Journal of Air Law and Commerce

Volume 69 | Issue 2 Article 9

2004

Back to the Future - The Use of Biometrics, Its Impact of Airport Security, and How This Technology Should Be Governed

Eric P. Haas

BACK TO THE FUTURE? THE USE OF BIOMETRICS, ITS IMPACT ON AIRPORT SECURITY, AND HOW THIS TECHNOLOGY SHOULD BE GOVERNED

ERIC P. HAAS*

THE UNITED STATES government is continually developing and exploring better, more reliable methods of securing this nation's airports in an effort to stay one step ahead of terrorists in the "war on terror." Since September 11, 2001, the federal government has established the Department of Homeland Security (DHS) and, within it, the Transportation Security Administration (TSA), which is responsible for passenger security at the nation's many airports. Commercial pilots are now able to carry handguns, and federal air marshals are standard on many domestic flights. Critics argue, however, that more security may still be needed. Recent developments include the implementation of United States Visitor and Immigrant Status Indicator Technology (US-VISIT) and Computer Assisted Passenger Pre-Screening (CAPPS II). Because terrorists are likely to become familiar with static security procedures over time, the government must continually respond by introducing newer, more advanced technologies. Recently the use of biometrics for identification and security has emerged as a promising new instrument in the "war on terror."

Most people are familiar with biometric technology from what they have observed in science-fiction movies. The most recent film to showcase the possibilities of biometric technology was Minority Report.[1] In the movie, people are continually subjected to eye scans so that computers are able to identify each person and then interact with the individual for purposes of targeted advertising, security clearance, and even law enforcement. In this futuristic movie environment, mandatory identification is

* The author is a J.D. candidate at Southern Methodist University. He is the recipient of the Wayne Vines Memorial Scholarship for Aviation Safety.

[1] MINORITY REPORT (Twentieth Century Fox 2002).

the norm, and it is impossible for anyone to live in anonymity. However, for better or worse, the technologies of tomorrow are here today, and biometric identification systems are already being implemented in airports and other high-profile locales. Following the establishment of the TSA, Congress authorized the agency to "[p]rovide for the use of . . . biometric[s], or other technologies to prevent a person who might pose a danger to air safety or security from boarding [an] aircraft."[2] Although biometrics and other new technologies show great promise in creating a more secure community, the newfound security may be obtained at the price of an individual's right to privacy and right to travel.

This paper will address whether biometric technology can effectively protect this nation's airports and borders while still preserving fundamental constitutional rights. In order to evaluate the constitutional use of biometric technology, this paper will begin with a survey of the case law surrounding the right to privacy, the right to travel, and airport screening procedures.[3] Part II will give an overview of biometrics and the most popular biometric identifiers. Part III will address current uses of biometrics and how the government plans to implement this technology in the near future. Finally, Part IV will advocate a test which the Supreme Court should adopt in future decisions concerning airport searches and how the test squares the competing interests of safety and privacy in the application of biometric technology.

I. CONSTITUTIONAL IMPLICATIONS OF AIRPORT SCREENING

A. The Right to Privacy—A Theoretical Split

The right to privacy is not expressly set forth in the Constitution; however, courts have generally held the Fourth Amendment to implicitly protect this fundamental individual right. The Fourth Amendment guarantees "the right of the people to be secure in their persons . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and

---

[2] 49 U.S.C. § 114 (a)(7) (2004).

[3] For purposes of this paper, "airport searches" and "airport screening procedures" will be used interchangeably to refer to standard airport security measures that apply to commercial airline passengers traveling within the United States (e.g. metal detectors and luggage x-rays).

particularly describing the place to be searched and the persons or things to be seized."[4] For purposes of analysis, the Fourth Amendment can be divided into the Search and Seizure Clause and the Warrant Clause. Over the years, the Supreme Court has given substance to the guarantees enunciated in the Fourth Amendment and carved out various exceptions through decisions that have defined the limitations of this constitutional assurance. An overview of these decisions will help in defining the right to privacy that exists today.[5]

The Supreme Court's opinion in *Katz v. United States*[6] is the watershed case for modern Fourth Amendment jurisprudence. *Katz* marked a departure from the traditional view of privacy rights that had previously defined privacy in terms of common law trespass. Justice Harlan's now famous concurrence developed a two-part test for determining occasions in which a right to privacy should be recognized. According to Justice Harlan's test, an individual must have (1) a subjective expectation of privacy and (2) society must be willing to recognize the individual's expectation as reasonable.[7] This test is the threshold question that must be addressed before engaging in any further Fourth Amendment analysis, since if there is no expectation of privacy, then there has not been an occasion to violate that right.[8]

Assuming that the Fourth Amendment is properly implicated, a search performed without a warrant is per se unconstitutional, unless the search falls within a narrowly crafted exception.[9] Exceptions to the per se rule, while rarely made, include the administrative search doctrine,[10] the *Terry* rule,[11] and consent.[12] As this brief discussion of Fourth Amendment case law will demonstrate, courts have thus far been willing to uphold warrantless airport searches as constitutional; however, the reasons

---

4 U.S. CONST. amend. IV.

5 *See* United States v. Edwards, 498 F.2d 496, 503 n.2 (2d Cir. 1974) (Oakes, J., concurring) ("The entire content of the concept of a Right to Privacy, while it has many fourth amendment antecedents, is basically a product of the 20th Century.").

6 389 U.S. 347 (1967).

7 *Id.* at 361 (Harlan, J., concurring).

8 United States v. Davis, 482 F.2d 893, 904-905 (9th Cir. 1973).

9 *Katz*, 389 U.S. at 357; *see also* Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

10 New York v. Burger, 482 U.S. 691 (1987).

11 *See* United States v. Albarado, 495 F.2d 799 (2d Cir. 1974); United States v. Epperson, 454 F.2d 769 (4th Cir. 1972).

12 *See* United States v. Henry, 615 F.2d 1223 (9th Cir. 1980).

justifying their decisions have varied greatly.[13] The result of this jumbled case law is a theoretical circuit split regarding the basis for justifying an airport search within the scrutiny of the Fourth Amendment.[14] The question is whether the different justifications that upheld airport searches in the past are still applicable to present-day airport procedures, which may involve more technologically-sophisticated techniques, such as the use of biometrics.

Airport screenings are commonplace today and are almost always conducted without a warrant. As such, a proper analysis must focus on the exceptions to the per se rule that justify warrantless airport searches. The administrative-search doctrine emphasizes the distinction made between searches which are authorized by penal statute and searches that arise as a means of agency adjudication.[15] An administrative search, which may be contrasted with a *Terry* "stop and frisk" search,[16] does not require that the search be supported by a specific showing of probable cause.[17] For instance, in *New York v. Burger*, the Supreme Court upheld a statute which authorized warrantless searches under the auspices of an administrative regulatory system.[18] The administrative-search exception holds that there is a reduced expectation of privacy for individuals who operate in "closely regulated" industries.[19] The exception applies to closely regulated industries because (1) the government has a more compelling interest to search those industries that are closely regulated, and (2) by choosing to operate within the regulatory arena such individuals are on notice of the governmental oversight.[20] However, even the abridgement of privacy rights that accompanies an administrative inspection must meet certain minimum requirements.[21] As the Court noted, "[f]irst, there must be a 'substantial' government interest that informs the reg-

---

[13] *See* United States v. Hartwell, 296 F. Supp. 2d 596 (E.D. Pa. 2003).

[14] The circuit split is theoretical and not factual, because virtually all cases addressing airport searches have upheld them as constitutional. The difference between the decisions is the legal basis that justifies the result in each case. *Compare* United States v. Davis, 482 F.2d 893 (9th Cir. 1973) *with* United States v. Epperson, 454 F.2d 769 (4th Cir. 1972).

[15] *Davis*, 482 F.2d at 908.

[16] *See* Terry v. Ohio, 392 U.S. 1 (1968).

[17] *Davis*, 482 F.2d at 908.

[18] 482 U.S. 691 (1987).

[19] *Id.* at 701.

[20] *Id.* at 701-02.

