone of privacy, consists of rights that are "fundamental" or "implicit in the concept of ordered liberty"[94] or as a later Court would put it, "deeply rooted in this Nation's history and tradition."[95] In what specific areas of the zone of privacy is the government forbidden entry? In considering privacy interests, the Court has implicitly categorized privacy as taking three distinct forms (Allen, 1991, p. 175).[96] These three forms of privacy include:

- Physical privacy or freedom from contact with other people or monitoring agents. Physical privacy enjoys its greatest constitutional protection under the Fourth Amendment freedom from unreasonable search and seizure.
- Decisional privacy or the freedom of the individual to make private choices about the personal and intimate matters that affect him without undue government interference. The Court has found that the individual is constitutionally protected in "personal decisions relating to marriage, procreation, contraception, family relationships, child rearing, and education."[97]

---

[92] *Planned Parenthood of Southeastern Pennsylvania v. Casey*, 505 U.S. 833, 846 (1992) (quoting *Daniels v. Williams*, 474 U.S. 327, 331 (1986)).

[93] *Id.* at 847.

[94] *Griswold v. Connecticut*, 381 U.S. at 500 (Harlan, J., concurring) (quoting *Palko v. Connecticut*, 302 U.S. 319, 325 (1937)).

[95] *Moore v. City of East Cleveland*, 431 U.S. 494, 503 (1977). These terms have been criticized for lack of clarity. See, e.g., Bork (1990, p. 118) "[T]he judge-created phrases specify no particular freedom, but merely assure us, in sonorous phrases, that they, the judges, will know what freedoms are required when the time comes."

[96] At least one scholar has more broadly categorized the Supreme Court's interpretation of constitutional protections for individual privacy as falling into four areas—"expression and association, searches and seizures, fundamental decisionmaking, and informational privacy" (Cate, 1997, p. 52).

[97] *Planned Parenthood v. Casey*, 505 U.S. at 851. In determining the commonality of these personal decisions and why they deserve constitutional protection, the Court, through Justice Sandra Day O'Connor's opinion in *Casey*, explained that:

> These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity

- Informational privacy or freedom of the individual to limit access to certain personal information about oneself. The Court of Appeals for the Ninth Circuit has defined this phrase as "the individual interest in avoiding disclosure of personal matters."[98] Privacy scholar Alan Westin defines it as "the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 337, citing Scott and Jarnagin, 1868, pp. 457–507). Similarly, Professor Lawrence Lessig (1999, p. 143), drawing heavily on the scholarship of Ethan Katsh (1995, p. 228), has defined privacy in this context as "the power to control what others can come to know about you." As Lessig explains, others can acquire information about you by monitoring and searching. Monitoring refers to that part of one's daily existence that others see, observe, and can respond to. Searching refers to that part of one's life that leaves or is a record that can later be scrutinized (Lessig, 1999, p. 143). Noting both quantity and quality aspects to informational privacy, a federal appellate court has phrased it in terms of, "control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of knowledge as well."[99]

The Army's use of biometrics could potentially require its soldiers, civilian employees, independent contractors, along with many other

---

> and autonomy, are central to the liberty protected by the Fourteenth Amendment. At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the attributes of personhood were they formed under compulsion of the State.

[98] *Doe v. Attorney General*, 941 F.2d 780, 795 (9th Cir. 1991) (quoting *Whalen*, 429 U.S. at 599-600). As the Supreme Court has not yet ruled definitively on the issue, the federal judiciary has no unified view as to whether there is a constitutionally protected right to informational privacy. The majority of circuits considering this issue (the Second, Third, Fifth, and Ninth Circuits) find that there is. See, e.g., *Doe v. City of New York*, 15 F.3d 264, 267 (2d Cir. 1994) (concluding there is "a recognized constitutional right to privacy in personal information"); *Fadjo v. Coon*, 633 F.2d 1172, 1175-76 (5th Cir. 1981); *United States v. Westinghouse*, 638 F.2d 570, 577 (3d Cir. 1980), and *Roe v. Sherry*, 91 F.3d 1270, 1274 (9th Cir. 1996); *Doe v. Attorney General*, 941 F.2d at 795-96. A minority conclude there is not. See *J.P. v. DeSanti*, 653 F.2d 1080, 1090 (6th Cir. 1981).

[99] *United States v. Westinghouse Elec. Corp.*, 638 F.2d at 577 n.5.

individuals, such as dependents, retirees, and foreign nationals, to participate in officially sanctioned biometric programs. In such programs, individuals would be compelled to provide biometric identification information to the Army for collection, maintenance, use and dissemination in Army databases. Such Army-mandated use of biometrics implicates physical and informational privacy concerns and, to a lesser extent, decisional privacy concerns.[100]

Physical Privacy. *Constitutional challenges to fingerprinting in noncriminal context.* The overwhelming majority of the Army's biometric applications will fall into the noncriminal context, for such matters as network or physical security, fraud prevention, convenience, efficiency, etc. While the federal courts have not had occasion to rule on the government-mandated use of biometrics, many decisions have established that an individual has minimal constitutional privileges concerning his fingerprints.[101]

Moreover, the courts have upheld numerous federal, state, and municipal requirements mandating fingerprinting for employment and licensing purposes, provided that the government has a rational basis for requiring fingerprinting (*American Law Reports*, 1999, p. 732).[102] In a federal context, the so-called rational basis test means that Congress must show that the fingerprinting requirement bears a rational relationship to a legitimate government objective or interest.[103] For example, courts have upheld government-mandated

---

[100]The following hypothetical example might illustrate how decisional privacy concerns could be implicated by a biometric scheme. In response to growing concerns about missing children, the Army decides to require all children attending day care programs on Army bases to be biometrically scanned for identification purposes. Parents object on the grounds that they are fully satisfied with the less-intrusive security already offered at the day care programs on Army bases and that their children will be unduly traumatized by the scanning. Educational zone of privacy concerns are possibly implicated.

[101]See, e.g., *Davis v. Mississippi*, 394 U.S. 721, 727 (1969); *Schmerber v. California*, 384 U.S. 757, 764 (1966).

[102]See also, e.g., Department of Justice (1990, pp. 48–52).

[103]See, e.g., *Utility Workers Union of America, AFL-CIO, v. Nuclear Regulatory Commission*, 664 F.Supp. 136, 139 (S.D.N.Y. 1987); *Iacobucci v. City of Newport*, 785 F.2d 1354, 1355-56 (6th Cir. 1986), *rev'd on other grounds*, 479 U.S. 921 (1986); *Thom v. New York Stock Exchange*, 306 F.Supp. 1002, 1010 (S.D.N.Y. 1969). The rational basis test is a lesser standard of judicial scrutiny than the compelling state interest test. Courts apply the compelling state interest test when state action affects the exercise of

fingerprinting for employment and licensing purposes in connection with the taking of fingerprints for spouses of liquor licensees; male employees of alcoholic beverage wholesalers; taxi drivers; cabaret employees; bartenders; dealers in secondhand articles; all employees of member firms of national security exchanges registered with the Securities and Exchange Commission; and all individuals permitted unescorted access to nuclear power facilities.[104]

For example, in *Utility Workers Union of America v. Nuclear Regulatory Commission*, a union representing 5,170 utility workers in nuclear power plants challenged as unconstitutional that part of a newly enacted federal statute requiring that these workers be fingerprinted.[105] The union claimed the fingerprinting requirement violated the workers' Fourth Amendment and privacy rights. The federal district court disagreed and upheld the fingerprinting requirement. Citing a long string of cases, the court noted that in noncriminal contexts, the judiciary has "regularly upheld fingerprinting of employees."[106]

As for the constitutional right to privacy claim, the court quoted from a leading federal appellate court case:

> Whatever the outer limits of the right to privacy, clearly it cannot be extended to apply to a procedure the Supreme Court regards as only minimally intrusive. Enhanced protection has been held to apply only to such fundamental decisions as contraception . . . and family living arrangements. Fingerprints have not been held to merit the same level of constitutional concern.[107]

Moreover, in applying the rational basis test, the court noted congressional concern over an incident of sabotage at a nuclear power

---

a fundamental right, such as political speech. See, e.g., Department of Justice (1990, p. 48).

