2016

Privacy Concerns Regarding the Use of Biometrics in Trusted Traveler Programs

Shari Merlano
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Shari Merlano

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Heather Mbaye, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Tim Bagwell, Committee Member,
Public Policy and Administration Faculty

Dr. Tanya Settles, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2016

Abstract

Privacy Concerns Regarding the Use of Biometrics in Trusted Traveler Programs

by

Shari Merlano

M.A., International Relations, American Public University, 2010

B.A., Political Science, University of Central Florida, 2006

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

December 2016

Abstract

One of the objectives of the U.S. government is to balance the individual's right to privacy and national security interests. Trusted Traveler programs create a risk-based security model where the traveling public is categorized into low or high risk. There are, however, some privacy concerns related to the acceptance of the use of biometric technology in the adoption of expedited security screening procedures in commercial airports. The theoretical construct of this case study of the TSA Pre-Check Program is based on Ajzen and Fischbein's theory of reasoned action, specifically through Davis' technology acceptance model. The purpose of this case study was to explore the perceptions of the traveling public regarding the protection of privacy and the use of biometric technologies. Data for this study included 325 social media postings, 50 privacy complaints reported to the Department of Homeland Security between 2009 and 2014, and publicly available data from the Government Accountability Office about expedited screening for the years 2011 – 2014. Data were coded into a priori themes and then subjected to a content analysis procedure. Findings indicate that the traveling public generally support expedited security screening and consent to waiving certain privacy rights in order to facilitate expedited screening. Complaints from travelers were also primarily related to wait times and secondary screening, and not privacy concerns. The positive social change implications stemming from this study include recommendations to the TSA to expand the Trusted Traveler programs such that the primary concern of the traveling public, reduction of wait time is balanced against privacy concerns about the collection of biometric data as part of a measured response to aviation security.

Privacy Concerns Regarding the Use of Biometrics in Trusted Traveler Programs

by

Shari Merlano

M.A., International Relations, American Public University, 2010

B.A., Political Science, University of Central Florida, 2006

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

December 2016

Dedication

This dissertation is dedicated to those individuals that have supported and guided me through this journey. Karen E. Hanlon, Rafael Serrano, David McCoy, Cheryl Calvert, Travis Hodge, and Kamaria Brown who for many days have encouraged me to continue on this journey. Denise Smith Allen, Ockeshia Christian, Sergio Montolio, and Dr. Lonnie Brinson, you all were my accountability partners to continue to write and guide me through this very frustrating process.

To the very special and caring Loretta Bates, whose energy and inspirational words have been my motivation and inspiration to continue to live life and making each and every dream come true. To Maria Jimena Browning, who through her guidance and coaching have provided me with many magical moments that have taken my breath away and taught me the true essence of humility, self-confidence, and unconditional love. These words are very small compared to the enormous gratitude I feel inside, leaving me once again, breathless!

Lastly, to my mother who has supported me in achieving this lifelong dream by helping me with the everyday things in life. I could not have done it without you all.

Acknowledgments

I would like to express my thanks and sincere appreciation to my dissertation committee chair, Dr. Heather Mbaye, who provided guidance and ensured that I was on track with meeting my objectives with this study. She brought out the passion within me to explore a topic that was challenging and influential in social change.

My second committee member, Dr. Tim Bagwell, who was passionate about the topic as he is a constant traveler and my Walden University Reviewers, Dr. Richard Box, Dr. Ian Bradsall, and Dr. Tanya Settles for their support, guidance, and assistance.

I would also like to thank the major contributions to those who helped me to conduct this study. I would like to acknowledge the support that Walden faculty and staff provided me in fulfilling this lifelong dream.

Most of all, I would like to thank Maria Jimena Browning for her love, support, and encouragement. She believed in me when I did not believe in myself. She coached me, rehearsed with me, provided constructive feedback, and even gave me a shoulder to cry on. I am thankful and blessed that she allowed me to share every bit of this process with her and through frustrating times was the anchor that kept me grounded.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Through the attacks on September 11, 2001, the United States and the world became aware of the reality of terrorism. Governments around the world created counter-terrorism measures to aviation security, as aviation was the chosen method by terrorist organizations to execute attacks due to its high media coverage. As a response to the terrorist attacks, the United States federal government passed and approved the U.S. Patriot Act of 2001 and the Aviation Transportation Security Act of 2001 (ATSA) enabling the creation of the Transportation Security Administration (TSA).

The ATSA established a new department that allowed for more communication and information sharing among different government agencies (TSA, 2013). In March 2003, two years after the creation of the TSA, the Department of Homeland Security (DHS) was created to supervise the TSA and Customs and Border Protection (CBP) which are the agencies entrusted with the implementation and management of Trusted Traveler programs (DHS, 2014).