[21] *Id.* at 702.

ulatory scheme pursuant to which the inspection is made."[22] "Second, the warrantless inspections must be 'necessary to further the regulatory scheme.'"[23] And "[f]inally, 'the statute's inspection program, in terms of certainty and regularity of its application, [must] provid[e] a constitutionally adequate substitute for a warrant."[24]

In addition to the regulatory requirements for conducting an administrative search, the search must be carried out within the confines of *reasonableness*.[25] Reasonableness may be defined as a compelling governmental interest that overshadows a conflicting intrusion of privacy. In *Skinner v. Railway Labor Executives' Ass'n*, the Supreme Court sustained random drug and alcohol tests performed on railway employees, even though the tests were deemed to be searches performed without a warrant.[26] According to the Court, "[i]n limited circumstances, where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion, a search may be reasonable despite the absence of such suspicion."[27] The Court was referring to the compelling governmental interest of "safety in rail transportation."[28] In reaching this result, the Court held that the reasonableness test of the Fourth Amendment requires a balancing of individual interests with governmental interests.[29] Justice Kennedy also observed that employees typically consent to significant restrictions on movement and privacy in the workplace; and in certain situations, dispensing with the warrant requirement is persuasive when obtaining a warrant will thwart the objective of the search.[30]

Following *Skinner*, a compelling governmental interest may render the warrant requirement unnecessary by characterizing the intrusion as a reasonable administrative search, but the question becomes, what qualifies as a compelling interest. In the context of airport security, the Fourth Circuit has addressed

---

22 *Id.*

23 *Id.*

24 *Id.* at 703.

25 United States v. Davis, 482 F.2d 893, 910 (9th Cir. 1973) (emphasis added).

26 489 U.S. 602, 633 (1989).

27 *Id.* at 624.

28 *Id.* at 631.

29 *Id.* at 619.

30 *Id.* at 623-26.

the issue. In *United States v. Epperson*,[31] the Fourth Circuit applied the search and seizure requirements of the Fourth Amendment to the use of a magnetometer at an airport.[32] The defendant, while attempting to board an airplane, was found carrying a loaded pistol after passing through a magnetometer.[33] The defendant argued that the pistol was the fruit of an unreasonable search conducted without a warrant.[34] While the Fourth Circuit agreed that the use of the device did constitute a search, the court held that the use of the magnetometer in this case was justified.[35] In reaching this result, the court took notice that "air piracy and its threat to national air commerce is known to all."[36] Thus, "[t]he danger is so well known, the governmental interest so overwhelming, and the invasion of privacy so minimal, that the warrant requirement is excused by exigent national circumstances."[37] Along the same lines, the Supreme Court has stated, "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation."[38]

While the presence of a compelling governmental interest is one way of justifying an administrative search, other courts have defined reasonableness in more general terms without expressly elevating the need to the status of a compelling governmental interest.[39] In *United States v. Edwards*, the Fifth Circuit determined the reasonableness of an administrative airport search by "balancing the need for a search against the offensiveness of the intrusion."[40] The court determined that "[w]hen the risk is the jeopardy to hundreds of human lives . . . inherent in the pirating or blowing up of a large airplane, the *danger alone* meets the test of reasonableness, so long as the search is conducted in good faith . . . and with reasonable scope and the passenger has been given advance notice."[41] The effect of this test places a heavy burden on an individual to overcome a showing that na-

---

[31] Magnetometer is the technical term for a metal detector.

[32] 454 F.2d 769 (4th Cir. 1972).

[33] *Id.* at 770.

[34] *Id.*

[35] *Id.* at 772.

[36] *Id.* at 771.

[37] *Id.*

[38] Haig v. Agee, 453 U.S. 280, 307 (1981) (citing Aptheker v. Sec'y of State, 378 U.S. 500, 509 (1964)).

[39] United States v. Edwards, 498 F.2d 496, 498 (5th Cir. 1974).

[40] *Id.* at 500.

[41] *Id.* (emphasis added).

tional security is at stake. In response, at least one judge has expressed concern of possible governmental overreaching in the test's practical application. Their concern is that individual civil liberties may be thwarted by an all inclusive "danger" test of reasonableness, limited only by a condition of "good faith."[42]

The Ninth Circuit was the first court to expressly hold that the administrative search doctrine governed airport boarding procedures. In *United States v. Davis*,[43] the court concluded that a preboarding screening satisfied the test of reasonableness. The court weighed the need to prevent hijackings against a narrowly tailored search for weapons and explosives.[44] In addition to the requirement that the search be properly limited in scope was the additional caveat that the individual must be free to avoid the search altogether by choosing not to board the airplane.[45] This element ensures that the intrusiveness of the search is limited only to individuals intending to board the plane and thus is consistent with the administrative need to conduct the search.[46]

Following the decision in *Davis*, the Ninth Circuit reaffirmed the administrative-search doctrine.[47] The court recognized that reasonableness still remained the critical question regarding the constitutionality of the administrative search.[48] Under the test of reasonableness, the court held that the compelling governmental interest in preventing air piracy justifies the limited privacy intrusion required to satisfy the administrative need.[49] By endorsing the administrative exception, the court expressly rejected the application of *Terry v. Ohio* in the context of airport searches.[50] Lastly, in addressing criticism that the exception was too broad, the court determined that unrestrained governmental abuse would be curtailed by a self-limiting principle inherent in an administrative search.[51] The principle was that "[s]o long as the government officials conducting the searches pursue a single-minded objective . . . searches will . . . be no more intru-

---

[42] *See, e.g.*, United States v. Bell, 464 F.2d 667, 675-76 (2d Cir. 1974) (Manfield, J. concurring).

[43] United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973).

[44] *Id.* at 910.

[45] *Id.* at 910-911.

[46] *Id.*

[47] United States v. $124,570 U.S. Currency, 873 F.2d 1240 (9th Cir. 1989).

[48] *Id.* at 1243.

[49] *Id.*

[50] *Id.* at 1247.

[51] *Id.* at 1245.

sive than is necessary to achieve air safety."[52] However, even with the administrative exception and its self-imposed limitations, the court was careful to point out that it would not rubberstamp any airport search in the name of safety and that it was the courts' responsibility to remain vigilant against governmental overreaching.[53]

In contrast to the administrative-search exception, a separate line of cases have justified warrantlessairport searches on the basis of the Supreme Court's decision in *Terry v. Ohio.*[54] Beginning with *United States v. Epperson,*[55] some circuits have evaluated airport searches under the auspices of reasonable suspicion and probable cause. In *Epperson,* the Fourth Circuit held that an airport search does not fall into any "recognized exceptions to the warrant requirement of the Fourth Amendment except that suggested by *Terry v. Ohio.*"[56] According to the court, "[t]he rationale of *Terry* is not limited to protection of the investigating officer, but extends to others in danger."[57] "The warrant procedure is designed to guarantee that a decision to search . . . is justified by a reasonable governmental interest. But reasonableness is still the ultimate standard."[58] In determining what is reasonable under the *Terry* standard, the court balanced "the governmental interest in searching against the invasion of privacy which the search entails. These interests must be balanced at two stages: the search must be 'justified at its inception' and 'reasonably related in scope to the circumstances which justified the interference in the first place.'"[59] Much as other courts have taken notice of the threat to national security that air piracy creates, the court in *Epperson* recognized that "the warrant requirement is excused by exigent national circumstances."[60] The court went on to say

> [I]t is clear to us that to innocent passengers the use of a magnetometer to detect metal on those boarding an aircraft is not a resented intrusion on privacy, but, instead a welcome reassur-

---

[52] *Id.*

[53] *Id.* at 1243-1244.

[54] 392 U.S. 1 (1968).

[55] 454 F.2d 769 (4th Cir. 1972).

[56] *Id.* at 770.

[57] *Id.* at 772 (quoting Terry v. Ohio, 392 U.S. 1, 30 (1968)) (internal quotation marks and punctuation omitted).

[58] *Id.* at 771 (quoting Camara v. Mun. Court, 387 U.S. 523, 539 (1966) (internal quotation marks omitted)).

[59] *Id.* (citing Terry v. Ohio, 392 U.S. 1, 20 (1968)).