[104]See *American Law Reports* (1999, p. 732, citations omitted); *Utility Workers Union of America*, 664 F.Supp. at 136.

[105]*Utility Workers Union of America*, at 136. The union directed its challenge to Section 606 of the Omnibus Diplomatic Security and Anti-Terrorism Act of 1986, codified as section 149 of the Atomic Energy Act of 1954, 42 U.S.C. § 2169 (1986). 10 C.F.R. § 73.57 implements the statute.

[106]*Id.* at 138-39 (citations omitted).

[107]*Id.* at 139 (quoting *Iacobucci v. City of Newport*, 785 F.2d at 1357-58).

plant in Virginia and concluded that "[u]sing fingerprints to verify the identity and any existing criminal history of workers with access to vital areas or safeguards information is a rational method of clearing these workers."[108]

Similarly, in a case involving a challenge to a New York state regulation requiring fingerprinting of all employees of national stock exchanges, a federal district court found that "[p]ossession of an individual's fingerprints does not create an atmosphere of general surveillance or indicate that they will be used for inadmissible purposes. Fingerprints provide a simple means of identification no more." The court observed that as long as the government had a "valid justification . . . for the taking of the prints under reasonable circumstances, their use for future identification purposes even in criminal investigations, is not impermissible."[109]

Constitutional challenges to fingerprinting in a criminal justice context: What will happen when Army authorities want a biometric identifier from a member of the Army community whom they suspect has committed a crime? Capturing the biometric identifier in this context should not run afoul of the Constitution. The Fourth Amendment to the U.S. Constitution governs searches and seizures conducted by government agents. It provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." As the amendment makes clear, the Constitution does not forbid all searches and seizures, only "unreasonable" ones. The Supreme Court defines a search as an invasion of a person's reasonable expectations of privacy.[110] To evaluate whether providing a biometric identifier in a criminal justice context constitutes a search, the judiciary focuses on two factors. First, the court examines the nature of the intrusion.[111] Actual physical intrusions into the body, such as blood-drawing,[112] Breathalyzer testing, and urine analysis,[113] can

---

[108] *Utility Workers Union of America*, 664 F.Supp. at 139.

[109] *Thom v. New York Stock Exchange*, 306 F.Supp. at 1010.

[110] See, e.g., *Katz v. United States*, 389 U.S. 347, 360-62 (1967) (Harlan, J., concurring).

[111] See *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 616 (1989).

[112] See *Schmerber v. California*, 384 U.S. at 767-68.

[113] See *Skinner*, 489 U.S. at 618.

constitute Fourth Amendment searches. Second, the court examines the scope of the intrusiveness paying close attention to the "host of private medical facts" revealed during the search.[114]

In the criminal justice context, the Supreme Court has examined the issue of whether acquiring information about an individual's personal characteristics constitutes a search. It has found that requiring a person to give voice exemplars is not a search because "the physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public," such that "no person can have a reasonable expectation that others will not know the sound of his voice."[115] Using the same reasoning, the Court has ruled that requiring a person to give handwriting exemplars is not a search.[116] It has also described fingerprinting as nothing more than obtaining "physical characteristics . . . constantly exposed to the public,"[117] and that fingerprinting "involves none of the probing into an individual's private life and thoughts that marks an interrogation or search."[118]

In cases where provision of a biometric identifier might be found to constitute a search (as in the hypothetical case of a physically intrusive DNA-based biometric that would reveal extensive private medical facts about the individual), "the ultimate measure of the constitutionality of a governmental search is 'reasonableness.' "[119] To make this determination, a court must balance the "intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[120] In the criminal context, a search is "reasonable" only if the law enforcement agency has probable cause of criminal activity.[121]

---

[114]See *id.* at 617.

[115]*United States v. Dionisio*, 410 U.S. 1, 93 (1973). See also LaFave et al., *Criminal Procedure*, Vol. 2, § 3.2(g) (LaFave et al., 1999).

[116]*United States v. Mara*, 410 U.S. 19, 93 (1973).

[117]*Cupp v. Murphy*, 412 U.S. 291 (1973).

[118]*Davis v. Mississippi*, 394 U.S. at 726-727. See also LaFave, *Criminal Procedure* at § 3.2(g).

[119]*Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995).

[120]*Id.* (quoting *Skinner*, 489 U.S. at 619) (internal quotation marks omitted).

[121]See *Zurcher v. Stanford Daily*, 436 U.S. 547, 554-55 (1978).

FBI experience: As the Army considers various biometric applications, it might benefit from study of the FBI experience involving the bureau's searchable criminal and civil fingerprint databases. In particular, the conclusion of the FBI's Office of the General Counsel (OGC) that the FBI's use for criminal justice purposes of fingerprint records obtained from servicemembers and federal employees is "legally unobjectionable" should be of interest to the Army.

Currently, individuals serving in the military service and those persons applying for federal employment must undergo fingerprinting.[122] While some of this fingerprinting is still done using the traditional ink-and-paper ten-print cards, much of it is being done electronically as a biometric, resulting in an image file, that can be transformed into a template. Eventually, all fingerprinting will be done through some type of biometric process.

By way of background, Congress in 1924 authorized the Department of Justice to begin collecting fingerprint and arrest record information voluntarily submitted for federal and state arrests. In 1930, Congress created the FBI's identification division, giving it responsibility for "acquiring, collecting, classifying, and preserving criminal identification and other crime records" and authorizing the exchange of these criminal identification records with authorized state, and local officials.[123] Today, the FBI's Criminal Justice Information Services (CJIS) Division is the world's largest fingerprint repository. Its current file holdings of fingerprint cards total over 219 million. This figure grows by over 5,000 each day (Archer, 1997).

The fingerprint records obtained from military members, federal applicants and others are submitted to the FBI. CJIS runs the finger-

---

[122]Executive Order 10450 (1953) requires federal employees in positions affecting the national security to submit fingerprints. Both DoD and the Army have Personnel Security Programs. These programs establish comprehensive policies and procedures applicable to personnel in the Army and other military branches; civilian employees in the DoD and Department of the Army; Army and DoD contractors; as well as other affiliated persons. Examples of affiliated persons include Red Cross or United Service Organizations personnel. The DoD Personnel Security Program and Army Personnel Security Program require the subject of each personnel security investigation to "provide fingerprints of a quality acceptable to the FBI" among other things. See 32 C.F.R. §§ 154.35, 154.8; AR 380-67, dated September 9, 1988.