Background of the Study

For a decade DHS and its agencies implemented a single model of screening for incoming and outgoing travelers in the United States and its territories. Through time and with congressional pressure, DHS sought innovative ways of conducting their operations as a result of budgetary cuts (TSA, 2009). In 2009, DHS introduced a series of Trusted Traveler programs that enable travelers to enroll in an expedited security screening experience within the United States and its territories. The TSA introduced a similar program in 2011 allowing frequent flyers the opportunity to pilot the program and set its implementation in 2013 (TSA, 2013).

In 2013, DHS agencies had fully implemented the Trusted Traveler Programs where enrollment is based on a traveler's background history, biometric collection, and acceptance of terms and conditions; with a renewal process at 5-year intervals (TSA, 2014). The DHS introduced biometrics into the expedited screening process for outgoing and incoming travelers to ensure citizen safety and freedom of commerce (9/11 Commission Report, 2004).

Trusted Traveler Programs are designed to target specific travelers and their needs. Global Entry is for the U.S. business traveler who often travels internationally and wants to speed through the lines upon entry into the United States and its territories (CBP, 2014). NEXUS is for the traveler who often travels to Canada for business or pleasure, SENTRI is for the traveler crossing between the United States and Mexico, and FAST is for the movement of shipping goods, provided that the company and driver are categorized as low risk (CBP, 2014).

These programs are administrated by CBP, which has agreements with other national governments such as Canada, Mexico, South Korea, Netherlands, Australia, and New Zealand to have enrolled travelers receive expedited security screening in those countries. Pre-Check is administered by the TSA and offers expedited security screening through commercial airports (TSA, 2013). The traveler has the option to enroll in any CBP program and will automatically receive entry into the TSA Pre-Check program as long as the traveler is flying with a participating airline carrier (CBP, 2014).

All of these Trusted Traveler programs include the capture of personal identification information (PII) such as biometrics to be used in the enrollment process. The collection, maintenance, use, and dissemination of PII is protected under the Privacy Act of 1974 and requires federal agencies to give public notice of their system of records by publication in the Federal Register; therefore, prohibiting the disclosure of information from a system of records without the written consent of the individual, unless the disclosure is under the 12 statutory exceptions (Woodward, 2008, pp. 357-379).

Statement of the Problem

To enforce the recommendation of the 9/11 Commission report to enhance security measures, DHS agencies need to be in compliance with the Privacy Act of 1974. The DHS has to address the concerns of privacy advocates who insist that the government is infringing into the civil liberties of the individual (Nelson, 2004). Therefore, DHS must be able to address these concerns related to privacy, before it is able to implement the use of biometrics as a security measure for screening of incoming and outgoing travelers (Nelson, 2004).

Besides remaining in compliance with the Privacy Act requirements and addressing the concerns of privacy advocates, DHS agencies have to consider the differences in individuals' attitudes, and perspectives. The acceptance of the technology has to be considered as the "end-user" will be affected by the collection, and the use of biometrics to enhance security in the expedited screening procedures (Moroson, 2012). The understanding of such individual beliefs can help DHS, TSA, airport managers, and industry experts in making decisions about whether the introduction of biometrics into the expedited security procedures would be met with resistance or acceptance among the traveling public (Boo & Jones, 2009).

Purpose of the Study

The purpose of this mixed-method study was to investigate privacy concerns of travelers regarding the use of biometrics in Trusted Traveler Programs. In this study, I investigated whether ease to use, usefulness, security, and awareness of the adopted biometric technology would influence its implementation into the expedited screening procedures of commercial airports in the United States.

In the study, I explored the various trends in the acceptance of biometric technologies in a commercial airport environment based on the Trusted Travelers given perception of privacy and airport experience and examined the factors that may contribute to the propensity of DHS agencies to adopt biometric technology into the expedited screening process. The role of *human behaviors* plays a significant role in the implementation of any public policy and must be considered in organizational operations. It is important that human behaviors be explored as they may have the ability to impact the adoption of new technologies and expedited security procedures (Chan, 2002).

Nature of the Study

The overall research design was to explore the relationship between privacy concerns of the individual participating in a Trusted Traveler Program and the adoption of biometric technologies into the identity verification process in commercial airports as an expedited security procedure. I used a document review as a method of collecting data from multiple sources of information. According to Creswell (2007), the document review method is used when there is a need for the data to answer *what* and *how* questions. The first phase of the data collection has been incorporated into the literature review, and included supporting documents that covered the use of biometrics in Trusted Traveler Programs (2011-2014). It also covered the theoretical foundation of the study (Davis' TAM model).