[60] *Id.*

> ance of safety. Such a search is more than reasonable; it is a compelling necessity to protect essential air commerce and the lives of passengers.[61]

Following *Epperson* and along the same lines, the Second Circuit in *United States v. Bell* applied the *Terry* rationale to a challenged airport search.[62] For the majority, it was important that, prior to the search, the defendant had met the profile of a suspected terrorist and had alerted the magnetometer.[63] In addition, the defendant had admitted being a prior criminal.[64] All these facts led the court to hold that the officer, who was experienced in screening suspected terrorists, had conducted the search within the proscriptions of *Terry*.[65]

While the majority opinion in *Bell* based its decision on the foundations of *Terry*, the other panel judges submitted separate opinions which addressed concerns and expressed doubt over the legitimacy of expanding the limits of warrantless airport searches. In concurrence, Judge Friendly proposed his "danger alone" test for reasonableness that would later be adopted by the Fifth Circuit in *United States v. Edwards*.[66] Judge Friendly stated that he would have no problem sustaining a search based on nothing more than the intuition of an officer or airline agent.[67] In response to Judge Friendly's extensive dicta, Judge Mansfield, in concurrence, stated that the threat of airplane hijacking does not justify "a broad and intensive search of all passengers."[68] Although he joined the court in condoning this search based upon its facts, Judge Mansfield cautioned that "[n]o necessity exists for punching a hole in the Fourth Amendment in order to enable the FAA[69] and airline authorities to deal effectively with the air piracy problem."[70]

---

[61] *Id.* at 772.

[62] 464 F.2d 667 (2d Cir. 1972); *cf.*, United States v. Albarado, 495 F.2d 799 (2d Cir. 1974).

[63] *Bell*, 464 F.2d at 673.

[64] *Id.*

[65] *Id.*

[66] *Id.* at 675 (Friendly, J. concurring); *see supra* notes 39-41 and accompanying text.

[67] *Id.*, at 675 (Friendly, J., concurring).

[68] *Id.* (Mansfield, J., concurring).

[69] Before the establishment of the Transportation Security Administration (TSA), the Federal Aviation Administration (FAA) was responsible for ensuring adequate airport security measures.

[70] *Bell*, 464 F.2d at 675 (Mansfield, J., concurring).

Other circuits have implicitly adopted the *Terry* rationale and have upheld the constitutionality of airport searches based on the proposition that the Fourth Amendment only proscribes *unreasonable* searches and seizures; and therefore, searches that are reasonable are constitutional.[71] In *United States v. Skipwith*, the Fifth Circuit supported this interpretation of the Fourth Amendment by reasoning that airport searches are analogous to border searches.[72] Under this rationale, the court applies a less restrictive test of probable cause to account for other factors which are germane to a border search.[73] However, in applying the border search test of reasonableness, the court in *Skipwith* added an additional step and considered the effectiveness of the proposed search in light of the governmental need and privacy intrusion.[74] In dissent, Judge Aldrich favored a more narrow rule that would be more consistent with the limitations of *Terry*.[75] In furtherance of this goal, Judge Aldrich proposed that the court adopt the same standard enunciated by the Supreme Court in *Mapp v. Ohio*,[76] excluding property unlawfully seized in order to "temper possibly overzealous airport searches."[77]

Following *Bell* and *Skipwith*, the Second Circuit held a search to be unreasonable under a more restrictive standard.[78] In rejecting Judge Friendly's view of reasonableness, the court reaffirmed the *Terry* rationale as controlling law in the evaluation of warrantless airport searches.[79] In so ruling, the court held that the search was unreasonable because it was "not as limited in its intrusiveness as it might have been."[80] The approach in *Albarado* of narrowly tailoring a search to meet the scope of the need was a corollary of the Supreme Court's decision in *Terry*.[81] In adopt-

---

[71] *See, e.g.*, United States v. Skipwith, 482 F.2d 1272 (5th Cir. 1973); United States v. Slocum, 464 F.2d 1180, 1182 (3d Cir. 1972) (adopting the Fourth Circuit's analysis in United States v. Epperson, 454 F.2d 769, 771 (4th Cir. 1972)).

[72] *See Skipwith*, 482 F.2d at 1276 (holding that "standards for initiating a search of a person at the boarding gate should be no more stringent than those applied in border crossing situations").

[73] *See* United States v. McDaniel, 463 F.2d 129, 132 (5th Cir. 1972).

[74] *Skipwith*, 482 F.2d at 1275-1276.

[75] *Id.* at 1280-1281 (Aldrich, J., dissenting).

[76] 367 U.S. 643, 657-59 (1961).

[77] *Skipwith*, 482 F.2d at 1281 (Aldrich, J., dissenting).

[78] United States v. Albarado, 495 F.2d 799, 810 (2d Cir. 1974).

[79] *Id.*

[80] *Id.* at 809.

[81] *See* Terry v. Ohio, 362 U.S. 1, 19 (1968) (stating that "[t]he scope of the search must be strictly tied to and justified by the circumstances which rendered its initiation permissible").

ing the *Terry* standard, the court expressly rejected the contention that the search might be upheld on the basis of consent.[82] In dicta, the court reasoned that making a person choose between either flying or not submitting to a search is tantamount to coercion because the possibility of finding some other mode of travel would be unreasonable and unrealistic.[83]

Although only dicta, the words of the Second Circuit regarding consent are contrary to an entire line of cases that have upheld implied consent to justify Fourth Amendment challenges to warrantless airport searches. The consent justification traces its doctrinal roots to the Supreme Court's opinion in *Florida v. Bostick*, where the Court held that random searches are not per se unconstitutional if they are made with an individual's consent.[84] In *Bostick*, the Court elaborated on its precedent laid down in *United States v. Mendenhall*,[85] which permitted law enforcement officers to conduct consensual searches at airports. Justice O'Connor, writing for the majority, rejected the application of a per se rule, and held that, considering the totality of the circumstances, an illegal seizure does not take place so long as an individual is "free to decline [an] officer's request or otherwise terminate the encounter."[86]

The determination of what qualifies as consent and whether consent can be implied in the context of an airport search is still a contested issue. In *United States v. Davis*, the Ninth Circuit rejected the assertion that *Terry* controlled the validity of airport searches and held that a passenger may implicity consent to a search by choosing to board a commercial airplane.[87] According to the court, extending *Terry* "to authorize airport screening searches would result in intrusions upon privacy unwarranted by the need."[88] While mentioning its plausible application in the case, the court did not elaborate any further on the issue of consent and instead chose to remand the case to the district court for comprehensive consideration of the issue.[89]

After *Davis* it was apparent that the Ninth Circuit would be willing to justify an airport search based on implied consent. Ac-

---

[82] *Albarado*, 495 F.2d at 806.
[83] *Id.* at 806-07.
[84] 501 U.S. 429 (1991).
[85] 446 U.S. 544 (1980).
[86] *Bostick*, 501 U.S. at 436-440.
[87] 482 F.2d 893, 905-13 (9th Cir. 1973).
[88] *Id.* at 907.
[89] *Id.* at 915.

cordingly, in *United States v. Pulido-Baquerizo*[90] the court held that "passengers placing luggage on an x-ray machine's conveyor belt for airplane travel . . . impliedly consent to visual inspection and limited hand search of their luggage."[91] In so holding, the court acknowledged that its decision was in line with other circuits that had upheld airport searches challenged under a theory of implied consent.[92]

In *United States v. Henry*, the Ninth Circuit re-addressed the theory of implied consent in the context of an airport checkpoint search, and again the court held that a warrantless search was not unconstitutional since the individual had impliedly consented to the search by attempting to board the plane.[93] In arriving at its decision, the court took notice of the fact that the public is well informed about airport security procedures, and in this case, there were even signs that informed passengers that they could refuse to be searched.[94] However, notice is only one part of the equation; the consent must be "freely and voluntarily given" and such a determination must be made "on the basis of the totality of the circumstances."[95] According to the court, "the crucial factor is whether [the suspect] could have freely withdrawn the briefcase and avoided the search."[96]

While the Ninth Circuit initially embraced the implied consent argument in initial challenges to the constitutionality of airport searches,[97] the court has since changed its justification to the administrative-search exception to validate warrantless airport searches.[98] As a result, the continued feasibility of the implied consent rationale in this context has been brought into question. According to the court, while passengers may still be seen to impliedly consent to a search that is limited in scope to

---

[90] 800 F.2d 899 (9th Cir. 1986).