[123]See *United States Department of Justice v. Reporters Committee for Freedom of Press*, 489 U.S. 749 (1989).

print record against its integrated, automated "criminal files" database in Clarksburg, West Virginia, to determine if the individual has any past criminal involvement.[124] CJIS receives about 32,000 fingerprint cards a day for such processing.[125] This database contains a comprehensive fingerprint record of individuals fingerprinted after arrest or incarceration (FBI, 1995).[126] CJIS has converted all of these fingerprint records into electronic format. Moreover, state and local criminal justice agencies have the capability to transmit their fingerprint records to CJIS electronically. Thus, the "criminal files" database is readily and easily searchable (FBI, 1999).[127]

If the criminal history background search reveals an individual's past criminal involvement, the fingerprint record becomes part of the "criminal files" database. This database has more than 132 million criminal cards representing 36.1 million individuals who have been arrested or convicted of a criminal offense in the United States.

If the search reveals no criminal history, the fingerprint record is kept in the CJIS "civil files" database (FBI, 1995). The "civil files" database maintains approximately 87 million civil fingerprint cards represent-

---

[124]See, e.g., FBI (1995). This process is sometimes referred to as a National Agency Check (NAC). See e.g., AR 380-67.

[125]This number includes criminal history background searches requested by federal and state governments and others for various permit, license and employment clearances in addition to federal employment applications and military service. See FBI (1995).

[126]See also *Identification Division Records System Notice*, printed in 55 Fed. Reg. 49174 (Vol. 55, No. 227, November 26, 1990).

[127]On August 10, 1999, FBI Director Louis J. Freeh inaugurated the full operation of the Integrated Automated Fingerprint Identification System (IAFIS), which provides federal, state, and local criminal justice agencies the ability to transmit fingerprint information electronically. Previously, criminal justice agencies mailed ink and paper fingerprint cards to the FBI for processing. After the cards were received, a semiautomated system classified the fingerprints and compared them to the fingerprint cards in the FBI's CJIS fingerprint database. This identification process sometimes took weeks to complete. IAFIS will compare the submitted images with its huge database of fingerprints, and respond within two hours. The response will include a complete criminal history of the person, if one exists. Even if the person fingerprinted provides false identification, IAFIS will make a positive identification by matching fingerprints. For a discussion of law enforcement use of such automated systems, see Garfinkel (2000, pp. 41–46) (in his book, Garfinkel expresses concerns about biometric technologies eroding privacy).

ing approximately 39 million people.[128] These individuals have been fingerprinted as a result of federal employment applications or military service, for alien registration and naturalization purposes, as well as for voluntary submission for personal identification purposes.[129]

The "civil files" database is not fully automated. The vast bulk of its fingerprint records are the paper and ink variety. However, since last year, the FBI has taken steps to automate the database from "Day One forward" as it receives biometric versions, i.e., new fingerprint cards in electronic (biometric) format (CJIS, 1998). The FBI also has the option of scanning into the database the paper and ink records to convert them into electronic format. The FBI could also electronically organize subfiles, known as Special Latent Cognizant (SLC) files, within the "civil files" database. For example, the FBI could organize an SLC file of fingerprints of DoD employees and military members. By getting civil fingerprint records electronically recorded into the "civil files" database and by organizing extensive SLC files, or subsets, within it, the "civil files" database, like the "criminal files" database, would be easily and readily searchable.

From a criminal investigative point of view, the capability to access and search latent fingerprints against all the fingerprint records in the "civil file" database would be of great benefit to law enforcement. For example, a latent fingerprint found at a crime scene on a military base could be searched against the DoD SLC file in the "civil files" database. In this way, more crimes could be solved.

In 1995, the FBI asked its OGC for its legal opinion as to whether the FBI could conduct such searches of its "civil files" database. After review, OGC concluded that "[u]sing civil fingerprint records for criminal justice purposes is legally unobjectionable" (FBI, 1995).[130] OGC determined that the use of CJIS "civil files" for criminal justice purposes is consistent with the Privacy Act because it is a routine

---

[128]See, e.g., CJIS (1998). Some people have more than one fingerprint record in the database. For example, many military veterans take employment with the federal government.

[129]See, e.g., CJIS (1998). The number of fingerprint records from voluntary submissions is very small.

[130]Please note: This OGC opinion does not have the force of law.

use. The two requirements for routine use are compatibility with the original use for which the data were collected and *Federal Register* publication.[131] OGC determined that the compatibility requirement is met because "using fingerprints collected for criminal history check purposes for criminal justice identification purposes is . . . completely compatible with the purposes for which they were first collected" (FBI, 1995). OGC also determined that because the FBI has properly published the routine use in the *Federal Register*,[132] "after reading the notice, no reasonable person could claim to be surprised to find that [his] fingerprints, once submitted to the FBI, will be used by the Bureau for identification purposes in either a criminal justice or civil setting" (FBI, 1995). Similarly, drawing on some of the case law discussed above, OGC determined that no constitutional right to privacy exists in an individual's identity and criminal history background.[133]

In sum, OGC has concluded that it is legally unobjectionable for the FBI to search its "civil files" database, which it can organize into SLC

---

[131] 5 U.S.C. § 552a(e)(4)(D).

[132] The FBI changed the routine uses set forth in the "Fingerprint Identification Record System" notice in February 1996. The notice reads, in pertinent part:

> Identification and criminal history record information within this system of records may be disclosed as follows:
>
> > To a Federal, State, or local law enforcement agency, or agency/organization directly engaged in criminal justice activity (including the police, prosecution, penal, probation/parole, and the judiciary), and/or to a foreign or international agency/organization, consistent with international treaties, conventions, and/or executive agreements, *where such disclosure may assist the recipient in the performance of a law enforcement function, and/or for the purpose of eliciting information that may assist the FBI in performing a law enforcement function; to a Federal, State, or local agency/organization for a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual criminal law enforcement efforts of the law enforcement community. . . .*

See 61 Fed. Reg. 6386 (Vol. 61, No. 34, February 20, 1996) (emphasis added).

[133] See FBI (1995) (quoting *Trade Waste Mgt Ass'n v. Hughey*, 780 F.2d 221, 234 (3d Cir. 1985), "While it may be that when conduct resulting in the convictions or charges was engaged in the person who engaged in it expected that such participation would remain secret, that expectation was never reinforced by law.")

subsets. This conclusion suggests that it would be legally unobjectionable for the Army, were it so inclined on policy grounds, to coordinate with the FBI to have the FBI organize an SLC file consisting of the overall Army community, or various SLC files containing further subsets of the Army community, such as active-duty and Department of the Army civilians, which the FBI could then search. The OGC conclusion further suggests that it would be legally unobjectionable for the Army, were it so inclined on policy grounds, to organize its own similar "civil" database of biometric identification information and search this database for criminal justice identification purposes, provided that the Army received the proper authority to do so and complied with the Privacy Act requirements, as the FBI did. No apparent constitutional barriers stand in the way. Before embarking on these database paths, however, the Army should undertake a detailed legal analysis based on exactly what it wants to do to make certain it is on firm legal ground. In addition, the Army will have to assess policy concerns related to such uses.

