Journal of Air Law and Commerce

Volume 81 | Issue 3 Article 6

2016

Fingerprints: A New Means of Identification in Airport Security Screening

Chase Hilton
Southern Methodist University

FINGERPRINTS: A NEW MEANS OF IDENTIFICATION IN AIRPORT SECURITY SCREENING

CHASE HILTON*

TABLE OF CONTENTS

* J.D. Candidate, SMU Dedman School of Law, May 2017; B.S. in Psychology, Louisiana State University. The author does not necessarily adopt the views contained within, but rather argues that fingerprints as a means of identification may be possible under the existing state of law, policy, and societal expectations.

I. INTRODUCTION

AIRPORT SECURITY HAS CHANGED, and with those changes have come the ever-versatile elastic pants, slip-on shoes, and various forms of comfortable garb to make undressing in the security line more reasonable. But fashion aside, passengers have been conditioned by the nearly rote requirements that those who are not part of the Transportation Security Administration (TSA) PreCheck program must do: remove their jackets, shoes, and belts and place their laptops in a separate bin.[1] Individuals who have traveled recently are all too familiar with those echoing words. But while security screening has changed greatly since the birth of mass air travel, there is one area that lacks advancement—passenger identification.

The Bureau of Transportation Statistics indicates that more than 851 million people in the United States took to the air in 2014,[2] and the newest administrator of the TSA, Peter Neffenger, stated that of those passengers, 660 million were screened by the TSA.[3] Thus, in an attempt to find the needle in the haystack, the current security screening procedures are "risk-based [and] intelligence-driven" to provide "expedited screening for trusted travelers and to focus on high-risk and unknown passengers at security checkpoints."[4] This manicured screening method, collectively called a Risk Based Strategy (RBS), is an attempt to "lessen the hay in the stack," and in a sense make the needle that much easier to find.[5] But alas, this method of threat prevention is not currently working. On June 1, 2015, major news sources reported that in an internal TSA investigation, security agents failed sixty-seven out of seventy tests (a failure rate of 95.7%), including the smuggling of weapons.[6] While the TSA neither confirmed nor denied the classified statistics leaked by the media, Melvin Carraway, the administra-

---

[1] *See Security Screening*, TRANSP. SEC. ADMIN., https://www.tsa.gov/travel/security-screening [https://perma.cc/AWB2-ENQ9].

[2] *Passengers, All Carriers – All Airports*, BUREAU OF TRANSP. STAT., http://www.transtats.bts.gov/Data_Elements.aspx?Data=1 [https://perma.cc/T3PC-4GUD].

[3] *TSA: Security Gaps: Hearing Before the H. Comm. on Oversight and Gov't Reform*, 114th Cong. 1–2 (2015) (statement of Peter Neffenger, Administrator, Transportation Security Administration), https://www.dhs.gov/news/2015/11/03/written-testimony-tsa-administrator-house-committee-oversight-and-government-reform [https://perma.cc/FV8A-YG8F].

[4] *Security Screening*, *supra* note 1.

[5] *See id.*

[6] Justin Fishel et al., *Undercover DHS Tests Find Security Failures at US Airports*, ABC NEWS (June 1, 2015, 7:04 AM), http://abcnews.go.com/US/exclusive-un-

tor of the TSA at that time, was immediately reassigned to another department within the Department of Homeland Security.[7]

The TSA's self-proclaimed mission is to "deter, detect, and disrupt threats,"[8] but with a failure rate over 95%, that mission is far from satisfied.[9] Currently, all passengers are screened using either advanced imaging technology (AIT), commonly called a body scanner, or walk-through metal detectors for those passengers who wish to forego the body scanner.[10] If one refuses the AIT scan or the metal detector, or sets off either of these instruments, that person is subjected to a pat-down.[11] Alas, all of these invasive security techniques are a means of unveiling hidden weapons, explosives, or other tangible objects that may be hidden on or in individuals' possessions, but what of the *individuals* themselves?

The importance of proper identification is the keystone to threat identification, detection, and prevention. Yet, identification may be one of the easiest security measures would-be terrorists could currently exploit. For example, Malaysia Airlines Flight 370 that went missing in March 2014 contained two passengers traveling with stolen passports.[12] In today's world of heightened security scrutiny, how does one board a plane without a passport, let alone while using a *stolen* passport? While the frequency of false identification is likely very low, the risk of allowing a falsely identified passenger through security is great.[13] On that issue, a researcher in the area of facial recognition, Dr.

---

dercover-dhs-tests-find-widespread-security-failures/story?id=31434881 [https://perma.cc/GT9F-Q8UV].

[7] Press Release, DHS Press Office, Statement by Secretary Jeh C. Johnson on the Transportation Security Administration (June 1, 2015), http://www.dhs.gov/news/2015/06/01/statement-secretary-jeh-c-johnson-inspector-general-findings-transportation-security [https://perma.cc/V2XT-NHWR].

[8] *Transportation Security Administration Efforts to Address IG Findings: Hearing Before the Subcomm. on Homeland Security of the S. Comm. on Appropriations*, 114th Cong. 1 (2015) [hereinafter *TSA Efforts*] (statement of Peter Neffenger, Administrator, Transportation Security Administration), http://www.dhs.gov/news/2015/09/29/written-testimony-tsa-administrator-senate-appropriations-subcommittee-homeland [https://perma.cc/UGL9-B2TX].

[9] Fishel et al., *supra* note 6.

[10] *Security Screening*, *supra* note 1.

[11] *Id.*

[12] Katia Hetter & Karla Cripps, *Who Travels with a Stolen Passport?*, CNN (Mar. 11, 2014, 10:53 AM), http://www.cnn.com/2014/03/10/travel/malaysia-airlines-stolen-passports/ [https://perma.cc/9Z93-QT3V].

[13] *See* Matthew Pryce, *Dr. Megan Papesh, Louisiana State University – Flaws of Facial Recognition Tech*, WAMC NORTHEAST PUB. RADIO (June 3, 2014), http://wamc

Megan Papesh, examined one's ability to match an individual to a presented photo identification within a controlled study.[14] The study indicated that one's recognition rates were "incredibly fallible, with error rates between 10 and 20 percent under ideal laboratory-induced conditions."[15] As Dr. Papesh stated, "[b]ecause society relies on face recognition and ID verification for so many tasks, people are under the impression that we are experts in this domain. Our research shows the precise opposite."[16] Most astoundingly, the results of the study indicated that "[w]hen observers infrequently encountered fakes, they failed to catch approximately 45 percent of them, even when given multiple opportunities to correct their errors."[17] The majority of passengers passing through airport security do in fact have valid identification, making the false forms of identification that much harder to spot. Thus, the need for better identification standards becomes even greater.[18]

But in light of current research, consider that the TSA only requires passengers over the age of eighteen to present photo identification and a proper boarding pass.[19] Examples of some accepted identifications include driver's licenses, state issued photo identity cards, and passports.[20] Even without proper identification, passengers may still be permitted per TSA regulations, but such passengers could be subjected to "additional screening."[21]

Identification is arguably the first and best means of threat detection and prevention. Much like Aristotle once stated, the whole is greater than the sum of its parts, individuals are a far greater threat in and of themselves than the means by which they may choose to inflict harm. Thus, identification standards in airport screening must be addressed to mitigate the potential errors and shortfalls. Rather than solely searching travelers for tangible threats, security checkpoints should proactively seek out travelers who *themselves* present significant threats. There-

---

.org/post/dr-megan-papesh-louisiana-state-university-flaws-facial-recognition-tech#stream/0 [https://perma.cc/34WL-MG6B].

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *See id.*

[19] *Identification*, TRANSP. SEC. ADMIN., https://www.tsa.gov/travel/security-screening/identification [https://perma.cc/HK67-93JM].

[20] *Id.*

[21] *Id.*

fore, the TSA should implement fingerprint scanning as a means of more reliable identification at airport security checkpoints. The implementation of such a procedure is appropriately rooted in case law, including Supreme Court precedent. However, this comment will examine the likely societal backlash and bring to light the contrasting issues of fingerprint implementation—privacy, safety, and security as a nation and as individuals.