[91] *Id.* at 901.

[92] *Id.* at 902; *see, e.g.*, United States v. Herzbrun, 723 F.2d 773, 776 (11th Cir. 1984); United States v. Wehrli, 637 F.2d 408, 409-410 (5th Cir. 1981); United States v. DeAngelo, 584 F.2d 46, 47-48 (4th Cir. 1978); United States v. Williams, 516 F.2d 11, 12 (2d Cir. 1975).

[93] 615 F.2d 1223, 1231 (9th Cir. 1980).

[94] *Id.* at 1228-1229 (noting that anyone refusing to give consent to be searched would not be permitted to board the airplane).

[95] *Id.* at 1230.

[96] *Id.*

[97] *See, e.g.*, United States v. Davis, 482 F.2d 893 (9th Cir. 1973); United States v. Henry, 615 F.2d 1223 (9th Cir. 1980); United States v. Pulido-Baquerizo, 800 F.2d 899 (9th Cir. 1986).

[98] United States v. $124,570 U.S. Currency, 873 F.2d 1240, 1247 (9th Cir. 1989).

weapons and explosives, they "would be surprised to learn that they are also submitting to a more generalized search for . . . things that are not in themselves illegal but merely look suspicious."[99] In dicta, the court went on to suggest that "[i]ndeed, we doubt that the government could extract so broad a consent as a condition for boarding an airplane."[100] While notice may be antecedent to a finding of implied consent, "the government cannot 'avoid the restrictions of the Fourth Amendment by notifying the public that all telephone lines would be tapped or that all homes would be searched.'"[101]

The most recent case addressing the constitutionality of a warrantless airport search is *United States v. Hartwell.*[102] The court in *Hartwell* acknowledged the divergence of opinion surrounding airport searches and determined that the implied consent rationale was still a viable justification.[103] While previous decisions have discussed the right of a passenger to choose not to fly and thereby avoid a potential search,[104] the court in *Hartwell* held that once an individual has triggered an alarm, the option of avoiding a subsequent search by choosing not to fly is no longer present.[105] To hold otherwise would give potential terrorists the equivalent of a get-out-of-jail-free card.[106]

So far, the Supreme Court has declined to address the issue of the proper analysis to adjudicate the validity of a warrantless airport search. Nevertheless, the Court has provided guidance regarding the limits of the Fourth Amendment and technological innovation. The most recent interpretation was the Court's opinion in *Kyllo v. United States.*[107] While, as previously discussed, a warrantless search is presumptively unconstitutional, determining what amounts to a search has been a more difficult question.[108] In *Kyllo,* the Court held that the use of a thermal imaging device for determining the amount of heat within an individual's home was an unreasonable search.[109] In reaching this result, the Court distinguished its holding in *Dow Chemical*

---

99 *Id.*

100 *Id.*

101 *Id.* (quoting 4 W. LAFAVE, SEARCH AND SEIZURE § 10.6(g) (2d ed. 1987)).

102 296 F. Supp. 2d 596 (E.D. Pa. 2003).

103 *Id.*

104 *See Davis,* 482 F.2d at 910-911.

105 *Hartwell,* 296 F. Supp. 2d at 605-606.

106 United States v. Herzbrun, 723 F.2d 773, 776 (11th Cir. 1984).

107 533 U.S. 27 (2001).

108 *Id.* at 31.

109 *Id.* at 40.

Co. v. United States, which had previously allowed the use of enhanced aerial photography of an industrial complex.[110] The level of technology employed in *Dow Chemical* appeared to be very similar in *Kyllo*, but as the Court explained, *Dow Chemical* was "not an area immediately adjacent to a private home, where privacy expectations are most heightened."[111] The conclusion to be drawn from *Kyllo* is that the Court is more concerned with where a search takes place than the type or sophistication of technology used in facilitating the search.

B. The Right to Travel—A Different Side of the Same Coin

Although the Fourth Amendment Search and Seizure Clause is frequently evaluated in order to determine the reasonableness of security measures, the Fifth Amendment Due Process Clause, which preserves an individual's right to travel, should also be factored into any Constitutional evaluation concerning security proposals. The Supreme Court recognized the right to travel in *Kent v. Dulles*.[112] The Court held that the right to travel is found in the Due Process Clause of the Fifth Amendment, and therefore, the Secretary of State may not abridge that right by refusing to issue a United States passport on the mere suspicion that the applicant is a communist.[113] While the decision in *Kent* was concerned with the right to travel internationally, in subsequent decisions, the Court has held that the "[c]onstitutional right to interstate travel is virtually unqualified."[114] Unlike the right to privacy, however, the right to travel is more ambiguous. The right to travel has been enunciated in numerous Supreme Court opinions, and its origins have been found in no less than ten separate places in the Constitution.[115]

---

[110] 476 U.S. 227, 239 (1986); *see also* California v. Ciraolo, 476 U.S. 207 (1986) (upholding a warrantless search of a backyard by means of aerial surveillance).

[111] *Dow Chemical*, 476 U.S. at 237 n.4.

[112] 357 U.S. 116, 125 (1958).

[113] *Id.* at 125-127.

[114] Haig v. Agee, 453 U.S. 280, 307 (1981).

[115] *See* Christopher S. Maynard, Note, *Nine-Headed Caesar: The Supreme Court's Thumbs-Up Approach to the Right to Travel*, 51 Case W. Res. L. Rev. 297, 314 (2000) (reporting that the right to travel has been found in "the Commerce Clause, the Comity Clause, the First Amendment, the Due Process Clause of the Fifth Amendment, the Ninth Amendment, Implied Fundamental Rights, and the Citizenship, Privileges or Immunities, Equal Protection and Due Process Clauses of the Fourteenth Amendment").

One theory asserts that airport searches implicitly limit an individual's right to travel by imposing invasive mandatory searches under the guise of implied consent or the administrative search exception. In response, proponents of the more rigorous security measures are quick to point out that individuals concerned about the invasion of privacy may still continue to travel uninhibited by car, rail, or ship. The Ninth Circuit, in addressing this counter-argument, has said, "[a] passenger is not, of course, compelled to travel by airplane, but many travelers would reasonably conclude that they had no realistic alternative."[116] However, in an apparent contradiction, the Ninth Circuit has also said that airport security measures can be seen as protecting the public's freedom to travel from terrorist interference, rather than abridging the individual's right.[117]

In *United States v. Bell*, the Second Circuit plainly rejected any right to travel argument in opposition to the anti-hijacking measures in place at the time.[118] According to the court, "[a]ny suggestion that the defendant's constitutional right to travel has been improperly interfered with would be amusing in other circumstances. We are trying to assure that right for the public and the resulting inconvenience of the few should be at least tolerable."[119]

The right to travel is not an unqualified right.[120] Nevertheless, the right to travel may not be conditioned upon the relinquishment of the right to privacy.[121] This leads to a contorted view of the right to travel. The right, while found in many different places, is not unconditional, but it cannot be conditioned upon the giving up of a fundamental right. Therefore, a logical estimate of the restrictions which may be imposed on the right to travel are most likely to be similar to the restrictions surrounding abridgement of the right to privacy: reasonableness. This determination is not very helpful because, as previously discussed, reasonableness can be a very amorphous standard.[122]

---

116 United States v. $124, 570 U.S. Currency, 873 F.2d 1240, 1248 n.8 (9th Cir. 1989).

117 United States v. Davis, 482 F.2d 893, 913 n.59 (9th Cir. 1973).

118 464 F.2d 667 (2d Cir. 1972).

119 *Id.* at 674.

120 *Davis*, 482 F.2d. at 912.

121 *Id.* at 913.

122 *See* United States v. McDaniel, 463 F.2d 129, 132 (5th Cir. 1972) (stating that "reasonableness may vary with circumstance").