DMDC experience: The Defense Manpower Data Center (DMDC) operates what is arguably DoD's largest biometric database. DMDC's experiences in this regard might be instructive to the Army. (The DMDC experience is also included in Appendix B.)

The Federal Managers' Financial Integrity Act of 1982 requires federal managers to establish internal controls to provide reasonable assurance that funds, property and other assets are protected against fraud or other unlawful use. As a result of this legislation, DoD launched Operation Mongoose, a fraud prevention and detection initiative. Operation Mongoose exposed a number of fraud schemes and indicated that DoD needed to improve servicemember identification and verification procedures. Responding to the need for better fraud prevention measures, the Acting Under Secretary of Defense (Personnel and Readiness) gave authority to the DMDC to initiate an electronic fingerprint capture policy in 1997.[134]

Since 1998, the DMDC has been capturing the right index fingerprint of all active-duty, reserve, and retired military personnel as well as survivors receiving a military annuity. This potential enrollment

[134]See Finch (1997) and, generally, Harreld (1999).

pool is some three million people. The print is captured during routine issuance (or reissuance) of military ID cards at some 900 DMDC sites. DMDC stores electronic copies of these fingerprints (the file images and the templates) in a comprehensive database, the Defense Enrollment Eligibility Reporting System (DEERS). DMDC stores no copies of fingerprints on the actual military ID card. DEERS can be accessed if a person's identity needs to be authenticated.

The DEERS database is believed to be the largest biometric database in DoD. As such, it complies with the Privacy Act. The Defense Privacy Office and other institutional assets assisted in ensuring compliance. To date, no successful legal challenge has been brought against the DMDC's biometric database.

Information Privacy—*Whalen v. Roe*.[135] *Introduction to Whalen v. Roe*: The Supreme Court's 1977 decision in *Whalen v. Roe* "began the process of identifying the elements of an American constitutional right of informational privacy" (Schwartz, 1995).[136] In 1999, a federal court cited *Whalen* for the proposition that "the Constitution protects an individual's privacy right to avoid disclosure of personal information."[137]

Whalen involved the constitutional question of whether the state of New York could record and store, in a centralized computer database, "the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs."[138]

---

[135]This section of the report is largely drawn from Woodward (1997a).

[136]Other legal scholars have perhaps interpreted the significance of *Whalen v. Roe* slightly differently. See, e.g., Allen (1991, p. 181), "The Court has come closest to recognizing an independent right of information privacy in *Whalen v. Roe*"; Roch (1986, pp. 71, 89), "[I]n *Whalen v. Roe*, the court [sic] recognized in dicta that there may exist a right to protect against improper disclosure of personal data."; Cate (1997, p. 63), "[H]aving found this new privacy interest in nondisclosure of personal information, the Court . . . applying a lower level of scrutiny, found that the statute did not infringe the individual's interest in nondisclosure"); and Strauss et al. (1995, p. 874), "A requirement that information of arguable utility to a lawful regulatory program be collected or submitted is unlikely to fall beyond the constitutional power of either federal or state government."

[137]*Wilson v. Pennsylvania State Police*, CA 94-6547, 1999 U.S. Dist. LEXIS 3165 *5 (E.D. Pa. March 11, 1999) (U.S. Mag. Judge Hart) (citing *Whalen v. Roe*, 429 U.S. at 599-600). See also *In re Crawford*, 1999 U.S. App. LEXIS 24941 at *16.

[138]*Whalen v. Roe*, 429 U.S. at 591.

While technology has changed greatly since 1977, the legal reasoning in *Whalen* is still relevant, particularly for biometrics, and more important, for the Army's use of biometrics. *Whalen* is instructive because it demonstrates the federal judiciary's likely approach to deciding some of the major constitutional law issues likely to be raised by Army-mandated biometric applications. Accordingly, the facts of the case, the holding, and the judicial reasoning deserve detailed examination.

Facts: In 1970, the New York legislature, disturbed about the growing drug problem, established a commission to evaluate the state's drug control laws.[139] After study, the commission made recommendations to correct perceived deficiencies in these state laws. Following up on these recommendations, the legislature amended the New York Public Health Law to require that "all prescriptions for Schedule II drugs" had to be prepared by the physician on an official state-provided form.[140] The completed form identified

- the prescribing physician;
- the dispensing pharmacy;
- the prescribed drug and prescribed dosage; and,
- the name, address, and age of the patient.

The statute required that a copy of the completed form be forwarded to the New York State Department of Health in Albany.[141] Albany received about 100,000 Schedule II prescription forms each month. There, the government agency recorded the information on magnetic tapes for eventual processing by computer. Based on his study of other states' reporting systems, the commission's chairman found

---

[139]See *id.* This commission was formally known as The Temporary State Commission to Evaluate the Drug Laws. See *id.* at 592 n.4.

[140]*Id.* at 593. The statute classified potentially harmful drugs in five schedules which conformed with relevant federal law. Schedule II drugs included the most dangerous of the legitimate drugs. Examples of such drugs would include opium, methadone, amphetamines, and methaqualone. These drugs all have accepted medical uses. The statute also provided for an emergency exception.

[141]The office which received the forms was the Bureau of Controlled Substances, Licensing and Evaluation. See *Roe v. Ingraham*, 403 F. Supp. 931, 932 (S.D.N.Y. 1975), *rev'd, Whalen v. Roe*, 429 U.S. 589 (1977).

that this comprehensive government-mandated database would serve two purposes: It would be a "useful adjunct to the proper identification of culpable professionals and unscrupulous drug abusers," and it would provide the authorities a "reliable statistical indication of the pattern of [the state's] drug flow" to help stop the diversion of lawfully manufactured drugs into the illegal market.[142]

Patients, doctors, and physicians' associations challenged the New York statute in court. The evidence offered before the federal district court, where the case was first heard, included testimony from

- two parents who "were concerned that their children would be stigmatized [as drug addicts] by the State's central filing system";
- three adult patients who "feared disclosure of their names" to unauthorized third parties; and,
- four physicians who believed that the New York statute "entrenches on patients' privacy and that each had observed a reaction of shock, fear, and concern on the part of their patients."[143]

The parties thus advanced two related privacy concerns, which eventually reached the Supreme Court's consideration: "the nondisclosure of private information," or informational privacy, and an individual's "interest in making important decisions independently," or decisional privacy.

Holding: In his opinion for the Court, Justice John Paul Stevens, joined by the Chief Justice and five other justices, found that "neither the immediate nor the threatened impact of the [statute's] patient-identification requirements . . . on either the reputation or the independence of patients . . . is sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment."[144] With these words, the Supreme Court rejected the privacy claim. In sum, the nation's highest court ruled that a government's centralized,

---

[142] *Whalen v. Roe,* 429 U.S. at 592 n.6.

[143] *Id.*

[144] *Id.* at 603-04.

computerized database containing massive amounts of sensitive medical information passed constitutional muster.

Judicial reasoning: What factors influenced the Supreme Court's reasoning? First, the Court seemed impressed by the New York legislature's creation of a specially appointed commission that held many hearings on and conducted a thorough study of the state's drug problem.[145] The commission consulted extensively with authorities in other states that used central reporting systems effectively. In other words, a commission empowered by the legislature had done its homework in an attempt to help solve the menacing problem of drugs. The Court concluded that the statute was "manifestly the product of an orderly and rational legislative decision."[146]

Arguably, the New York statute had not had much of an impact on the drug problem. For example, 20 months after its enactment, examination of the database led to only two investigations involving illegal use of drugs. As a kind of political process check, the Court explained that the state legislature, which gave this patient identification requirement its legal life, can also sound its death knell if it turns out to be an "unwise experiment."