Part II of this comment discusses the historical background of air travel threats, the security efforts to prevent them, and the future of air travel threat prevention. Part III discusses the legal standards for fingerprinting an individual, as well as the legal justifications that allow for airport security checkpoint searches and detention of one's person and possessions. Part IV applies the current law to the implementation of fingerprinting as a means of identification and presents the potential problems and protections necessary to safeguard individuals' privacy. Finally, Part V gives the conclusion.

II. SECURITY SCREENING IN AIRPORTS: TANGIBLE THREAT PREVENTION

A. Historical Background

To the millennial generation, September 11, 2001 (9/11), may have served as the first time the airline industry was used as a tool for political or tyrannical means, but threats to the airline industry have been pervasive and persistent since the 1960s. In the midst of widespread hijackings, or "skyjackings," President John F. Kennedy approved legislation in 1961 making air piracy punishable by death or imprisonment, marking the first time the government truly became involved in the private airline industry.[22] From 1961 to 1968 there was an average of one plane hijacking a year.[23] Specifically, in 1969, "there were 40 attempted hijackings of United States aircraft, 33 successful."[24]

Without undermining the 9/11 attacks, September 11, 1970, could in fact be deemed the beginning of the age of terrorism

---

[22] *See* Federal Aviation Act of 1958, Pub. L. No. 85-726, 72 Stat. 737 (codified at 49 U.S.C. §§ 101–80504).

[23] United States v. Davis, 482 F.2d 893, 898 (9th Cir. 1973), *overruled in part by* United States v. Aukai, 497 F.3d 955 (9th Cir. 2007).

[24] *Id.*

and the war against it.[25] When a multitude of plane hijackings occurred within a matter of days, President Richard Nixon responded with a statement on September 11, 1970, addressing several ways to protect U.S. citizens and deal with piracy in the skies.[26] President Nixon immediately placed armed U.S. government agents on planes, extended the use of electronic surveillance at all U.S. airports and foreign countries, and directed the Department of Transportation to hasten its discovery of advanced screening methods for detecting weapons and explosives and to determine whether military metal detectors and x-ray devices could be made ready for use in airports.[27]

By 1972, the Federal Aviation Administration (FAA) issued an emergency rule requiring all passengers and carry-on items to be screened,[28] with the purpose being "to prevent or deter the carriage aboard its aircraft of sabotage devices or weapons in carry-on baggage or on or about the persons of passengers."[29] Unfortunately, on March 9, 1972, a Trans World Airlines jet was blown apart by a bomb placed in the luggage compartment, and within twenty-four hours, bomb dogs found an explosive device on a plane at John F. Kennedy International Airport.[30] This event immediately prompted the FAA to implement explosive detection teams consisting of trained canines as part of the Explosives Detection Canine Team program.[31] Two years later, the Air Transportation Security Act of 1974 was adopted, which prompted the use of metal detectors in airports, as well as the

---

[25] Stephen Collinson, *Nixon's Own 9/11: When Terrorism Came of Age*, CNN (July 29, 2015, 5:02 PM), http://www.cnn.com/2015/07/27/politics/terrorism-1970s-richard-nixon/ [https://perma.cc/BK78-Q36D].

[26] Gerhard Peters & John T. Woolley, *Richard Nixon: Statement Announcing a Program to Deal with Airplane Hijacking*, THE AM. PRESIDENCY PROJECT (Sept. 11, 1970), http://www.presidency.ucsb.edu/ws/index.php?pid=2659 [https://perma.cc/T22L-BQRN].

[27] *Davis*, 482 F.2d at 899–900.

[28] *See id.* (quoting Press Release, Fed. Aviation Admin., No. 72-26 (Feb. 6, 1972)).

[29] *Id.* (citing 37 Fed. Reg. 2500–01 (Feb. 2, 1972)).

[30] *Bomb T.W.A. Jet; Device is Found on United Plane*, CHI. TRIB. (Mar. 9, 1972), http://archives.chicagotribune.com/1972/03/09/page/1/article/bomb-t-w-a-jet-device-is-found-on-united-plane [https://perma.cc/Q6LJ-J4L9].

[31] *Utilizing Canine Teams to Detect Explosives and Mitigate Threats: Hearing Before the Subcomm. on Transp. Sec. of the H. Comm. on Homeland Sec.*, 113th Cong. 1 (2014) (testimony of Melanie Harvey, Director, Transportation Security Administration), https://homeland.house.gov/hearing/subcommittee-hearing-utilizing-canine-teams-detect-explosives-and-mitigate-threats/ [https://perma.cc/QT6J-24LH].

use of x-ray technology to examine passengers' carry-on luggage.[32]

B. Modern Security Efforts

Fast forward nearly thirty years to the terror associated with 9/11. The TSA was created by the Aviation and Transportation Security Act on November 19, 2001, as a means of threat interdiction following the coordinated attacks on 9/11.[33] Until this point, all of the aforementioned measures of advanced security introduced were a means of identifying, confiscating, and preventing *tangible* methods of harm.[34] Specifically, the predominant case in the 1970s, *United States v. Davis*, proclaimed that magnetometer and x-ray scans were "justified as an administrative procedure, an exception to the warrant rule tolerated as necessary to insure safety in air travel."[35]

But what of the *persons* behind the hijackings, threats, and dangerous weapons or explosives? The TSA created the "No Fly List" and "Secure Flight," which are a means of tracking those persons identified by the Federal Bureau of Investigation (FBI) and other intelligence agencies to be a threat to national security.[36] The No Fly List was quite literally a collection of names that agencies compiled that were deemed unworthy of the right to travel by air because they posed a risk to security.[37] The Associated Press suggested that as many as 10,000 names were listed on the No Fly List in 2011.[38] A secondary list of individuals, called the "Selectee List," laid out names of individuals who would be subjected to greater scrutiny in the security screening process but were still granted the ability to fly.[39] Secure Flight was implemented in 2009 as a watchlist matcher to verify that

---

[32] Jane Engle, *U.S. Aviation Security Timeline,* L.A. Times (June 12, 2011), http://articles.latimes.com/2011/jun/12/travel/la-tr-airline-safety-timeline-20110612 [https://perma.cc/7CAF-245S].

[33] *Evolution Timeline*, Transp. Sec. Admin., https://www.tsa.gov/video/evolution/TSA_evolution_timeline.pdf [https://perma.cc/4QQC-W579].

[34] *See id.*

[35] United States v. Maldonado-Espinosa, 767 F. Supp. 1176, 1186 (D.P.R. 1991). *See* Part III.B for discussion on the warrantless search rationale in airports. *Davis* was overruled in 2007 but only on the means by which an airport search was deemed appropriate.

[36] Dan Lowe, Note, *The Flap with No Fly – Does the No Fly List Violate Privacy and Due Process Constitutional Protections?*, 92 U. Det. Mercy L. Rev. 157, 158–59 (2015).

[37] *Id.* at 158.

[38] *Id.* at 159.

[39] *Id.* at 160.

individuals scheduled to fly were not a part of the No Fly List by running their name, gender, and date of birth against a series of watchlists.[40] The goal behind Secure Flight was to "prevent the misidentification of passengers who have names similar to actual people on the government watchlists and . . . allow more than 99% of travelers to print their boarding passes from home or kiosks and avoid undergoing additional screening because of a mismatch."[41] But once at the security checkpoint, these individuals would be identified only by their boarding pass and photo identification, which, as common knowledge and research now indicates, can be easily forged and fooled.[42] Alas, the development of these lists and programs could all be for naught if the individual can easily skirt the current identification standards.

C. TSA's Future of Airport Security

On September 2, 2015, the TSA presented its five-year strategic technology plan to the public in which it posed four themes:

> Integrating principles of Risk-Based Security (RBS) in capabilities, processes, and technologies;
>
> Enhancing core mission delivery by focusing on a system (or systems) that analyzes threats, risks[,] and opportunities across the aviation security environment;
>
> Streamlining acquisitions, requirements, and test and evaluation processes; and
>
> Increasing transparency in engagement with stakeholders to enable innovation.[43]

The methodology of airport security screening is dramatically changing from the aforementioned one-size-fits-all approach that required scanning of all passengers stemming from the laws

---

[40] Bob Burns, *Individuals on the No Fly List Are Not Issued Boarding Passes*, TSA Blog (May 11, 2012, 4:38 PM), http://blog.tsa.gov/2012/05/individuals-on-no-fly-list-are-not.html [https://perma.cc/P8NN-F8FT].