At least one court has reached this same conclusion regarding the right to travel. The Ninth Circuit has stated that "governmental restrictions upon freedom of travel are to be weighed against the necessity advanced to justify them,"[123] and a restriction may only be justified "by a clear showing that they are necessary to promote a compelling governmental interest."[124] Unquestionably, this standard mirrors the test applied in a right to privacy determination. As a result, reasonableness in the right to travel context may be presumed for security measures which also satisfy reasonableness in a right to privacy determination.

II. AN OVERVIEW OF BIOMETRIC TECHNOLOGY

Airports around the country and abroad are beginning to utilize biometrics for security and identification purposes. Biometric technology utilizes the unique characteristics of an individual in order to recognize or identify that person.[125] Biometric identifiers include any characteristic that differentiates one person from another: fingerprints, hand geometry, retina scans, iris scans, gait, facial imaging, voice recognition, or DNA.[126] Although, as the previous list demonstrates, the types of biometric identifiers are vastly different, biometric systems operate within the same standard structure.

When a digital biometric measurement is first collected, it is reduced to a number or code and then stored in a database. Once a database is compiled, whenever a biometric measurement is taken, it is compared to other measurements previously stored in the database to see if there is a match.[127] In this way, biometric characteristics function as human passwords—they are unique to the individual, cannot be forged, and cannot be stolen.[128] Indeed, some biometric identifiers are more optimal

---

[123] *Davis*, 482 F.2d at 912.

[124] *Id.* at 913 n.57 (citing Shapiro v. Thompson, 394 U.S. 618, 642-44 (1969) (Stewart, J., concurring)).

[125] Arun Ross, Salil Prabhakar & Anil Jain, *An Overview of Biometrics*, *at* http://biometrics.cse.msu.edu/info.html (last visited Jan. 28, 2004).

[126] A.K. Jain, A. Ross and S. Prabhakar, *An Introduction to Biometric Recognition*, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, SPECIAL ISSUE ON IMAGE- AND VIDEO-BASED BIOMETRICS, Vol. 14, No. 1, pp. 7-11, January 2004.

[127] Ross, Prabhakar & Jain, *supra* note 125.

[128] Clyde Wayne Crews, Jr., *Human Bar Code: Monitoring Biometric Technologies in a Free Society*, POLICY ANALYSIS, Sept. 17, 2002.

than others, in terms of security, efficiency, and reliability.[129] The best biometric identification systems for wide-scale public use are accurate, non-invasive, capable of accommodating large amounts of information, and accepted by the general public.[130]

Biometric identifiers such as DNA, hand geometry, or gait are not widely used or accepted. These identifiers are either too invasive to gain wide-range acceptance or not individual enough to facilitate broad-scale implementation. For domestic and international airports, the most promising biometric measurements are digital fingerprinting, facial recognition, and iris scans.[131] As will be seen, these three types of biometric measurements hold the most possibilities for wide-scale implementation in security and identification.

A. FINGERPRINTING

Fingerprinting is the oldest, most widely known form of biometric identification.[132] Compared to other biometric identifiers, fingerprinting is one of the least expensive systems to employ. No two fingerprints are the same, so fingerprints can be accurately matched.[133] In addition, the FBI has already compiled a database of approximately 70 million fingerprints.[134] Because fingerprinting has been around for such a long time, many people have become accustomed to its use, but for the same reason, others have attached a criminal stigma to the use of fingerprinting.[135] The use of fingerprints does have other drawbacks. Inkless fingerprint scanners have been fooled simply by breathing on the sensor, and fingers with cuts, scrapes, or scars may not be recognizable.[136]

---

[129] Salil Prabhakar, Sharath Pankanti, & Anil K. Jain, *Biometric Recognition: Security and Privacy Concerns*, IEEE SECURITY & PRIVACY, March/April 2003, at 36.

[130] John Kavanaugh, *National Identity Register Could Be An Expensive Flop, Warns BCS*, Computer Weekly.com, *at* http://computerweekly.co.uk/articles/article.asp?liAritcleID=127588&liArticleTypeI (last visited Jan. 31, 2004).

[131] Leela Jacinto, *Biometrics Takes Flight After Terrorist Attacks*, ABC News.com, at http://abcnews.go.com/sections/scitech/CuttingEdge/WTC_biometrics010921.html (last visited Jan. 31, 2004).

[132] Salil Prabhakar & Anil Jain, *Fingerprint Identification*, *at* http://biometrics.cse.msu.edu/fingerprint.html (last visited Jan. 28, 2004).

[133] Jain, Ross & Prabhakar, *supra* note 126.

[134] *Id.*

[135] Prabhakar, Pankanti, & Jain, *supra* note 129, at 39.

[136] Brett Glass, *Balky Biometrics*, ABC News.com, *at* http://www.abcnews.go.com/sections/scitech/zdm/biometric_security_pcmag_031229.html (last visited Jan. 20, 2004).

B. Eye Scans

There are two types of biometric measurements that can be taken from a person's eyes: retina scans and iris scans. The retina is the conglomeration of blood vessels located at the rear of the eye.[137] A retina scan is one of the most secure biometric identifiers because the retina is not easily modified or copied.[138] However, obtaining a reliable retina scan is a semi-invasive procedure that requires close interaction with special eyepiece that must focus a light stream towards the back of the eye in order to take the image.[139] Furthermore, a retina scan may reveal more about the person than merely their identity.[140]

A better alternative to using the retina may be the iris, which is the colored region of the eye that surrounds the pupil.[141] Like the retina, an iris is distinctive and difficult to tamper with, but unlike its ocular counterpart, an iris scan is fast with virtually no discomfort.[142] Also, testing has shown that the iris is more secure than a fingerprint.[143] Iris scanning technology is currently being tested and developed at London's Heathrow airport as a way to more efficiently identify foreign citizens as they pass through customs.[144] If the Heathrow testing is successful, New York's JFK airport and Washington's Dulles airport will consider implementing iris scanning technology as well.[145] The weakness, as some critics have pointed out, is that assembling a database of terrorist's irises is highly improbable, if not completely unrealistic.[146] Also, in previous tests, some scanners been fooled by merely putting a picture in front of the sensor.[147]

---

137 Jain, Ross & Prabhakar, *supra* note 126.

138 *Id.*

139 *Id.*

140 *Id.* (In addition to identification, a retina scan may reveal medical conditions or drug use).

141 *Id.*

142 *Id.*

143 Jacinto, *supra* note 131.

144 *Airport tests passenger eye IDs*, BBC News, *at* http://news.bbc.co.uk/1/hi/uk/1808187.stm (last visited Jan. 28, 2004).

145 *Id.*

146 Addie S. Ries, *Comment: America's Anti-Hijacking Campaign—Will It Conform to Our Constitution?*, 3 N.C. J. L. & Tech. 123, 148 (2001).

147 Glass, *supra* note 136.

C. Facial Imaging

Facial imaging is a one of the most manageable, non-invasive means of biometric identification.[148] Facial imaging systems can scan large numbers of people in high traffic settings. For example, in 2001, Tampa Bay police utilized facial imaging to monitor fans as they entered the Superbowl.[149] Casinos have been utilizing facial recognition technology for years.[150] Unlike its fingerprint or iris scan counterparts, facial recognition does not "require the cooperation of the person being identified."[151] According to biometric advocates, facial recognition systems can identify persons as they age or change hairstyles. Unfortunately, the systems sometimes have problems viewing persons at different angles or in different light.[152] Moreover, individuals may be able to evade an accurate measurement simply by wearing a hat and sunglasses. This is an example of the correlation between invasiveness and accuracy—the less invasive the biometric technique is, the more difficult it is to obtain a reliable measurement. Thus, what facial recognition loses in accuracy, it compensates for with covertness.

D. The Role of Databases

A collection of biometric information is only as useful as the operator's ability to effectively organize it and rapidly access it.[153] Thus, the heart of any biometric identification system is the database, which contains all the previously stored biometric identities for base comparison. The information life cycle of a database can be separated into four stages: collection, use and disclosure, processing, and retention-destruction.[154] Some advocates argue that biometrics themselves are harmless; rather, it is their use in databases, which link the biometric measurements

---

148 Jain, Ross & Prabhakar, *supra* note 126, pp. 7-11.

149 Vickie Chachere, *Biometrics Used at the Super Bowl to Detect Criminals in Crowd*, ABC News.com, *at* http://abcnews.go.com/sections/scitech/DailyNews/superbowl_biometrics_010213.html (last visited Jan. 31, 2004).