In its analysis of the informational privacy concerns raised, the Court paid close attention to what specific steps the state agency had taken to prevent any unauthorized disclosures of information from the centralized database. In particular, the Court noted the following:

- The forms and records were kept in a physically secure facility.
- The computer system was secured by restricting the number of computer terminals that could access the database.
- Employee access to the database was strictly limited.
- There were criminal sanctions for unauthorized disclosure.

The Supreme Court took a somewhat practical approach to the way personal information is used in the contemporary age. It accepted

---

[145]See *id.* at 591. The Temporary State Commission to Evaluate the Drug Laws issued two reports, which the legislature made part of the legislative history of the statute.

[146]*Id.* at 597.

the view that disclosure of such medical information to various government agencies and private sector organizations, such as insurance companies, is "often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient. Requiring such disclosures to representatives of the State having responsibility for the health of the community does not automatically amount to an impermissible invasion of privacy."[147]

In addressing decisional privacy issues, the Court acknowledged genuine concern that the very existence of the database will disturb some people so greatly that they will refuse to go to the doctor to get necessary medication. However, given the large number of prescriptions processed at Albany, the Court came to the conclusion that the "statute did not deprive the public of access to the [legal] drugs."[148]

The Court's opinion concluded with a cautionary note that still echoes loudly 23 years later:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.[149]

The New York statute and its related implementation showed "a proper concern with, and protection of, the individual's interest in privacy."[150] The Court, however, limited the effect of its decision by reserving for another day consideration of legal questions that could arise from unauthorized disclosures of information from a

---

[147] *Id.* at 602 (footnote omitted).

[148] *Id.* (noting that Albany received approximately 100,000 prescription forms for Schedule II drugs monthly).

[149] *Id.* at 605.

[150] *Id.*

government database "by a system that did not contain comparable security provisions."[151]

Justice Brennan's concurring opinion: In his concurring opinion, Justice William Brennan, more so than his colleagues, expressed his concern over the potential erosion of informational privacy in the face of emerging technologies. "The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."[152] While this specific "carefully designed program" did not "amount to a deprivation of constitutionally protected privacy interests," Justice Brennan suggested that there is a core right to informational privacy and stressed that future programs might be subjected to a compelling state interest test or strict scrutiny by the court of the government action.[153]

Justice Stewart's concurring opinion: Justice Potter Stewart, in his concurrence, took issue with what he implicitly viewed as Justice Brennan's expansive privacy approach as well as with his brethren's view of constitutional privacy interests. According to Stewart, no general right of privacy can be found in the Constitution. Moreover, in Stewart's view, privacy concerns are matters left largely to the individual states.[154]

Cautionary note: The *Whalen* Court expressed its concern about the potential for "unwarranted disclosures" from the government's databases. As Professor Bevier, writing in a similar context, has explained:

> The fact that the government collects such great quantities of data gives rise to concern . . . that the data will be inappropriately disseminated, within government or to outsiders, or that it will be otherwise misused or abused. Recent advances in computer technology, which permit data to be manipulated, organized, compiled,

---

[151] *Id.* at 605-06.

[152] *Id.* (Brennan, J., concurring).

[153] See *id.* (Brennan, J., concurring).

[154] See *id.* (Stewart, J., concurring).

> transferred, distributed, and retrieved with hitherto unimaginable ease, exacerbate such concern. (Bevier, 1995, p. 457.)[155]

With the exception of Justice Stewart, all of the justices adopted a prospective approach. That is, by intensely focusing on the facts of *Whalen*, the Court left itself ample judicial wiggle room to find that government-mandated use of new technologies combined with powerful computer systems might lack necessary constitutional safeguards. Because the *Whalen* decision is tied so intimately to the specifics of *Whalen*, a future Court could easily distinguish the facts of a future case from the facts of *Whalen* to reach a different decision.

In sum, a lesson for the Army to take away from *Whalen* is that a future Court might find an informational privacy right violated unless the government agency collecting the information (1) had made clear its need and purpose in collecting the information and (2) had taken strong and effective measures to prevent unwarranted disclosures from its databases. In other words, if the government agency ignores these steps, the Court's cautionary note of *Whalen* could turn into a clear-sounding constitutional alarm bell in the future.[156]

The legacy of Whalen: Recent case law suggests that the federal judiciary accepts the informational privacy concept articulated in *Whalen*. In 1999, the Court of Appeals for the Ninth Circuit explained that one of the constitutionally protected privacy interests of *Whalen* is "the individual interest in avoiding disclosure of personal matters."[157] Moreover, the Ninth Circuit, like the *Whalen* court, found that the right to informational privacy is not absolute but must be balanced with the governmental interest.

In *In re Crawford*, the court held that federally required public disclosure of the SSNs of certain paralegals does not violate any consti-

---

[155]See also Garfinkel (2000, pp. 260–266).

[156]For this observation, the principal author thanks Professor Steve Goldberg of the Georgetown University Law Center who shared it in September 1996. Professor Goldberg explained that when a Supreme Court opinion offers broad pronouncements and little factual analysis, it is a sure sign that the Court is on comfortable turf. However, when the opinion deals with intense factual scrutiny, the Court is less sure of itself and thus keeping its options open for the long run.

[157]*In re Crawford*, 1999 U.S. App. LEXIS 24941 at *7-8.

tutional or statutory rights of these individuals. The federal law at issue requires a bankruptcy petition preparer (BPP), a type of paralegal, to include his or her SSN on all documents filed with the federal bankruptcy courts. By law, these documents are public records that can be accessed by anyone. Jack Ferm, a BPP, refused to provide his SSN on bankruptcy documents he had filed with a bankruptcy court in Nevada. He feared disclosure of his SSN would make him particularly vulnerable to the crime of identity theft. When the court fined him for refusing to provide his SSN, Ferm filed a lawsuit in federal court, claiming the disclosure of his SSN violated his privacy rights.

Although the court sympathized with Ferm's "speculative fear," it noted that an SSN, "unlike HIV status, sexual orientation, or genetic makeup" is "not inherently sensitive or intimate information, and its disclosure does not lead directly to injury, embarrassment, or stigma."[158] The court balanced Ferm's interest in nondisclosure of his SSN with the governmental interests. The many factors the court considered included:

> [T]he type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.[159]

The court found that the disclosure requirement serves the Bankruptcy Code's "public access" provision, which is rooted in the traditional right of public access to judicial proceedings. After weighing the many relevant factors, the court concluded:

> [T]he speculative possibility of identity theft is not enough to trump the importance of the governmental interests [requiring public disclosure]. In short, the balance tips in the government's favor.

---

[158] *Id.* at *13-14. In Ferm's case, he had not suffered any actual identity theft at the time he brought his suit, thus the court determined his fear as "speculative."

[159] *Id.* at *11 (citing *Doe v. Attorney General*, 941 F.2d at 796, quoting *Westinghouse*, 638 F.2d at 578).