[41] Bob Burns, *Secure Flight: TSA Now Performing 100% Watchlist Matching for Domestic Flights*, TSA Blog (June 11, 2010, 3:50 PM), http://blog.tsa.gov/2010/06/secure-flight-tsa-now-performing-100.html [https://perma.cc/PD4A-NFUX].

[42] *See* Pryce, *supra* note 13.

[43] *Transportation Security Acquisition Reform Act: Examining Remaining Challenges: Hearing Before the Subcomm. on Transp. Sec. of the H. Comm. of Homeland Sec.*, 114th Cong. 2 (2016) (statement of Jill Vaughan, Assistant Administrator, Transportation Security Administration), https://docs.house.gov/meetings/HM/HM07/20160107/104303/HMTG-114-HM07-Wstate-VaughanJ-20160107.pdf [https://perma.cc/WLH3-4ZHK].

of the '70s.[44] In line with its four themes, the TSA hopes to reduce the scrutiny of search on those passengers who are deemed "known" or "trusted" so that emphasis may be placed on travelers who travel infrequently or sporadically with the implementation of programs such as TSA PreCheck and Secure Flight.[45] Thus, those passengers who enroll in certain airline programs may receive expedited security screening with minimal focus on the search and detention of their person.[46] The TSA began using RBS in October 2011 when TSA PreCheck was first implemented to carry out the goals of reducing security checkpoint lines and enhancing passengers' experiences with security.[47]

To carry out those goals, Peter Neffenger, the head administrator of the TSA, proclaimed that he "envision[s] a future where some known travelers will be as vetted and trusted as flight crews. Technology on the horizon may support passengers becoming their own 'boarding passes' by using biometrics, such as fingerprint scans, to verify identities linked to Secure Flight."[48] The evolution of screening is moving toward technology that makes security checkpoints less invasive and more efficient.[49] Neffenger's goal is to move away from screening known and vetted passengers and require more extensive searches of unvetted passengers.[50] But in terms of identification verification, current identification policy still only requires that an individual present a valid photo identification or undergo a more thorough security screening.[51] This screening may include a hand search of one's carry-on and a pat-down of an individual's person, in addition to a wand metal detector search.[52] Neffenger's implementation of biometrics into the security screening process aligns with verifying the identity of passengers who have already submitted fingerprints through programs such as TSA PreCheck and distances itself from merely tangible threat pre-

---

[44] *See supra* Part II.B.

[45] *TSA: Security Gaps*, *supra* note 3.

[46] *Id.*

[47] *Transportation Security Administration (TSA), Office of Security Capabilities Strategic Five-Year Technology Investment Plan*, FED. BUS. OPPORTUNITIES (Sept. 2, 2015, 10:58 AM), https://www.fbo.gov/index?s=opportunity&mode=form&id=e21937c258a962298f69181298829124&tab=core&_cview=0.%202%20P%2027 [https://perma.cc/E5KN-PXFZ].

[48] *TSA: Security Gaps*, *supra* note 3.

[49] *See id.*

[50] *Id.*

[51] *Identification*, *supra* note 19.

[52] *Id.*

vention.[53] Most importantly, Neffenger's goal could be appropriately achieved through fingerprinting all passengers. As the following section examines, Supreme Court precedent likely supports widespread fingerprinting in the airport security context. Perhaps in the near future security screening really will permit travelers to act as their own human boarding passes, especially as the law seems to support that notion as well.

III. STANDARDS FOR SEARCHING: FINGERPRINTS AND AIRPORT SECURITY

A. Legal Requirements to Obtain Fingerprints

In examining the requirements for fingerprinting or using biometric data, one must first understand the legal requirements for identification in the airport and for obtaining a fingerprint from an individual. The past decade of case law indicates that the current identification policy that requires an individual to present valid photo identification or undergo a more thorough security screening has been upheld as constitutional.[54] In 2006, John Gilmore challenged the identification policy of the TSA that required passengers to present identification before boarding or, in the alternative, undergo a more invasive search.[55] Gilmore was informed that without his identification he could enter the terminal by becoming a "selectee."[56] This required removing his shoes, passing through a magnetometer, a handheld magnetometer scan, a body pat down, and a hand search of his carry-on, in addition to a scan of his carry-on luggage.[57] When Gilmore reached the security checkpoint, he did not present identification, refused to have his bag hand-searched, and was denied access to the terminal.[58] Upon asking for clarification of the identification policy, Gilmore was told by security personnel that the security directive that declared the identification policy was "sensitive security information."[59] Gilmore alleged in his complaint, inter alia, that this directive hindered his "right to due process, right to travel, right to be free from unreasonable

---

[53] *See infra* Part IV.B for the various programs in place now that currently use biometric technology or require biometric data of travelers.

[54] *See* Gilmore v. Gonzales, 435 F.3d 1125, 1137–38 (9th Cir. 2006); *Identification*, *supra* note 19.

[55] *Gilmore*, 435 F.3d at 1129.

[56] *Id.* at 1130.

[57] *Id.*

[58] *Id.*

[59] *Id.* at 1130–31.

searches and seizures, right to freely associate, and right to petition the government for redress of grievances."[60]

The Ninth Circuit ultimately determined that the directive did require a showing of identification or a selectee search, but did not elucidate upon the TSA's reasoning for identification.[61] Due to the sensitive nature of the security directive, the court heard the directive in camera to determine its finality.[62] The Ninth Circuit held that the request for identification did not implicate Gilmore's Fourth Amendment rights, as "'[a] request for identification by the police does not, by itself, constitute a Fourth Amendment seizure.'"[63] Thus, because mere identification is neither a search nor a seizure, asking for identification cannot implicate the Fourth Amendment.[64]

Along these same lines, the fingerprinting of individuals may also merely serve as a means of identification.[65] In 1969, the U.S. Supreme Court held in *Davis v. Mississippi* that the defendant's Fourth Amendment rights were violated when police picked up twenty-five minors (including the defendant) and brought them to the police station for fingerprinting to match fingerprints found at the scene of a rape.[66] The Court held that the fingerprinting of the defendant violated his Fourth Amendment rights because the defendant underwent two fingerprinting sessions, he was interrogated, and the detention was not authorized by a judge.[67]

Expanding upon the holding, the Court stated that detentions without probable cause for the sole purpose of obtaining fingerprints violated the Fourth Amendment rights of individuals.[68] However, Justice Brennan added for the majority, "because of the unique nature of the fingerprinting process, such detentions might, under narrowly defined circumstances, be found to comply with the Fourth Amendment even though there is no probable cause in the traditional sense."[69] Justice Brennan highlighted that the nature of fingerprinting is simply a means of identification that may outweigh and trump other forms.

---

[60] *Id.* at 1131.
[61] *Id.* at 1136–37.
[62] *Id.* at 1131.
[63] *Id.* at 1137 (quoting INS v. Delgado, 466 U.S. 210, 216 (1984)).
[64] *Id.* at 1138.
[65] *See* Davis v. Mississippi, 394 U.S. 721, 727 (1969).
[66] *Id.* at 722, 728.
[67] *Id.* at 728.
[68] *Id.*
[69] *Id.* at 727.