150 Simon Liu & Mark Silverman, *A Practical Guide to Biometric Security Technology*, IT Professional, *at* http://www.computer.org/itpro/homepage/jan_feb01/security3.htm (last visited Jan. 20, 2004).

151 Gail R. Light, *Security vs. Liberty: Weighing the Options*, MSU Today, Spring 2002, *available at* http://www.msutoday.msu.edu/research/index.php3?article=20Jun2002-9.

152 Jain, Ross & Prabhakar, *supra* note 126.

153 John J. Brogan, Comment, *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, 25 Hastings Comm. & Ent. L.J. 65, 69 (2002).

154 US-VISIT Program, Increment 1 Privacy Impact Assessment, Dec. 18, 2003.

to other sensitive information, that makes them invasive.[155] Accordingly, the invasiveness of biometric technology is directly correlated to the structure of the underlying database.[156]

The government's attempt to construct a national database that would utilize biometric identification has many privacy experts worried about Big Brother.[157] Often privacy concerns arise because government officials do not implement enough controls to properly guard the public's interest.[158] By concentrating governmental information in a central database, the possible risk of identity theft is increased along with the scope of the harm if someone's identity is compromised.[159] In order to control the invasiveness of information acquisition, the distinction between public and private databases should be properly maintained in a decentralized format.[160]

E. Utilization of Biometric Technology

Although biometric identifiers may be useful in potentially solving a litany of problems, the most obvious is the current issue of identity theft. Because of their ability to verify a person's identity, travel documents and identification cards that utilize biometrics are gaining popularity and acceptance. Also, an increasing number of airports are considering the use of biometrics to decrease the time spent at security checkpoints.[161] The use of biometrics in almost all cases will constitute a search; however, whether the search is subject to Fourth Amendment scrutiny has yet to be determined.

III. THE APPLICATION OF BIOMETRIC TECHNOLOGY IN AIR TRAVEL

The examination of the case law surrounding the right to privacy and the right to travel highlights some threshold questions

---

155 Dennis Carlton, *Integrity and Security at the Borders: The US VISIT Program*, Testimony to the House Select Committee on Homeland Security (Jan. 28, 2004), *at* http://www.biometricgroup.com/US-VISIT.html (last visited Jan. 31, 2004); *see also*, Larry Jacobs, *Attacking Terrorism—And Privacy?*, ABC News.com, *at* http://abcnews.com (last visited Jan. 31, 2004).

156 Brogan, *supra* note 153, at 82.

157 *See* George Orwell, 1984 (Harcourt Brace Javanovich, Inc. 1949).

158 Chachere, *supra* note 149.

159 Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 Harv. J.L. & Tech. 319, 337 (2002).

160 *Id.*

161 *Biometrics for Safer Air Travel*, findBiometrics.com, *at* http://www.findbiometrics.com/Pages/airport_articles/airports_4.html (last visited Jan. 20, 2004).

regarding the legitimacy of using biometric technology and its place in airport security. In order to strike an equitable balance between privacy and security, biometric technology must be developed and utilized in the least intrusive, most effective manner and under the control of realistic safeguards. Furthermore, due to the theoretical split in authority dealing with the legitimacy of airport searches, new proposals must undergo multiple evaluations in order to account for the distinctive nuances of each justification. This paper will address current and future uses of biometrics and whether each may be reconciled with the fundamental rights discussed above.

A. US-VISIT

On October 28, 2003 the Department of Homeland Security (DHS) unveiled United States Visitor and Immigrant Status Indicator Technology (US-VISIT).[162] Beginning January 12, 2004, visitors from selected countries that enter the United States at various ports of entry will be photographed and fingerprinted by Customs officials.[163] According to the DHS, the use of biometric identifiers will make security more effective than the use of name databases alone, especially since persons will not be able to claim another's identity or forge travel documents.[164] The biometric data that the DHS gathers will be securely stored in a governmental database and made available only to authorized officials.[165] Nevertheless, US-VISIT is sure to encounter issues of privacy relating to the use of digital fingerprinting, facial recognition, and centralized databases.

Initially, US-VISIT will apply only to "covered individuals."[166] Covered individuals are defined as "nonimmigrant visa holders traveling through air and sea ports."[167] Following the Supreme Court's decision in *United States v. Verdugo-Urquidez*,[168] such a program will probably not fall within the protections of the Fourth Amendment. In *Verdugo-Urquidez*, the Court addressed the scope of the Fourth Amendment, which protects "the peo-

---

162 *US-VISIT FACT SHEET*, findBiometrics.com, *at* http://www.findbiometrics.com/Pages/feature%20articles/usvisit.html (last visited Jan. 20, 2004).

163 *Id.*

164 *Id.*

165 *Id.*

166 US-VISIT Program, Increment 1 Privacy Impact Assessment, Dec. 18, 2003.

167 *Id.*

168 United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

ple."[169] According to the Court, "'the people'. . . refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[170] The Court went on to say that "[t]he Bill of Rights is a futile authority for the alien seeking admission for the first time to these shores."[171] Thus, as long as US-VISIT only applies to covered individuals, the protections afforded by Fourth Amendment will not apply.[172]

As described, the US-VISIT program raises concerns regarding the collection of sensitive biometric identification, use of the information, and database management. In an attempt to quell some of those concerns, the DHS has appointed a privacy officer to oversee implementation of the program and utilization of the information collected.[173] Yet, administrative controls must be more explicitly defined and enforced in order to effectively regulate the immense database network that US-VISIT has created.[174]

Moreover, it is possible US-VISIT will not remain limited to covered individuals. Although the US-VISIT program is still in its infant stages, government officials have already suggested modifying the program to facilitate general airport security.[175] The most recent proposal for the government's modified system has been named "Trusted Traveler."[176] Initially available only on a volunteer basis, individuals would submit to a background check and then receive a card which identifies the individual as a "trusted traveler."[177] This "smart card" is secured from forgery or theft by the addition of a biometric identifier such as a finger-

---

169 *Id.* at 265.

170 *Id.*

171 *Id.* at 271 (quoting Bridges v. Wixen, 326 U.S. 135, 161 (1945)).

172 While the program may remain limited to covered individuals, the United States will need to incorporate biometrics into United States passports and similar travel documents or risk having them become the instruments of choice for terrorists seeking to avoid the biometric requirements of US-VISIT. *See* Carlton, *supra* note 155.

173 US-VISIT Program, Increment 1 Privacy Impact Assessment, Dec. 18, 2003.

174 *Id.*; *see also* John Pallatto, *What Price Security? US-VISIT*, eWeek, *at* http://www.eweek.com/print_article/0,3048,a=116163,00.asp (last visited Jan. 31, 2004).

175 Sara Kehaulani Goo, *U.S. to Push Airlines for Passenger Records*, Washington Post, *at* http://www.washingtonpost.com/ac2/wp-dyn/A8504-2004Jan11?.

176 *Report Calls for Trusted Traveler System and Offers Alternative to CAPPS II*, RPPI.org, *at* http://rppi.org/052903.html (last visited Feb. 13, 2004).

177 *Id.*

print or an iris scan.[178] According to the government, "Trusted Traveler" would increase airport security, while simultaneously decreasing the amount of time passengers spend at security checkpoints.[179] However, the program may create a de facto national identification card and institute a class system of air travel, which has troubled many opponents of the program.[180]

The idea of a national identification card is not novel but has recently gained renewed momentum with the government's efforts to increase national security. The latest derivative of a national identifier is the smart card. A smart card is the size of a driver's license or credit card and is encoded with a biometric measurement from its owner.[181] The smart card relieves the need to have an independent biometric database, since the biometric information is stored on the card itself. Implementation of the "Trusted Traveler" program would require consent; but if displaying the card were a prerequisite to boarding an airplane, then questions arise as to whether the consent is truly voluntary.[182]

The smart card is generally publicized as a convenience. Smart cards are already being used to control access to restricted airport areas, and the TSA has begun to issue employees tamperproof ID badges with biometric components.[183] Because the card allows persons to be accurately identified with biometric verification without the need for any further validation, there is a reduction in security time and expense. In fact, similar technology is utilized by individuals everyday, without any mention of privacy.[184] But some feel "[r]equiring photo [identification] to travel and creating databanks for profiling passengers' personal travel habits invades the privacy of millions . . . and threat-

---

178 Barbara De Lollis, *'Trusted-traveler' card could speed security check*, USA Today, *at* http://www.usatoday.com/tech/news/2002/07/02/trusted-traveler.htm (last visited Feb. 13, 2004).