> Accordingly, we cannot say that Congress transgressed the bounds of the Constitution in enacting the statutes at issue here.[160]

In re Crawford is a recent example illustrating that the Supreme Court's approach in *Whalen* remains firmly in place within the federal judiciary. It is prudent for the Army to study *Whalen* closely, to explain its military need for biometrics and to have database safeguards in place.

What Constitutionally Based Religious Concerns Does Biometrics Raise?

Overview. As explained above, some limited segments of American society have expressed religious objections to the use of biometrics. Among these objections, individuals oppose being compelled to participate in a government-mandated biometric application. The New York Department of Social Services and the Connecticut Department of Social Services (DSS) have encountered legal challenges based on religious concerns from entitlement program recipients who refused to provide a biometric identifier. Based on these objections, the Army might encounter a similar legal challenge to its mandated use of biometrics. Accordingly, the New York DSS and Connecticut DSS experiences might offer useful insights for the Army.

New York Experience. Liberty Buchanan, a New York resident, received AFDC and Food Stamps for herself and her four minor children. In 1996, New York DSS told her she would be required to participate in an AFIS. New York law required participation in AFIS as a condition of eligibility for AFDC and other entitlements.[161] Buchanan refused to participate in AFIS. She based her refusal on her religious convictions, grounded in part on her interpretation of the "mark of the beast" language in the Book of Revelation. Because she refused to provide a fingerprint, DSS discontinued the family's benefits. After a DSS agency hearing, the State Commissioner of Social Services affirmed the DSS decision, finding that Buchanan did not demonstrate a good cause basis for exemption from the finger

---

[160] *Id.* at *16. The court did, however, "encourage the Bankruptcy Courts to consider enacting rules to limit the disclosure of BPP SSNs."

[161] See 18 N.Y.C.R.R. § 351.2(a).

imaging requirement. Buchanan then appealed to the New York state court. After a hearing, the court found that Buchanan had failed to "set forth any competent proof that the AFIS actually involved any invasive procedures marking them in violation of [her] beliefs."[162] Accordingly, the court upheld the DSS decision.

Connecticut Experience. Similarly, in Connecticut, John Doe, his wife, and minor children—recipients of Temporary Family Assistance (TFA)—refused to submit to the Connecticut DSS digital imaging requirement.[163] Beginning in January 1996, DSS, pursuant to state law, began requiring all TFA recipients to be biometrically imaged for identification purposes by providing copies of the fingerprints of their two index fingers (*Uniform Policy Manual*, 2000).[164] In April 1996, Mr. and Mrs. Doe objected, based on their religious beliefs. DSS exempted them from the requirement in April 1996 and October 1997. In July 1998, however, DSS reviewed its policy and determined that the Does would have to comply with the digital imaging requirement. Doe requested a DSS hearing.

At the August 1998 hearing, he testified about his objections to providing a biometric identifier. He based these objections on his religious beliefs. Doe testified that the Book of Revelation discusses the "mark or number of the beast," which the "beast" tries to make all people receive on their hand or forehead. According to Doe, those who accept the mark "shall drink of the wine of the wrath of God" and be condemned. By submitting to digital imaging and allowing himself to be marked in this way, he would violate his religious convictions. He therefore requested a "good cause" exception to the digital imaging requirement as provided in the DSS regulations.[165]

In November 1998, the hearing officer ruled that Doe, "although having strong religious beliefs, some of which he interprets as a bar-

---

[162] *Buchanan v. Wing*, New York Supreme Court, Appellate Division, Third Judicial Department, December 4, 1997, 79341.

[163] "John Doe" is an alias used to protect the true identity of the individual out of respect for his and his family's privacy.

[164] See also Connecticut State DSS (1996, 2000).

[165] *Uniform Policy Manual* (2000), "Good cause is considered to exist when circumstances beyond the individual's control reasonably prevent participation with the Digital Imaging process."

rier for him to be digitally imaged, does not have as a result of this religious belief a circumstance beyond his control which prevents him from being digitally imaged" (Connecticut State DSS, 1998). Doe appealed from this final DSS decision to the Connecticut state court. While his case was pending, the DSS Commissioner decided to vacate the hearing decision and grant the Does an exception from the digital imaging requirement (Connecticut State DSS, 1999).

Goldman v. Weinberger. While the Army has not yet encountered any legal challenges to its biometric applications, the U.S. military has encountered objections to military regulations based on an individual's religious beliefs. One of the best-known legal challenges brought against the military on this basis is the case of *Goldman v. Weinberger*, decided by the Supreme Court in 1986.[166]

S. Simcha Goldman, an Air Force officer and ordained rabbi of the Orthodox Jewish faith, was ordered not to wear his yarmulke while on duty and in uniform, pursuant to Air Force regulations.[167] Goldman then brought an action in federal district court, claiming that the application of the Air Force regulation to prevent him from wearing his yarmulke infringed upon his First Amendment freedom to exercise his religious beliefs. The District Court agreed with Goldman and permanently enjoined the Air Force from enforcing the regulation against him. The Court of Appeals reversed, and Goldman appealed to the Supreme Court.

The Supreme Court held that Goldman's religious objections, grounded in the First Amendment's free exercise of religion clause, did not prohibit the challenged regulation from being applied to Goldman, even though its effect is to restrict the wearing of the headgear required by his religious beliefs. The Court found that the First Amendment does not require the military to accommodate such practices as wearing a yarmulke in the face of the military's view that such practices would detract from the uniformity sought by dress regulations. In his majority opinion, then-Justice Rehnquist

---

[166]*Goldman v. Weinberger*, 475 U.S. at 503.

[167]Air Force Regulation 35-10 provides, in pertinent part, that authorized headgear may be worn out of doors but that indoors "[h]eadgear [may] not be worn . . . except by armed security police in the performance of their duties." AFR 35-10, ¶ 1-6.h(2)(f) (1980).

explained that, "when evaluating whether military needs justify a particular restriction on religiously motivated conduct, courts must give great deference to the professional judgment of military authorities concerning the relative importance of a particular military interest."[168]

Congress reacted to the *Goldman* decision by passing a statute effectively eviscerating the Court's ruling. In 1987, Congress amended the U.S. Code to permit a member of the armed forces to "wear an item of religious apparel while wearing the uniform of the member's armed force," with two exceptions: when "wearing of the item would interfere with the performance of the member's military duties" or if "the item of apparel is not neat and conservative."[169]

In 1990, the Supreme Court decided another important case involving religious beliefs. In *Employment Division, Department of Human Resources of Oregon v. Smith,* ("*Smith*"), Alfred Smith and Galen Black brought suit against the Oregon State Employment Division after it refused their claims for unemployment compensation.[170] Their employer had discharged them from their jobs on "misconduct" grounds because they had ingested peyote, a hallucinogen, as part of the sacramental observances of their Native American religion. Under Oregon law, peyote is a controlled substance and thus prohibited.

In *Smith*, the Supreme Court held that the First Amendment's free exercise of religion clause does not require exemption from a religiously neutral law for those whose religious beliefs preclude them from complying with the law. *Smith* holds that the legislature is free, however, to grant religious exemptions to the neutral laws if it so chooses.[171] Thus, in *Smith*, the First Amendment's free exercise clause did not prohibit the application of Oregon state drug laws to use of peyote for religious purposes. However, were it so inclined, the Oregon state legislature could create a religious exemption.