> Detention for fingerprinting may constitute a much less serious intrusion upon personal security than other types of police searches and detentions. Fingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search. Nor can fingerprint detention be employed repeatedly to harass any individual, since the police need only one set of each person's prints. Furthermore, fingerprinting is an inherently more reliable and effective crime-solving tool than eyewitness identifications or confessions and is not subject to such abuses as the improper line-up and the "third degree."[70]

Sixteen years later, the Supreme Court revisited Fourth Amendment rights and fingerprinting in *Hayes v. Florida*, a factually similar case.[71] Again, the defendant was taken to the police station without probable cause to arrest and was fingerprinted without consent.[72] There, the Court took the view that when someone is forcibly moved to a police station, a seizure of one's person has taken place, which requires probable cause.[73] However, Justice White also indicated, "[n]one of the foregoing implies that a brief detention in the field for the purpose of fingerprinting, where there is only reasonable suspicion not amounting to probable cause, is *necessarily impermissible* under the Fourth Amendment."[74] White supported this statement by echoing the Court's position in *Adams v. Williams*, where the Court held that "[a] brief stop of a suspicious individual, *in order to determine his identity* or to maintain the status quo momentarily while obtaining more information, may be most reasonable in light of the facts known to the officer at the time."[75] The cornerstone of the holding indicates that fingerprinting an individual in the absence of a warrant or probable cause becomes illegal once a person is *forcibly removed* from his or her home or other place, brought to the police station, and detained for investigation without judicial supervision.[76]

Based upon the holdings in *Davis* and *Hayes*, citizens' reasonable expectations of privacy in their fingerprints is actually much lower than the general consensus might demand. The Southern District of New York suggested that fingerprinting is a minimally

---

[70] *Id.*

[71] *See* Hayes v. Florida, 470 U.S. 811, 812–13, 816 (1985).

[72] *Id.* at 813.

[73] *Id.* at 816.

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

[75] *Id.* (emphasis added) (quoting Adams v. Williams, 407 U.S. 143, 146 (1972)).

[76] *Id.*

invasive technique of identification that may actually prevent law enforcement abuse and produce more reliable, accurate results.[77] The overarching theme presented by the court is that law enforcement must have a warrant to seize one's person to obtain fingerprints, but how might this apply to individuals who are already lawfully detained in an airport context?[78] Assuming arguendo that those individuals in airport security screening are not lawfully detained, might those checkpoints fall into the "narrowly defined circumstances" that may allow fingerprinting even though there is not probable cause in the "traditional sense"? With current technology, it is possible to take someone's fingerprint *in the field,* and with *limited detention*, as fingerprint scans can be done in a matter of seconds. It is likely that the narrow exceptions carved out by the Supreme Court could be satisfied, and thus, there would be no implication of Fourth Amendment rights. However, to fully examine the issue of fingerprinting as a means of airport security, this comment will analyze whether it would be possible to implement such a procedure even if the Fourth Amendment did apply.

B. The Fourth Amendment and Airports: Competing Interests

In order to understand how the TSA may implement biometric technology into the existing security screening process, it is important to understand how the current screening methods are legally justified. While it may be apparent that airport searches invade one's reasonable expectation of privacy through the use of metal detectors, body scanners, and pat-downs, courts have consistently upheld airport searches under various exceptions to the warrant requirement such as reasonableness, consent, and the administrative search doctrine.[79] The following sections present the boundaries of one's Fourth Amendment rights and how they have been applied in the context of airport security.

---

[77] Thom v. N.Y. Stock Exch., 306 F. Supp. 1002, 1009 (S.D.N.Y. 1969).

[78] *See id.*

[79] The Supreme Court has not explicitly stated which justification suffices, but it has indicated that the government properly supported its governmental interest in seeking to uphold administrative searches by giving as an example airport security screenings. "The point is well illustrated also by the Federal Government's practice of requiring the search of all passengers seeking to board commercial airliners, as well as the search of their carry-on luggage, without any basis for suspecting any particular passenger of an untoward motive." Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 675 n.3 (1989).

1. Has a Search Taken Place?

The Fourth Amendment protects individuals' rights to "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[80] In *Katz v. United States*, the Supreme Court laid out the boundaries of the Fourth Amendment and the warrant requirement.[81] Justice Stewart stated that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection."[82] To determine the reasonableness of searches, subsequent courts have applied Justice Harlan's two-prong test from *Katz*, which requires that (1) a person have a subjective expectation of privacy; and (2) members of society are willing to accept that expectation of privacy as reasonable.[83] Thus, when one has an expectation of privacy that society would be willing to accept as reasonable, a warrant is required to search.[84] Alternatively, when no search has taken place, the government is not required to have a warrant.[85]

The Supreme Court recently reexamined its position on whether a search has occurred under the Fourth Amendment in *United States. v. Jones*.[86] The Court held that a trespass by government agents with the *intent to obtain information* constituted a search, and thus their actions required a warrant under the Fourth Amendment.[87] There, the defendant was under investigation by the FBI.[88] The government received a warrant to place a global positioning system tracking device on the vehicle of Jones's wife in D.C within ten days.[89] However, the government placed the tracker on the vehicle eleven days later in Maryland.[90] The Supreme Court heard the case to determine

---

[80] U.S. CONST. amend. IV.
[81] Katz v. United States, 389 U.S. 347, 351 (1967).
[82] *Id.*
[83] *Id.* at 361.
[84] *See id.*
[85] *Id.*
[86] United States v. Jones, 132 S. Ct. 945, 951 (2012).
[87] *Id.*
[88] *Id.* at 948.
[89] *Id.*
[90] *Id.*

whether the warrantless use of the tracker violated the Fourth Amendment.[91] Justice Scalia opined that the government occupied private property to get information, and while the occupation alone would not be an invasion of privacy, the intent of the government to obtain geographic information impeded the defendant's reasonable expectation of privacy.[92] Rather than narrow the holding in *Katz*, the Court added this additional requirement that one must first examine whether a trespass has occurred with the intent to gain information, and if not, the reasonable expectation of privacy standard remains.[93]

Directly tied to the use of private, personal information in the airport security context is Justice Alito's concurring opinion in *Jones*.[94] Alito added that *pervasive and prolonged* surveillance of a citizen's activities may constitute a search, even if that surveillance occurs in a public place.[95] Without specifically identifying what constituted a prolonged surveillance, Justice Alito noted that the tracking of the vehicle's movements in *Jones* for four weeks surely crossed that threshold.[96] Alito supported this argument by recalling the past securities afforded by individuals:

> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.[97]

Consider these comments in the context of implementing greater identification standards in airport security. It may be just as easy to track one's movements through the logs used for the biometric identifiers associated with particular individuals.[98] Surely the scanning of 660 million travelers constitutes a *pervasive* search in the grand scheme of things.[99] However, proper

---

[91] *Id.* at 949.

[92] *Id.* at 950–51.

[93] *See id.* at 951–52.

[94] *Id.* at 957 (Alito, J., concurring).

[95] *Id.* at 964.

[96] *Id.*

[97] *Id.* at 963.

[98] *See infra* Part III.C for discussion on the privacy rights of individuals and the use of fingerprint technology.

[99] *See TSA: Security Gaps*, *supra* note 3 (TSA Administrator Peter Neffenger stated that 660 million travelers were screened by TSA in 2014).

security techniques, encryption, and privacy protocols would minimize the risk of an intrusion by the government.

2. Exceptions to the Fourth Amendment

The Fourth Amendment protects one's person and possessions against *unreasonable* search and seizure, and there must be probable cause for a warrant to issue.[100] Thus, in determining the constitutionality of each facet of the Fourth Amendment, the Court has carved out exceptions to the Fourth Amendment requirements through legal vehicles such as reasonableness, consent, and the administrative search doctrine. Each exception focuses largely on the reasonableness of the search.[101] The means by which courts have previously justified *physical searches* of individuals and how these applications could be applied to mere fingerprint data are discussed below. The following sections outline the major turning points in court decisions.

a. Consent

The first court to rule on airport security screenings in 1973, in *United States v. Davis*, focused primarily on the balancing of the needs of the individual and the government.[102] In 1971, the defendant attempted to pass through airport security at San Francisco International Airport with a gun in his briefcase.[103] At the gate, an airline employee told him that a routine security search was needed. The employee then proceeded to take Davis's briefcase, open it, and discover a gun.[104] In a quote that exemplifies the current conditions of air travel, the Ninth Circuit stated that "[t]he search of appellant's briefcase was not an isolated event. It was part of a nationwide anti-hijacking program conceived, directed, and implemented by federal officials in cooperation with air carriers."[105] However, the court stated that a balancing regime based upon the premise that the searches conducted in airports at that time were based upon a "general regulatory scheme in furtherance of an administrative purpose, rather than as part of a criminal investigation."[106]

---

[100] *See* U.S. CONST. amend. IV.