179 *Id.*

180 Sobel, *supra* note 159, at 359; *see also* Press Release, ACLU, *Color Profiling or Racial Profiling? What is the Difference?* (July 12, 2003) [hereinafter Press Release ACLU] (on file with author).

181 RUWANTISSA I.R. ABEYRATNE, AVIATION TRENDS IN THE NEW MILLENIUM 75-76 (Ashgate 2001).

182 *See* United States v. $124,570 U.S. Currency, 873 F.2d 1240, 1247 n. 8 (9th Cir. 1989).

183 *Association of Flight Attendants Supports Biometric Security Systems*, BiometriTech 2003, *at* http://www.tmcnet.com/biometritech/02/042402a.htm (last visited Jan. 20, 2004).

184 For example: Tollway tags, Grocery Store Club Cards, and "Smart" Credit Cards.

ens their right of privacy without materially affecting the safety of the flying public."[185]

Additionally, the smart card can be viewed as a means of electronic surveillance. The Supreme Court is not unfamiliar with the concept of electronic surveillance; indeed, the Court's decision in *Katz* was a product of unwarranted government eavesdropping.[186] In subsequent opinions, many justices have expressed deep concern that such intrusions will eventually eviscerate the protections of the Fourth Amendment.[187] Specifically, Justice Douglas, opined that "the use of [uncontrolled] electronic surveillance . . . promises to lead us into a police state."[188]

The right to privacy may be said to include the right to anonymity. There was once a time when, if you obeyed the law, no one would pay attention to your comings and goings. In fact the Supreme Court has recently granted certiorari to address that very question in *Hiibel v. Sixth Judicial Circuit of Nevada.*[189] At issue is "whether an individual has the right to refuse to identify himself to a law enforcement officer before arrest."[190] The outcome of this case will have a definite impact on future litigation involving privacy rights, since the right to anonymity and freedom from government surveillance are implied in the right of privacy.

B. CAPPS II

In conjunction with the introduction of US VISIT, the DHS and TSA are planning to initiate an updated system for screening commercial airline passengers.[191] Computer Assisted Passenger Pre-Screening (CAPPS II), which is set to replace the airlines' existing system (CAPPS I), has many privacy advocates concerned, since the program will require airlines to turn over all passenger records and other personal information to the TSA.[192] The information collected from the airlines is then

---

185 Sobel, *supra* note 159, at 359.

186 Katz v. United States, 389 U.S. 347, 351 (1967).

187 United States v. White, 401 U.S. 745, 760 (1971) (Douglas, J., dissenting).

188 *Id.* (Douglas, J., dissenting).

189 Hiibel v. Sixth Jud. Dist. Ct. of Nev., 540 U.S. 965, (2003).

190 Electronic Privacy Information Center, *Hiibel v. Sixth Judicial Circuit of Nevada, at* http://www.epic.org/privacy/hiibel/default.html (last visited Jan. 31, 2004); *see also* Hiibel v. Sixth Jud. Dist. Ct., 59 P.3d 1201 (Nev. 2003).

191 Goo, *supra* note 175.

192 *Id.*

processed by a commercial database in order to validate the identity of the passenger.[193] After each individual is identified, the program will cross-reference the passenger with private government databases containing terrorist intelligence, criminal records, and other undisclosed variables.[194] The result is a "risk factor" denominated by either a green, yellow, or red color code.[195] These codes are then used to determine whether a passenger should be subjected to additional scrutiny or perhaps excluded from flying altogether.[196]

Such an accumulation of information by the government has many civil libertarians worried.[197] But according to the chief privacy officer at the DHS, "if the databases are merged, the government would impose strict rules about which agencies can use the passenger information and how it could be used."[198] To many citizens concerned about governmental intrusion, this guarantee is of little comfort.

While profiling is not new to airport security, the CAPPS II program seeks to utilize profiling in a more invasive and controversial way, compared to the system in place under CAPPS I. A few court decisions briefly addressed profiling when it was first introduced by the government in early 1970's as a means of reducing incidents of air piracy. In *United States v. Skipwith*, the defendant argued that a search that was partly based on a profile was unreasonable.[199] While the court acclaimed profiling as a "useful tool" in combating air piracy, it expressed doubts as to whether the profile alone would satisfy the reasonableness test and ultimately decided the case on other grounds without finding the need to address the profile question.[200]

The Third Circuit also touched on the use of profiling in *United States v. Slocum*.[201] The defendant proposed that "the Profile" was used as an inappropriate means of establishing probable cause by way of statistical comparisons.[202] Like the Fifth Circuit, the Third Circuit failed to address the issue regarding

---

193 Press Release, ACLU, *supra* note 180.

194 *Id.*

195 *Id.*

196 *Id.*

197 *Id.*

198 Goo, *supra* note 175.

199 482 F.2d 1272, 1275 (5th Cir. 1973).

200 *Id.*

201 464 F.2d 1180 (3d Cir. 1972).

202 *Id.* at 1183.

the legality of "the Profile."[203] Instead, the court concluded that "solely because the Profile operates on the basis of statistical comparison . . . [does not necessarily mean] it should be considered as an attempt to establish probable cause."[204] As a result, "the Profile" fell outside the requirements of the Fourth Amendment.[205]

Profiling is problematic and controversial because it is contrary to the constitutional presumption of innocence. With the use of profiling, a search takes place without any probable cause or individual suspicion. Instead, the suspicion is based on statistical probabilities.[206] Based on the results of a CAPPS II risk assessment, a traveler may be subjected to increased scrutiny or barred completely from boarding an aircraft. While most challenged security measures impede the right to privacy or travel, barring a person from boarding an aircraft based on nothing more than statistical probability completely eradicates that right and is unheard of in the United States legal system. Such a program invalidates the presumption of innocence and substantiates action based on nothing more than the individual's statistical intent without the support of a complementary actus reus element.

"[N]o court has ever approved a dragnet search of all citizens in a highcrime [sic] area of any urban center, based upon the justification that the danger of criminal conduct would be reduced."[207] However, "a dragnet" is exactly how the Director of the ACLU's Technology and Liberty Project has described the CAPPS II program.[208] "[P]rofiling presupposes the right to scrutinize citizens in ordinary circumstances."[209] Furthermore, the use of profiling eradicates one of the safeguards relied upon in past airport search cases, that "the net can sweep no wider than necessary since the broad right to search is limited to the last possible point in time and space which could protect the aircraft, the boarding gate."[210] In support of profiling, some have argued that the indiscriminate application of a profile to

---

203 *Id.*

204 *Id.*

205 *Id.*

206 Sobel, *supra* note 159, at 365.

207 United States v. Skipwith, 482 F.2d 1272, 1275 n.4 (5th Cir. 1973).

208 Press Release, ACLU, *supra* note 180. ("CAPPS II is illusory security on the cheap . . . [i]nstead of zeroing in on suspects based on real evidence of wrongdoing, it sweeps every airline passenger through a dragnet.").