---

[168] *Goldman v. Weinberger*, 475 U.S. at 507 (citation omitted).

[169] See 10 U.S.C. § 774 (1999).

[170] *Employment Division, Department of Human Resources of Oregon v. Smith,* 494 U.S. 872 (1990).

[171] *Id.* at 889.

Lessons Learned. As it plans its biometric applications, the Army can draw several broad lessons from *Goldman*. First, *Goldman* demonstrates that just as the Supreme Court deferred to the Air Force uniform regulation, the federal judiciary will be somewhat deferential to an Army biometric application. Second, the congressional reaction to the *Goldman* decision demonstrates that Congress is not unwilling to require the military to make special allowances for religious objections of members of the military community. Third, the military, as an institution, and the Army, as an armed service, know that they take orders from Congress.

In the context of the Army's use of biometrics, the lesson from *Smith* reinforces a lesson from *Goldman*: While the Army's requirement for participating in biometric applications, just like the Oregon law prohibiting peyote, will be religiously neutral, Congress, like the Oregon state legislature, could grant, if it were so inclined, religious exemptions to the neutral requirement.

The Army, for example, has an extensive, established policy in place to accommodate religious practices.[172] It approves requests for accommodation of religious practices unless the accommodation will have an adverse impact on "military necessity," which consists of unit and individual readiness, unit cohesion, morale, discipline, safety, or health. As the Army's primary advisor on matters pertaining to religious accommodation, the Army Chief of Chaplains is an important institutional asset on whom the Army leadership may call for guidance in determining how religious objections to biometric applications should be handled. As the official charged with establishing the Army's policy on the accommodation of religious practices, the Deputy Chief of Staff for Personnel (DCSPERS) will also play a key role.

INTERNATIONAL LAW CONCERNS

European Union Data Protection Directive

Overview. The European Union Privacy Directive, also known as the EU Data Protection Directive or Directive 96/46/EC, took effect on

[172]See AR 600-20, ¶ 5-6 "Accommodating religious practices," dated July 15, 1999.

October 25, 1998.[173] The directive prohibits the transfer of personal data to any country that does not provide an "adequate" level of protection, as determined by the EU, for the privacy of the data. To ensure compliance with this adequacy requirement, all EU member states were obligated to enact comprehensive privacy legislation, by the effective date of the directive, requiring organizations to implement personal data policies. The United States, however, does not rely on this type of comprehensive legislation to protect privacy, but instead uses a "sectoral approach," relying on a combination of legislation, regulation, and self-regulation. These differing approaches to protecting privacy created uncertainty as to the impact on U.S. organizations of the directive's adequacy requirement.[174]

To address these concerns, the United States and the European Commission agreed in July 2001 on a "safe harbor" framework, under which eligible U.S. organizations can satisfy the "adequacy" requirements of the directive by voluntarily adhering to a set of data protection principles.[175]

Major Provisions. The directive has the potential to be far-reaching. For example, the EU personal data policies provide for the following:

- Transparency: Data must be processed fairly and lawfully.
- Purpose Limitation: Data must be collected and possessed for specified, legitimate purposes and kept no longer than necessary to fulfill the stated purpose.
- Data Quality: Data must be accurate and up-to-date.

---

[173]The official name of the directive is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html. For a comprehensive analysis of the EU Privacy Directive, see Swire and Litan (1998).

[174]See Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce, dated July 21, 2001, available at http://www.export.gov/safeharbor/SHPRINCIPLES FINAL.htm.

[175]See Commission Decision Pursuant to Directive 05/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions, issued by the U.S. Department of Commerce, available at http://europa.eu.int/comm/internal_market/en/media/dataprot/news/decision.pdf.

- Data Transfers: Article 25 of the directive restricts authorized users of personal information from transferring that information to third parties without the permission of the individual providing the data, or data subject. In the case of data transfers across national boundaries, the directive prohibits data transfers outright to any country lacking an "adequate level of protection," as determined by the EU. Article 25 is a major source of U.S. concern.
- Special Protection for Sensitive Data: This provision requires restrictions on, and special government scrutiny of, data collection and processing activities of information identifying "racial or ethnic origin, political opinions, religious or philosophical beliefs, . . . [or] concerning health or sex life." Under the directive, such data collection or processing is generally forbidden outright.
- Government Authority: Each EU member state must create an independent public authority to supervise personal data protection. The EU will oversee the directive's implementation and will engage in EU-level review of its provisions.
- Data Controllers: Organizations processing data must appoint a "data controller" responsible for all data processing, who must register with government authorities.
- Individual Redress: A data subject must have the right to access information about himself, correct or block inaccuracies, and object to information's use.

Article 1 of the directive requires member states to protect the "fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." In essence, the EU has made privacy a fundamental human right.

Applicability to Biometrics. The directive defines personal data as any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity. While the word "biometric" is

not specifically cited in the text, biometric identifiers will likely be implicated by the directive's definition of personal data.

Applicability to the U.S. Army. If a U.S. organization wishes to receive personal data from an EU organization—for example, if the U.S. Army wishes to collect biometric finger images from its employees, including foreign nationals, at a base in Germany—the U.S. organization can comply with the directive in three ways. It can either join the safe harbor, satisfy one of the directive's other exceptions, or seek an adequacy determination (U.S. Department of Commerce, 2001).

If an organization decides to participate in the safe harbor, it must comply with the safe harbor requirements, which are set forth in a set of seven privacy principles, and it must publicly declare its adherence to these principles. This "self-certification" of compliance must be made annually to the U.S. Department of Commerce, which will maintain a regularly updated list of safe harbor participants through its Web site.[176] With regard to enforcement, organizations must have in place compliance verification procedures, as well as dispute-resolution mechanisms to resolve complaints about compliance. Further enforcement is provided for under U.S. federal or state law governing unfair and deceptive acts (U.S. Department of Commerce, 2001).

Accordingly, to be eligible to join the safe harbor, a U.S. organization must be subject to the jurisdiction of specified government bodies in the United States.[177] The Federal Trade Commission and the Department of Transportation are the only two such government bodies specified in the safe harbor agreement. As such, the U.S. Army would seem to be ineligible to join the safe harbor at this time, although the safe harbor agreement makes provision for its "review

---

[176]For the seven privacy principles, as well as the guidance for the implementation of these principles contained in the Frequently Asked Questions, see U.S. Department of Commerce (2001).

[177]See Article 1(2)(b) of Commission Decision Pursuant to Directive 05/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions, issued by the U.S. Department of Commerce, available at http://europa.eu.int/comm/internal_market/en/media/dataprot/news/decision.pdf.

in light of experience," such that the number of those organizations eligible to join the safe harbor may expand in the future.[178]

Even if the Army cannot avail itself of the safe harbor route to compliance with the directive, it appears very likely that the Army's use of biometrics will fit within one of the several exceptions and exemptions contained in the directive. Prominent among them, Article 3(2) of the directive contains an exception for public security and defense matters. It is not clear, however, whether this exception would be interpreted to apply narrowly—to only militaries of the EU member states or broadly—to the U.S. military operating in EU member states.[179] Peter P. Swire, formerly the U.S. government's Chief Counselor for Privacy, and co-author, Robert E. Litan, have contended in their study of the directive that the public security and defense exception would apply to the U.S. military operating in EU member states. Also, they believe a strong argument can be made that Article 25's "adequacy" requirement would be satisfied because the Privacy Act protects the privacy interests of U.S. nationals in the U.S. military and the federal government.