[101] *See, e.g.*, United States v. Davis, 482 F.2d 893, 910 (9th Cir. 1973), *overruled in part by* United States v. Aukai, 497 F.3d 955 (9th Cir. 2007).

[102] *See id.* at 912–13.

[103] *Id.* at 896.

[104] *Id.*

[105] *Id.* at 897.

[106] *Id.* at 908.

The Ninth Circuit summarily defined the boundaries of the administrative search doctrine within the airport security context to be reasonable if "(1) it is no more extensive or intensive than necessary, *in light of current technology*, to detect weapons or explosives; (2) it is confined in good faith to that purpose; and (3) passengers may avoid the search by electing not to fly."[107] Thus, the court found that the search was constitutional without a warrant because the danger to air travel was "grave and urgent" and the potential damage to property, persons, and air travel was great.[108] However, the ability of an individual to choose not to fly was imperative, as the reasonableness requirement of the administrative search could only be satisfied if the intrusiveness of the search could be matched with the need that justifies it.[109]

Other courts relied upon this notion and modified it, holding that a person subjected to a search has impliedly consented by choosing to board with the knowledge of widespread air piracy and notices of airport security measures.[110] But by 2007, the Ninth Circuit overruled the holding that passengers may "consent" because "requiring that a potential passenger be allowed to revoke consent to an ongoing airport security search makes little sense in a post-9/11 world. Such a rule would afford terrorists multiple opportunities to attempt to penetrate airport security by 'electing not to fly' on the cusp of detection until a vulnerable portal is found."[111] Thus, while *Davis* was initially an attempt to apply an administrative search regime, subsequent courts refuted the notion that consent was a necessary factor, causing the test to rely only upon the balancing of interests and underlying motive.[112]

b. Administrative Search Doctrine

To this day, the Supreme Court has not explicitly professed the appropriate Fourth Amendment rationalization regarding airport security screening, but it has alluded to the administrative search doctrine as being the leading constitutional justifica-

---

[107] United States v. Marquez, 410 F.3d 612, 616 (9th Cir. 2005) (emphasis added).

[108] *Davis*, 482 F.2d at 910.

[109] *Id.*

[110] United States v. Dalpiaz, 494 F.2d 374, 376 (6th Cir. 1974).

[111] United States v. Aukai, 497 F.3d 955, 960–61 (9th Cir. 2007).

[112] *See id.* at 961–62.

tion.[113] In 1987, the Supreme Court decided the watershed case on the administrative search doctrine, *New York v. Burger*, which has defined administrative searches for all subsequent analyses.[114] In *Burger*, state regulatory statutes allowed warrantless searches of automobile junkyards as an exception to the Fourth Amendment warrant requirement in an attempt to deter criminal behavior.[115] The holding postulated that warrantless searches of heavily regulated industries without probable cause were constitutional because those industries had lower expectations of privacy, which, paired with the substantial governmental interest, outweighed the invasion of privacy.[116] The balancing scheme laid out by the Supreme Court took into account (1) the substantial governmental interest that informs the regulatory scheme; (2) whether the warrantless inspection was necessary to further the regulatory scheme; and (3) whether the regulatory scheme was a constitutionally adequate substitute for a warrant.[117]

In 1989, Justice Kennedy compared the *Von Raab* case in which the court applied a balancing of government and individual privacy rights with that of the airport screening process.[118] In *Von Raab*, the Court decided a special needs case in which certain U.S. Customs workers were drug tested as a job requirement. The pertinent factors considered by the Court were that the tests were not turned over to law enforcement, applying for a government position was enough to expect a lower expectation of privacy, and that the government had an interest in ensuring front line personnel are of high integrity and are physically fit.[119]

> The point is well illustrated also by the Federal Government's practice of requiring the search of all passengers seeking to board commercial airliners, as well as the search of their carry-on luggage, without any basis for suspecting any particular passenger of an untoward motive. Applying our precedents dealing with administrative searches, *see, e.g.*, *Camara v. Municipal Court of San Francisco*,[120] the lower courts that have considered the question

---

[113] *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 675 n.3 (1989).
[114] *See* New York v. Burger, 482 U.S. 691 (1987).
[115] *Id.* at 693.
[116] *Id.* at 711–12.
[117] *Id.* at 702–03.
[118] *Von Raab*, 489 U.S. at 675 n.3.
[119] *Id.* at 679.
[120] 387 U.S. 523, 535 (1967). In *Camara*, the Court used a balancing approach very similar to that seen in *Burger* and simply applied that balancing of personal

> have consistently concluded that such searches are reasonable under the Fourth Amendment.[121]

Likewise, in 1997, the Court again suggested that the administrative search doctrine was indeed the appropriate standard to apply in airport screening.[122] In *Chandler v. Miller*, the Court considered whether candidates for public office in Georgia could be ordered by state law to submit to drug-screening before filing for candidacy.[123] In deciding the case, the Court examined the government interest—effective administration—paired with the privacy interest of politicians.[124] The Court ultimately determined that because politicians are constantly in the public light, the government interest did not outweigh the privacy interests of politicians to mandate drug-testing.[125] However, in doing so, the Court again compared the case with administrative searches in the airport screening context because they directly impacted public safety.[126] As Justice Ginsburg aptly stated,

> Where the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as "reasonable"—for example, searches now routine at airports and at entrances to courts and other official buildings. But where, as in this case, public safety is not genuinely in jeopardy, the Fourth Amendment precludes the suspicionless search, no matter how conveniently arranged.[127]

The lower courts are also adopting the administrative search doctrine, but without the concern of traveler consent.[128] In 2011, the D.C. Circuit upheld a Fourth Amendment challenge under the administrative search doctrine in which the court held that the use of body scanners was constitutional.[129] The court was persuaded by other circuits and the suggestions of the Supreme Court in holding that "screening passengers at an airport is an 'administrative search' because the primary goal is not to determine whether any passenger has committed a crime but

---

privacy and governmental interest to safety inspections of homes without a warrant issued on probable cause as part of a regulatory scheme for public safety.

[121] *Von Raab*, 489 U.S. at 675 n.3.

[122] *See* Chandler v. Miller, 520 U.S. 305, 309 (1997).

[123] *Id.* at 308.

[124] *Id.* at 318.

[125] *Id.* at 321.

[126] *Id.* at 323.

[127] *Id.* (citations omitted).

[128] *See* Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1, 10 (D.C. Cir. 2011); United States v. Aukai, 497 F.3d 955 (9th Cir. 2007).

[129] *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

rather to protect the public from a terrorist attack."[130] In balancing the interests of individuals and the government interest for public safety, the court held that the intrusion upon individual privacy was necessary for the promotion of "legitimate governmental interests."[131]

But in consideration of the indisputably invasive body scanner technology, the court stated that the body scanner was a crucial technological advancement as it could not only detect guns and weapons, but also liquids and explosives, which greatly outweighed the individual privacy concerns.[132] Passenger privacy was deemed protected by a facial distortion on all images produced by the body scanners, deleting it as soon as the passenger was cleared.[133] Additionally, and ironically, the court held that the privacy interests of individuals were also protected because any passenger may opt out of the body scanner search "in favor of a patdown."[134] This opt out option of course begs the question, does that mean that consent *is* still a factor? The answer being, of course, that consent is likely a factor in the *reasonableness* of the administrative search, but it is not a dispositive factor in the constitutionality of the search. Thus, in the D.C. Circuit's eye, a Hobson's choice is, nevertheless, still a choice.

IV. ANALYSIS AND DISCUSSION

As the *Davis* court poignantly stated, "[l]ittle can be done to balk the malefactor after such material [explosive or weapon] is successfully smuggled aboard, and as yet there is no foolproof method of confining the search to the few who are potential hijackers."[135] Nearly half a century has passed since the *Davis* court decision, but the same concerns for air safety are still present and real. To confront the terror that existed on September 11, 1970, the Court implemented what was at that time an invasion of privacy—metal detectors.[136] But by the late 2000s, the implementation of an even greater physical invasion of privacy was implemented: advanced imaging technology body scanners. The public consensus at each introduction of security technol-

---

130 *Id.*

131 *Id.*

132 *Id.*

133 *Id.*

134 *Id.*

135 United States v. Davis, 482 F.2d 893, 910 (9th Cir. 1973), *overruled in part by* United States v. Aukai, 497 F.3d 955 (9th Cir. 2007).