209 Sobel, *supra* note 159, at 366.

210 *Skipwith*, 482 F.2d at 1276-1277.

everyone reduces the effect of stigma as well as the overall level of intrusion since only persons meeting the profile are singled out for more invasive searches.[211] This way the government is able to better focus its efforts on those persons that qualify for increased screening and increase the overall effectiveness of the search.[212]

With regards to the DHS security initiatives, the most invasive threat to individual privacy is the possible merger of US-VISIT with elements of the CAPPS II program. The product would be the plot Minority Report brought to reality—all persons would be biometrically identified and potentially barred from air travel based merely on statistical intent.[213] This scenario is likely in light of the opposition surrounding the current CAPPS II identification scheme. Many civil liberty organizations have opposed the collection of personal information from passengers that is then used to verify that the passenger is who he or she claims to be. An alternative to the unwarranted collection of personal data would be to employ biometrics in the same capacity as the US-VISIT program for identification. This alternative would reduce the cost of passenger identification by simply expanding US-VISIT to apply to all travelers, not just those entering the country. Indeed, "Trusted Traveler" contains elements of both programs (background checks and biometrics for identification); although at the moment on a volunteer basis only.[214] But how could citizens be sure that the program would not spread to other modes of travel or other aspects of society?[215] As Judge Oakes wisely observed, "[t]oday airports, tomorrow some other forms of search which may be applied to everyone."[216] There is little doubt that this type of program would not qualify as merely a limited intrusion on privacy.

---

211 *See* United States v. Edwards, 498 F.2d 496, 500 (5th Cir. 1974); United States v. Slocum, 464 F.2d 1180, 1183 (3d Cir. 1972).

212 De Lollis, *supra* note 178.

213 *See supra* note 1.

214 *But see* De Lollis, *supra* note 178 (stating that "Trusted Traveler" is not truly voluntary because "the price of not having one of these cards is going to be even more intrusive questioning and searches").

215 Press Release, ACLU, *supra* note 180.

216 *Edwards*, 498 F.2d at 502 (Oakes, J., concurring) (internal quotation marks emitted).

IV. ASSESSMENT AND ANALYSIS

To date, no reported court decisions have specifically addressed the constitutionality of either US-VISIT or CAPPS II.[217] However, if history is an accurate predictor, the trend is likely to be short-lived. In the late 1960's, the FAA initiated an anti-hijacking program in response to the threat of air piracy. At the time of the program's implementation, airport screening procedures were not uniform and incidents of air piracy were at all-time record numbers. In the years following its establishment, the new anti-hijacking initiative faced an array of court challenges questioning the program's constitutionality;[218] and as a result, a new body of law was developed. Thus, as the effects of US-VISIT and CAPPS II on the traveling public become more apparent, a new cluster of cases will begin to make their way through the federal court system and another string of authority will begin to emerge.

As cases come forth to challenge the constitutionality of US-VISIT and CAPPS II, the courts will most likely rely on the airport search cases of the 1970's with a renewed inquiry regarding how these programs should be evaluated. In light of the national security ramifications surrounding judicial scrutiny of these programs, a uniform method of review should be adopted. Under the circumstances presently facing security personnel today and in light of the recent establishment of the DHS and TSA, US-VISIT and CAPPS II should be reviewed under the administrative-search exception to the Fourth Amendment.

The administrative-search doctrine is appropriate for a number of reasons. First, the commercial air travel industry qualifies as a closely-regulated industry. Second, by establishing the TSA, Congress has specifically set up a regulatory scheme to monitor airport security, and *reasonable* airport searches are necessary to further that objective. Third, the government has a compelling interest in preventing another terrorist attack. Finally, the administrative-search doctrine is better suited to preserve property and balance competing government and individual interests than either the *Terry* rule, or implied consent.

---

[217] Some civil liberties organizations have initiated litigation concerning the disclosure of airline records to the government in relation to CAPPS II testing and implementation.

[218] Specifically, the cases challenged the use of profiling, the magnetometer, and physical searches taking place at the boarding gate. *See supra* notes sections (I)(A)-(B).

The implied consent exception to the strictures of the Fourth Amendment is not properly applied in the context of airport searches because such consent is the product of inadvertent coercion. Determining whether consent has been given is a fact intensive examination based on the "totality of the circumstances." If adopted, a highly factual inquiry would be required to determine if the consent in each case was "freely and voluntarily given." Such a rule would quickly prove to be inefficient to adequately address multiple privacy challenges based on ever-changing technology. An even more compelling reason not to adopt implied consent is the trend of recent cases that have questioned the rule's continuing viability in the context of airport searches.

Likewise, the *Terry* exception to the rule against warrantless searches should not apply to airport searches. The rule in *Terry*, while instructive, is based on the reasonable suspicion of the investigating officer. As such, the exception contains a subjective perception of the officer and could not be used to objectively review standardized security programs that pertain to millions of air travelers. Additionally, because the *Terry* rule is based on the presence of cause, the CAPPS II program would allow *Terry* to overlook otherwise invalid searches on the basis of the statistical cause established by the CAPPS II risk assessment.

Although, in the past, the administrative search doctrine has applied only to the regulated industry in question, due to the suitability of the exception to general airport searches and the incongruity of *Terry* and consent, the exception should be extended to apply to all individuals tangentially related to the industry, including passengers. With the rule so modified, as courts review the employment of biometrics technology, US-VISIT, or CAPPS II under Fourth Amendment scrutiny and apply the administrative search doctrine, some aspects of the programs, in their current state, will probably not pass constitutional muster. In taking the programs into consideration, relevant factors to the determination should include the reasonable scope of a program, the presence or absence of notice, and the overall level of invasiveness compared to the program's efficiency.

Any search utilizing more invasive technology must compensate with greater effectiveness. Collecting biometric measurements and doing background checks involves a greater intrusion than citizens have previously realized. Taking into account the current state of the technology, its debatable faults, and the fact

that such a system has never been implemented or tested on such a broad scale, the costs may outweigh the promised benefits.

Lastly, a warrantless airport search should be specifically tailored according to the security need in order to be reasonable. "Even though the governmental purpose be legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved."[219] But for commercial air passengers, the use of general profiling under CAPPS II and universal biometric tracking under US-VISIT can hardly be classified as specifically-tailored.

V. CONCLUSION

As biometric technology is rapidly advancing, its current state of effectiveness still leaves much to be desired. In terms of reasonableness, the advances offered by biometric technology as it now stands do not offer the gains in security that are expected with the corresponding invasion of privacy that occurs when biometric technology is implemented.

Society should be apprehensive of technological advances that threaten to invade previously undisturbed areas of life. The words of Justice Douglas more than thirty years ago are still applicable to the circumstances that citizens face today.

> Invasions of privacy demean the individual. Can a society be better than the people composing it? When a government degrades its citizens, or permits them to degrade each other, however beneficent the specific purpose, it limits opportunities for individual fulfillment and national accomplishment. If America permits fear and its failure to make basic social reforms to excuse . . . electronic surveillance, the price will be dear indeed. The practice is incompatible with a free society.[220]

"[H]istory reveals that the initial steps in the erosion of individual rights are usually excused on the basis of an 'emergency' or the threat to the public. But the ultimate strength of our

---

[219] United States v. Davis, 482 F.2d 893, 912-913 (9th Cir. 1973) (quoting Sheldon v. Tucker, 364 U.S. 479, 488 (1961)).

[220] United States v. White, 401 U.S. 745, 764 (1971) (Douglas, J., dissenting) (quoting R. CLARK, CRIME IN AMERICA 287 (1970)).

constitutional guarantees lies in their unhesitating application in times of crisis and tranquility alike."[221]

While biometric technology provides vast potential for improving security, it may be at too high a price in terms of lost privacy, individuality, anonymity and liberty. If programs such as US-VISIT and CAPPS II become assimilated into our way of life, then what liberty is there left to protect? While creating a police state may insulate the United States from many types of terrorism, it will substitute one inequity for another and in the end may create more problems than it solves.

---

[221] United States v. Edwards, 498 F.2d 496, 502 (1974) (Oakes, J., concurring); *see also* Laura Dawn Lewis, *So What Do We Have?*, commentary following Press Release, ACLU, *supra* note 180. (suggesting that if done in incremental steps, "society accepts [ ] each adjustment with little resistance via rationalizations of 'it is for your own good.' Study Germany in the 1930's and this is *exactly* how the country changed.") (emphasis in original).


SOUTHERN METHODIST UNIVERSITY
DALLAS, TEXAS

Casenotes


SOUTHERN METHODIST UNIVERSITY
DALLAS, TEXAS