Thus, the EU would determine that the Privacy Act provides an "adequate level of protection." However, as Swire and Litan point out, the Privacy Act does not extend to foreign nationals. "Difficulties could arise, therefore, with records kept by the U.S. government about employees or other persons who are foreign nationals, such as when their employment or medical records are trans-

---

[178]See Paragraph (9) of Commission Decision Pursuant to Directive 05/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions, issued by the U.S. Department of Commerce, available at http://europa.eu.int/comm/internal_market/en/media/dataprot/news/decision.pdf.

[179]Article 3(2) of the directive reads in pertinent part:

> This Directive shall not apply to the processing of personal data: in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

See *Directive*, available at http://www2.echo.lu/legal/en/dataprot/directiv/chap1.html#HD_NM_29.

ferred back to Washington" (Swire and Litan, 1998, p. 129). At any rate Swire and Litan do not believe the EU Commission will want to target the U.S. government for an early enforcement action because of the special diplomatic and legal problems such an action would raise (Swire and Litan, 1998, p. 129).

The directive's other exemptions may come into play. For example, Article 13(1) permits EU states to adopt legislative measures to restrict the scope of certain of the directive's obligations and rights, provided the restriction constitutes a necessary measure to safeguard national security, defense, and public security, among others.[180]

Moreover, Article 26(1) provides for derogation, or the partial revocation of a law, from Article 25. Specifically, EU member states "shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that: . . . (d) the transfer is necessary or legally required on important public interest grounds."[181]

In principle, it may be argued that the exemptions provided for in Article 13 and 26(1) refer to national security reasons of the EU member states only, not the national security reasons of a foreign country, such as the United States. Nevertheless, the plain language of the Article 13(b) exception is "defence." Hence, a broad interpretation of defense cannot be ruled out. Similarly, Article 26(1)(d) establishes a derogation on the condition that "the transfer is necessary or legally required on important public interest grounds." Arguably, the U.S. Army's presence in EU member states serves an important public interest. Unfortunately, there is not much official guidance or scholarly work on the eventual application of the national security exception to this or similar cases.

Most important, many international agreements are in force between the United States and EU member states where the United

---

[180]Obligations and rights provided for in Articles 6(1), 10, 11(1), 12, and 21 of the directive may be restricted. See *Article 13(1) of the Directive*, available at http://www2.echo.lu/legal/en/dataprot/directiv/chap2.html#HD_NM_34.

[181]See *Article 26(1)(d) of the Directive*, available at http://www2.echo.lu/legal/en/dataprot/directiv/chap4.html

States has a military presence. These agreements, some of them classified, would pertain to the original grants of rights for the U.S. military presence in the host nation.[182] NATO multilateral agreements are also in force. These international agreements may contain provisions for derogation of some or all of the directive's obligations for the U.S. Army as a data controller. In case they do contain such provisions, the case law of the European Court of Justice should be reviewed to assess the impact of these international agreements of the EU member states with regard to EU Community Law.

Although the directive and its implementation are too recent to allow full evaluation of the precise impact the directive will have on Army biometric applications, on balance it appears likely that Army biometric applications will qualify for exemption from the directive's requirements. Also, to the extent that some U.S. Army bases are considered "joint" bases between the United States and the host nation EU member state, or to the extent these U.S. Army bases serve the defense of the EU member state by virtue of the international agreements to which they subscribed (e.g., mainly NATO), it is reasonable to think that EU member states could eventually authorize at least some of the exceptions provided for in the directive either with regard to the processing of personal data within the U.S. bases or the transfer of human resources data to the United States.

It should be noted, however, that the extent and scope of the exemptions and restrictions provided for in the directive are matters within the competence of the individual member states. Consequently, the precise interpretation of the exemptions could differ from one member state to another.

The final means for compliance with the directive—seeking an adequacy determination from the EU—is likely not a viable option given the political sensitivities involved. In any event, based on the discussion above, the Army will likely have no need to resort to this option.

Although the application of the EU Data Protection Directive to U.S. Army biometric applications appears complicated and confusing, the Army should bear in mind that it has experienced institutional assets

[182]For example, the bilateral agreement with Italy is classified.

on whom it may call, including Army Judge Advocate General and DoD OGC as well as EUCOM (European Command), USAREUR (United States Army, Europe), SHAPE (Supreme Headquarters Allied Powers Europe (NATO)) and the U.S. Department of State, who have dealt with similar issues in the past. Moreover, regardless of what the Army does with biometric applications and where it does it, the directive's applicability to the U.S. Army operating in EU member nations will eventually have to be decided because the Army is a huge collector of personal data in Europe and the directive defines personal data broadly and levies many requirements on the data collector.

Other International Law Concerns

As explained in the EU subsection above, when the Army operates in an overseas environment, there are some situations in which it is desirable for the Army to comply with foreign laws and some situations in which it is not desirable to do so. For example, the Italian government recently tried to require the U.S. military in Italy to accept Italian occupational safety and health laws. Other host nations attempt to force the U.S. military to accept their labor or environmental laws.

Just as with EU member states, the United States has entered into many bilateral agreements with other host nations where it has a military presence. For example, the United States and Japan have many such bilateral agreements (U.S. Forces Japan, 2000). These bilateral agreements can provide guidance for the Army as it plans biometric applications oversees. For example, many of these agreements give the Army great discretion in force protection and operational matters.[183] Again, once it determines exactly what type of biometric application it wants to require in an overseas location, the Army needs to look for specific legal guidance from its institutional assets to determine how it should proceed.

---

[183]See, e.g., Article III, Section 1, of the Agreed Minute to the Treaty of Mutual Cooperation and Security, dated January 19, 1960, providing that "[w]ithin the facilities and areas [Japan has permitted the United States to use], the United States may take *all the measures necessary for their establishment, operation, safeguarding and control*" (emphasis added), available at http://www.yokota.af.mil/usfj/Treaty2.htm.

CONCLUSION

This review has attempted to address legal concerns raised by Army use of biometrics. While not discussing every conceivable legal objection, this review was intended to provide the Army leadership with a useful starting point for legal analysis as it embarks on biometric applications. This review has also explained that while Army biometric applications raise legal concerns, these concerns about a new technology can be accommodated by the Army's and DoD's many institutional assets responsible for privacy issues. From the legal perspective, Army use of biometrics gets a tentative "Good to Go" for U.S.-based applications, provided it follows the statutory, administrative, and constitutional requirements discussed in this review.

In the international setting, the Army needs to be aware of the requirements of the EU Data Protection Directive and its impact on the U.S. government. Although the Army's use of biometrics will likely comply with the directive through one of the directive's exceptions, the Army must pay close attention to the way these exceptions are interpreted to avoid any difficulties. Moreover, any U.S. Army biometric application operating in a foreign nation must be examined from the international law perspective with the relevant bilateral agreements authorizing the U.S. Army's presence in the foreign nation as a starting point.

Before implementing any biometric application, the Army must undertake a thorough legal analysis of exactly what it wants to do and where it wants to do it. In this way, the Army will be much less likely to run afoul of the Privacy Act and similar statutory and administrative requirements, as well as the Constitution.