136 *See id.*

ogy has been disdain and uneasiness, but with each successive advancement comes the potential for a subtle inoculation to the public's senses.

In the current world of metadata, each small invasion of personal privacy has resulted in an inoculation by a million encroachments, rather than death by a million slices. Courts have upheld the constitutionality of technology that scans one's body with such detail that the TSA subsequently implemented technology to blur facial features and private areas for the officer who views the image in a private screening room.[137] This technology that allows a TSA officer to know your body a bit better than you do was supported by more than eighty percent of Americans in 2010.[138] With this in mind, is the average American ready, willing, and able to provide a fingerprint to take to the skies? With hesitation, maybe. Are the courts ready, willing, and able to require fingerprints to take to the skies? Likely. If the TSA required travelers' fingerprints to board a plane, it would likely satisfy the current precedent. A fingerprint submission is arguably far less invasive than the information obtained from a body scanner. As such, the law is ripe for discussion regarding the legal boundaries and the personal privacy concerns in light of the current technology.

A. Application of Fingerprint Technology in Current Airport Screening

Lest you disagree with the Supreme Court, fingerprinting is considered a *less invasive* intrusion into one's right to be let alone.[139] The Supreme Court offered that a "brief detention in the field for the purposes of fingerprinting" with only reasonable suspicion is not necessarily impermissible under the Fourth Amendment.[140] Of course, the *Davis* and *Hayes* cases were decided in the 1960s and 1980s, respectively. Thus, it could be said that the Justices in those cases were unaware of the vast technological advancements, such as an iPhone that uses one's finger-

---

[137] Deema B. Abini, *Traveling Transgender: How Airport Screening Procedures Threaten the Right to Informational Privacy*, 87 S. Cal. L. Rev. Postscript 120, 125–26 (2014).

[138] Stephanie Condon, *Poll: 4 in 5 Support Full-Body Airport Scanners*, CBS News (Nov. 15, 2010, 6:56 PM), http://www.cbsnews.com/news/poll-4-in-5-support-full-body-airport-scanners/ [https://perma.cc/CZ33-ADKP].

[139] *See* Davis v. Mississippi, 394 U.S. 721, 727 (1969).

[140] *See* Hayes v. Florida, 470 U.S. 811, 816 (1985).

print as a password.[141] However, the opinions indicate quite clearly that fingerprints are not private because they are so openly obvious on an individual and left behind each place the individual visits and touches.[142] That said, *Davis* and *Hayes* are still deemed good law. Moreover, in *Katz*, Justice Williams discussed this point exactly by clearly stating that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[143]

Along those lines, fingerprints identify *who you are* and potentially *where you have been*, but not what you have done. Rationalize that with the understanding that the government can retrieve information voluntarily turned over to a third party, such as numerical data entered into or received on a phone, called a pen register.[144] The government need only obtain a subpoena or provider consent to obtain pen registers as those do *not* amount to a search.[145] Because fingerprints are left everywhere and only provide that a particular individual has been in a particular location, that surely has less potential criminality attached to it than to information regarding who an individual has talked to and for how long. Certainly communication records reveal more private and potentially incriminating information, and even there the government has a low bar to reach by a mere showing that the information sought is relevant to an ongoing criminal investigation![146] Even further, the Third Party Doctrine established in *United States v. White* states that information voluntarily overturned to third parties has no reasonable expectation of privacy.[147] The Third Party Doctrine has been extended to video surveillance,[148] financial records,[149] personal trash,[150] and even to overhead aerial surveillance.[151] Mere identification by means of a fingerprint surely amounts to a lesser expectation of privacy

---

[141] *About Touch ID Security on the iPhone and iPad*, APPLE, https://support.apple.com/en-us/HT204587 [https://perma.cc/X8EJ-XXHJ].

[142] *See Hayes*, 470 U.S. at 812–13.

[143] Katz v. United States, 389 U.S. 347, 351 (1967).

[144] Smith v. Maryland, 442 U.S. 735, 744–45 (1979).

[145] *Id.* at 745–46; *see* Electronic Communications Privacy Act of 1986, 18 U.S.C. § 3121.

[146] *See* 18 U.S.C. § 3123.

[147] United States v. White, 401 U.S. 745, 751 (1971).

[148] United States v. Gonzalez, 328 F.3d 543, 546 (9th Cir. 2003).

[149] United States v. Miller, 425 U.S. 435, 440 (1976).

[150] California v. Greenwood, 486 U.S. 35, 37 (1988).

[151] Florida v. Riley, 488 U.S. 445, 451–52 (1989).

than one's financial records and aerial surveillance, both of which may be obtained by the government without a warrant.

Because fingerprinting is merely a means of identification, courts have attempted to refute any other holding, going so far as to state "the public has long recognized [fingerprinting] as a valuable and reliable means of identification, and to suggest that a stigma attaches when it is so used is to fly in the face of reality."[152] Therefore, implementing fingerprint scanning to travel via air likely does not implicate the Fourth Amendment and would be constitutionally permissible if it were to be implemented today. However, to further emphasize how the implementation could be allowed *even if it did amount to a search*, the following reviews the implementation under the assumption that a search has occurred under the *Jones* or *Katz* standard.[153]

Under the *Jones* test, the use of a fingerprint at the airport would not be deemed a search because there is no intent of the government to obtain information, but rather the government seeks mere identification.[154] Additionally, the information obtained through a fingerprint would be no more of a requirement than the current use of a driver's license and a boarding pass—identification.[155] It could be stated that Justice Alito's concurrence in *Jones* could pertain to such use of fingerprints because it would amount to a pervasive and prolonged search due to the sheer *amount* of fingerprints that the TSA would be screening.[156] However, this argument fails on at least two grounds. While *Jones* was not an exceptionally narrow holding, it was limited to physical intrusions to obtain personal information.[157] While it is true that consent is not necessary under the current administrative search justification, if fingerprint submissions were mandated, courts may determine that travelers consented to their fingerprint being used and have thus waived their right to Fourth Amendment privacy, much as courts have held in prior case law.[158] Secondly, *Jones* stands for technology used to obtain *personal* information about an individual.[159]

---

[152] Thom v. N.Y. Stock Exch., 306 F. Supp. 1002, 1009 (S.D.N.Y. 1969).

[153] *See* United States v. Jones, 132 S. Ct. 945, 964 (2012); Katz v. United States, 389 U.S. 347 (1967).

[154] *Jones*, 132 S. Ct. at 951.

[155] *See Identification*, *supra* note 19.

[156] *See Jones*, 132 S. Ct. at 964.

[157] *See id.* at 949.

[158] *See* United States v. Aukai, 497 F.3d 955, 961–62 (9th Cir. 2007).

[159] *See Jones*, 132 S. Ct. at 949.

Courts have appropriately indicated that fingerprint information is neither personal nor requiring of special treatment.[160]

Because there may or may not be a physical intrusion by the government to obtain personal information from an individual, a search must be examined under the two-part *Katz* analysis. Application of Harlan's concurrence in *Katz* easily leads one to the conclusion that individuals do in fact have a reasonable expectation of privacy in their fingerprints, but is society willing to accept that privacy interest as reasonable?[161] Today, society views a fingerprint as uniquely personal and, as such, deserving of privacy. In stark contrast, dated precedent indicates that a fingerprint is not as personal and private as some believe.[162] Thus, under *Katz*, it is quite likely that fingerprinting an individual amounts to a search due to societal expectations. However, even assuming that it does amount to a search, the exceptions outlined in *Davis* and *Hayes* could surely be satisfied.[163] Because the Court emphasized that a brief detention in the field in which there is only reasonable suspicion would not necessarily be impermissible, this use of a fingerprint may also be deemed reasonable, notwithstanding the fact that it is indeed a search under *Katz*.[164]

Just as previous airport screening techniques have been justified under the administrative search doctrine, a requirement that one submit a verified fingerprint to the TSA, the airlines, or both prior to boarding a plane falls squarely within the administrative search exception as well. Therefore, even if a search is found under the *Jones* or *Katz* tests, fingerprinting would still be permissible under the current use of the administrative search doctrine.

First, consider the test laid out in *United States v. Aukai*, where the Ninth Circuit stated that an airport screening search is constitutional so long as it is "no more extensive nor intensive than necessary, *in light of the current technology*, to detect the presence of weapons or explosives and that it is confined in good faith to that purpose."[165] As previously discussed, this standard is appli-

---

[160] *See* Hayes v. Florida, 470 U.S. 811, 816 (1985); Davis v. Mississippi, 394 U.S. 721, 727 (1969).

[161] *See* Katz v. United States, 389 U.S. 347, 360–62 (1967).

[162] *See Hayes*, 470 U.S. at 816; *Davis*, 394 U.S. at 727.

[163] *See Hayes*, 470 U.S. at 816; *Davis*, 394 U.S. at 728.

[164] *See Hayes*, 470 U.S. at 816.

[165] United States v. Aukai, 497 F.3d 955, 962 (9th Cir. 2007) (emphasis added) (internal alterations omitted) (citing United States v. Davis, 482 F.2d 893, 913

cable for the *tangible threats* that may be deterred by searches. The use of biometric data does not fall into that category, but even if considered an invasive search, the inconvenience suffered by travelers would be so minute that submitting fingerprint data would hardly tip the scale toward the invasion being more extensive or intensive than necessary.[166] Just as fingerprints surely evoke a lesser expectation of privacy than financial records or cell phone records, it is doubtful in today's data-driven market that one would consider a fingerprint scan as invasive as a body scan.[167]

Courts have upheld the administrative search exception so long as the search is part of a regulatory scheme that furthers the interest of the government by preventing the carrying of explosives or weapons onboard without overstepping the boundaries of personal privacy.[168] While biometric data would not prevent the carrying of explosives or weapons *directly*, it would indirectly prevent travelers on the No Fly List from gaining access to air travel, with or without explosives or weapons. The potential for harm coming from known threats who are already placed on a No Fly List is substantial, regardless of whether that person is also carrying weapons or explosives.[169] More importantly, because the current method of simply confirming one's identity through a photo identification and boarding pass can be so easily fooled or forged,[170] fingerprinting tips the scale in favor of reasonableness. The individual privacy invaded by a fingerprint submission would again be *de minimis* compared to that of the highly invasive body scanner, especially in comparison to the governmental and societal interest served—personal and national security.[171]

(9th Cir. 1973), *overruled in part by* United States v. Aukai, 497 F.3d 955 (9th Cir. 2007)).

166 *See Hayes*, 470 U.S. at 816; *Davis*, 394 U.S. at 727–28.

167 *See* Abini, *supra* note 137, at 125–27 (discussing the invasive nature of body scanning technology and the requirements TSA implemented to mitigate the intrusion).

168 *See Aukai*, 497 F.3d at 960.

169 For instance, consider Malaysian Airlines Flight 370, where two passengers boarded the plane using stolen passports. While only speculation may arise from that incident, fingerprint identification could prevent these gaps in the screening process. *See supra* note 12 and accompanying text.

170 *See* Pryce, *supra* note 13.

171 For instance, consider that a known terrorist would probably not attempt to board a plane without taking precautions to shield their identity through disguise and false identification.

B. Privacy Interests and Problems

The biggest hindrance to the TSA's implementation of fingerprint scanning in lieu of one's boarding pass and photo identification is simply personal privacy. While aged precedent may suggest that a fingerprint is merely an identifier, society may not quite conform to that notion—at least not yet. However, fingerprint data has become a key identifier across many platforms, including Visa applications.[172] Currently, to enter the United States, the mantra of the Department of State is "secure borders, open doors," which is indicative of its requirement that all incoming foreigners must submit ten fingerprints.[173] The catch? Biometric data is only taken on *incoming* Visa holders.[174] Foreign nationals who wish to enter our country are clearly subjected to a lower expectation of personal privacy than we personally accept as reasonable to be part of our society. But with the growing threat of homegrown terrorists and radicals, now is the time to consider that instead of reducing our expectation of privacy, we must demand greater standards of identification for all.[175] Thus, if biometric data is to be implemented, it should apply not only to incoming foreign flights, but also to outgoing and domestic flights as well.

The possibility of a slippery slope of invasive activities and the short-term memory of society is obviously of great concern with each new security measure. Some authors have posited that we are now in an age of "micro-police state[s]," where airport security measures result in an erosion of societal expectations, namely privacy.[176] In a discussion of TSA's PreCheck program, one author even stated "[p]ublic memory is often short, and citizens frequently become desensitized to government privacy invasions, particularly ones that are deemed necessary for national security."[177] However, fingerprint submissions to the government have not necessarily been met with hesitation by all. At the

---

[172] *Safety & Security of U.S. Borders: Biometrics*, U.S. Dep't of State, https://travel.state.gov/content/visas/en/general/border-biometrics.html [https://perma.cc/DUK3-DM3P].

[173] *Id.*

[174] *Id.*

[175] *See* Carrie Blackmore Smith & Joel Beall, *Number of Homegrown Terrorists is Rising*, USA Today (Jan. 17, 2015, 10:23 PM), http://www.usatoday.com/story/news/nation/2015/01/17/number-of-homegrown-terrorists-is-rising/21940159/ [https://perma.cc/CV65-9LHA].

[176] Roger Clark, *The Inalienable Right to Fly*, L.A. Law., Sept. 2006, at 60.

[177] See Katie Cristina, Comment, *The TSA's New Precheck Is Beginning to Look A Lot Like Capps II: The Privacy Implications of Reviving the Tenets of the Failed Predeces-*

publication of this comment, more than four million people have registered for TSA PreCheck.[178] PreCheck enrollment requires submission of biographic information, an eighty-five dollar fee, *and* fingerprints to receive a rapid screening process at the airport.[179] While four million is a small drop in the bucket compared to the entire population of travelers, the fee associated with PreCheck is nearly the same price as a direct flight from Dallas/Fort Worth Airport to Los Angeles International Airport. Given the chance as part of their ticket price, would people be willing to submit fingerprints that would be kept for only a short period to verify their identity? Voluntary enrollment into TSA PreCheck indicates that may or may not be an answer in the affirmative.

It has further been posited that because the Fourth Amendment exceptions are satisfied by such a low threshold in the sake of fighting terrorism, the only true means of personal protection is through the democratic process.[180] Thus, the fear driven mentality of the citizenry may feel that the use of programs such as TSA PreCheck and the laws surrounding airport security screening will allow the implementation of just about any newfangled interdiction effort.[181] However, arguments along those lines are inapplicable to fingerprinting as a part of airport screening, even outside of Fourth Amendment scrutiny

First, the fingerprints would be rapidly taken in the field, as the goal of TSA is to have a fast-moving, free-flowing security checkpoint, and thus the Fourth Amendment would not be implicated.[182] The technology currently exists and could easily be implemented into airports within the boundaries previously laid out by the Supreme Court.[183] Second, fingerprinting at the airport would in no way invoke the other factors considered in *Hayes* and *Davis* like forcible movement to the police station or police interrogation.[184] Lastly, fingerprints are commonly required throughout many fields. All members of the security ex-

---

sor, 78 J. AIR L. & COM. 617, 648 (2013). The author's comment was referring to the implementation of PreCheck, which is a voluntary program.

178 *TSA Pre✓®*, TRANSP. SEC. ADMIN., https://www.tsa.gov/precheck/ [https://perma.cc/538D-JMS9].

179 *Id.*

180 *See* Cristina, *supra* note 177, at 648.

181 *See id.* at 649.

182 *See* Davis v. Mississippi, 394 U.S. 721, 727 (1969).

183 *Id.*; *see* Hayes v. Florida, 470 U.S. 811, 817 (1985).

184 *See Hayes*, 470 U.S. at 816; *Davis*, 394 U.S. at 728.

change must be fingerprinted,[185] lawyers must submit fingerprints for application to the bar,[186] and some states require that bartenders, day care workers, and even real estate workers must submit fingerprints.[187] Fingerprinting across those fields is necessary as a means of identification and fraud prevention, and usage of fingerprinting should be no different for such an elective means of travel.

C. Necessary Protections

The potential for a government too bent on national security at the expense of personal privacy and autonomy is certainly at the edge of everyone's mind. Thus, while airport security screening falls squarely into the administrative search doctrine, to fully satisfy the public and coax the privacy needs of individuals, implementation of fingerprint scanning will require several protections. Requiring individuals to submit fingerprints before flight to confirm their identity, and again to confirm their identity at the security checkpoint, requires a delicate *Burger* analysis and special needs balancing of an individual's right to feel let alone and that of the government interest—public safety.[188] In order to have a qualified fingerprint upon which to reference travelers as they pass through security checkpoints, the TSA will likely need to implement fingerprinting offices at airports or privately contracted offices. This process could follow similar protocols as those currently used with the TSA PreCheck program.[189] Additionally, because an "original" fingerprint would necessarily need to be stored as a reference point, there are necessary protections to ensure individual privacy, security of data, and peace of mind. Therefore, three issues must be addressed: (1) law enforcement limitations; (2) temporal limitations; and (3) spatial limitations.

First, collection of fingerprint data from individuals prior to flight must be stored so that it can be accessed later to confirm the identity of the individual. Of utmost importance is that the

---

[185] Achraf Farraj, *Refugees and the Biometric Future: The Impact of Biometrics on Refugees and Asylum Seekers*, 42 Colum. Hum. Rts. L. Rev. 891, 925 (2011).

[186] *Fingerprint Information*, Tex. Board L. Examiners, https://ble.texas.gov/fingerprint-information [https://perma.cc/NVE7-LXKA].

[187] Farraj, *supra* note 185, at 925.

[188] *See* New York v. Burger, 482 U.S. 691, 702–03 (1987).

[189] *TSA Pre✓®*, *supra* note 178 (indicating that one need only locate an enrollment center, make an appointment, and bring a birth certificate and driver's license, or a passport, to have fingerprints and a small interview conducted).

fingerprints collected are used to *identify*, not penalize, travelers. In *Von Raab*, the Supreme Court upheld drug testing of specific classes of U.S. Custom's workers based upon several factors, but of importance was that the information received from the drug tests was not turned over to law enforcement.[190] Thus, all fingerprint data obtained by the TSA or airlines in any implemented fingerprint identification scheme must be placed under seal and made inaccessible to law enforcement agents. This, of course, begs the question, what of the terrorists that are identified? One must remember that the goal of implementing fingerprint identification is merely confirmation of identity and alternatively that those individuals that may be identified through the No Fly List may or *may not* be subject to criminal prosecution independent of their predicted threatening nature.[191] Law enforcement agents may not arrest individuals for their potential to commit crimes, lest we enter into a world similar to that of *The Minority Report*.

Second, because the threat of data breach is a grave problem that requires proactive rather than reactive measures, the length of time the fingerprint data should be stored must be balanced with this risk.[192] The government interest of public safety lies in properly identifying individuals, but that requires having a fingerprint comparison on file. Currently, biometric data stored for asylum seekers and refugees is stored for seventy-five years, but as some have professed, the duration of storage must be as short as necessary.[193] An opt-out feature of sorts should also be implemented, in which individuals are allowed to withdraw their fingerprint data from storage with a confirmation of deletion sent to the requesting individual. This ensures that individuals who wish to fly can submit fingerprints, travel, and then subsequently remove their fingerprints from the database with the only caveat being that they must repeatedly submit qualifying biometric information before a future flight. Because of the risk

---

[190] Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 678–79 (1989).

[191] Lowe, *supra* note 36, at 159.

[192] *See* Robert Hackett, *Massive Federal Data Breach Affects 7% of Americans*, TIME (July 9, 2015), http://time.com/3952071/opm-data-breach-federal-employees/ [https://perma.cc/RM97-7CYQ].

[193] Farraj, *supra* note 185, at 933.

of data breaches, necessary encryption of all stored fingerprint data must be implemented as well.[194]

Lastly, because fingerprint data would be used at each security checkpoint through which a traveler passes, it would be easy to keep a record of geographic history. But again, the government interest is in public safety, which necessarily begins with confirmatory identification as a means of threat prevention, and not law enforcement. To remedy the problem of geographic tracking, the fingerprint that is taken at each checkpoint should be deleted after the traveler has been cleared at the security checkpoint, much like the current procedure calls for in the images produced from body scanners.[195] Thus, while the original fingerprint submission is maintained as a reference point, the airport security checkpoint is merely a cross-reference with a short shelf-life. Alternatively, if it is found that law enforcement agencies or the TSA has stored, tracked, or monitored the travel of individuals by their fingerprints, judicial scrutiny would be necessary as broad sweeping surveillance of such a large amount of data would fall within the pervasive government search coined by Justice Alito.[196] Thus, individuals' fingerprints would necessarily be safeguarded by the affirmative measure of deleting all point of entry fingerprints and through judicial scrutiny into any breach of such protocol under *United States v. Jones*.[197]

D. Safety and the Benefits of Fingerprinting

The overarching theme of the TSA, the government, and even the courts in examining airport security checkpoints is *safety*.[198] The circuit courts have justified,[199] and the Supreme Court has mentioned, that it too has justified airport searches under the administrative search doctrine,[200] likely because the

---

[194] *See* Hackett, *supra* note 192. Note that an entire article could be devoted to what would be an appropriate level of encryption and protection of individuals' fingerprints.

[195] *See* Tobias W. Mock, *The TSA's New X-Ray Vision: The Fourth Amendment Implications of "Body-Scan" Searches at Domestic Airport Security Checkpoints*, 49 Santa Clara L. Rev. 213, 230 (2009).

[196] *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

[197] *See id.*

[198] *TSA Efforts*, *supra* note 8.

[199] *See* Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., 653 F.3d 1, 10 (D.C. Cir. 2011); United States v. Marquez, 410 F.3d 612, 616 (9th Cir. 2005); United States v. Davis, 482 F.2d 893 (9th Cir. 1973), *overruled in part by* United States v. Aukai, 497 F.3d 955 (9th Cir. 2007).

[200] *See* Chandler v. Miller, 520 U.S. 305, 323 (1997).

overarching threat of air safety was so grave. But as stated earlier, no exception is needed for fingerprints as precedent and scholars pointedly assert.[201] Thus, the true cusp of safety starts with *identifying the threat.* The threat need not be a gun, explosive, or any tangible object, but merely a person who poses a significant threat to society. Government agencies already compile lists of these individuals in an attempt to combat this problem,[202] but the current methods of identifying travelers to positively identify threatening *people* are too weak, too easily fooled.[203] Because the No Fly list operates merely on biographic data, fingerprint data would create a cohesive scheme of air safety that combines the current data used for the No Fly list with the fingerprints supplied by travelers wishing to fly.[204] Lastly, as a means of proactive threat interdiction, requiring a fingerprint might deter would-be terrorists, as forging a fingerprint is a much greater task than simply a photo identification and boarding pass.

V. CONCLUSION

For some, air travel is almost a daily or weekly event, for others perhaps merely for vacation, but for all it is a concern. Society is concerned about the safety of flying, the hassle of security, and the loss of many liberties simply by visiting a family member or traveling for work. Air travel has been a means of terror for nearly four decades now, and the time is ripe for advancements not only in the security screening, but also in the threat identification. Threat prevention starts with traveler identification. Because technology has advanced to allow for fast, easy, and minimally invasive scanning of fingerprints, the law should keep to its word. The Supreme Court has spoken and as such deemed one's fingerprint to be merely a means of identification and thus, there is no need to carve or pry for exceptions under the Fourth Amendment. The law is ready to accept fingerprinting as a means to identify and prevent threats and with the advances in technology, perhaps society's views may shift in the coming years to match that of precedent.

---

[201] *See* Hayes v. Florida, 470 U.S. 811, 816–17 (1985); Davis v. Mississippi, 394 U.S. 721, 727–28 (1969); David H. Kaye, *A Fourth Amendment Theory for Arrestee DNA and Other Biometric Databases*, 15 U. PA. J. CONST. L. 1095, 1139 (2013).

[202] Lowe, *supra* note 36, at 159.

[203] Fishel et al., *supra* note 6.

[204] Lowe, *supra* note 36, at 159–60.