The second phase of the data (Chapter 4) collection process included primary and secondary documents that covered the reaction of individuals enrolled into Trusted Traveler Programs and their concerns about privacy, ease of use, and usefulness of the biometric system. I examined archival documents to determine the government's actions to safeguard an enrollee's privacy and the role of attitudes, organizational factors, and social demographics in the process of the acceptance to the use of biometric technologies. Further discussion of the methodology and the research design used is provided in Chapter 3.

Research Questions

The following research questions guided the study:

Research Question 1: Do privacy concerns of travelers affect the adoption of biometric technology into the expedited screening procedures at commercial airports?

Research Question 2: Do ease of use, usefulness, awareness of the technology, and security affect the adoption of biometric technology into the expedited screening procedures at commercial airports?

Theoretical Foundations

The theoretical framework is based upon Morosan (2012) research on feelings generated on the use of biometric technology in various industries. It further focuses on the technology acceptance model (TAM) by Davis (1989). Davis' TAM discusses the ease of use of the technology and theories between organizational, social, and technical factors that Trusted Travelers experience within a commercial airport environment to enhance security measures.

In this study, Davis' TAM was reference as it takes into account an individual's perceived ease of use and the usefulness of the technology (Davis, 1989). Furthermore, Davis' (1989) model explains the two beliefs that determine the attitudes for organizations to adopt new technologies. The model suggests that the attitude towards adoption will likely be decided on the adopter's positive or negative experience (Grembergen & Haes, 2008).

Trusted Traveler Programs incorporate a change in society because it places the traveling public into two categories, *low-risk* and *high-risk* changing air travel screening procedures. When a traveler decides to participate in a program, he or she willingly gives up personal information in order to obtain benefits that expedite security screening during traveling.

Operational Definitions of Terms

Biometric: The digital representation of an individual's distinct behavioral and physical characteristics (NSTC, 2006a).

Biometric template: Is the information captured of a sample of a biometric that becomes the electronic data based on the observation of the characteristics of an individual (NSTC, 2006a).

Biometric system: Is the process of comparing sets of biometric data with an existing set that was previously collected, it is used to assist human-driven comparisons to help screening officers compare an image of an individual on an identification card or on a storage device (NSTC, 2006a). This process collects a sample, converts that sample into a template and compares the templates to those previously collected (GAO, 2002). All biometric systems perform *recognition* to *again know* a person who has previously enrolled into the system. These systems conduct a verification process by the comparison of a new biometric with an existing one that has previously enrolled into the system (Morosan, 2012).

Enrollment: The process that a biometric system is specifically set to identify a person. The person must present an identifier that later is link to an acquisition device producing a biometric template (GAO, 2002, p.3).

Verification: The process to confirm whether an individual is who they claim to be and the transaction that connects the process governing the physical access to the resources of an organization (NSTC, 2006a).

Identification: The process to confirm whether an individual is who they claim to be except that no identifier is provided. A trial template is compared with the reference templates of all those enrolled into the system (GAO, 2002, p.4).

False match rate: This occurs when a system incorrectly matches an identity (GAO, 2002, p.5).

False non-match rate: This occurs when a system rejects a valid identity (GAO, 2002, p. 5).

Failure to enroll rate: This rate measures the probability that a person will be unable to enroll into a biometric system (GAO, 2002, p.5.).

Subcommittee on Biometrics and Identity Management: This subcommittee is under the U.S Government National Science & Technology Council (NSTC). The council developed a report on the examination of the implementation of biometrics into the use of government services. The subcommittee examined the use of biometrics of government services into data management, collection of biometrics, ease of use and speed in verification, and an appeal process in the event that the technology fails to verify the individual (NSTC, 2006a).

Privacy: The conceptual definition of privacy based on Warren and Brandeis (1890) is the "claim that an individual's interest arises as an assertion against other individuals or organizations to prevent interference from an individual's autonomy" (Warren & Brandeis, 1890). Each individual has the desire for physical space where he or she can be free from embarrassment, accountability, intrusion, or interruption, and the attempt to control the disclosures of personal information about themselves (Warren & Brandeis, 1890).

The Privacy Act of 1974: The law requires a set of fair information principles governing how the government collects, use, and maintains the use of personally identifiable information in databases and record systems (Nelson, 2004).

The Government Act of 2002: The law requires government agencies to implement assessments of the use of information technology and the potential affects it may bring on privacy (Nelson, 2004).

Trusted Traveler: Is a U.S. citizen or foreign national who has been approved by CBP to participate in a Trusted Traveler Program and is eligible for expedited security screening with TSA Pre-Check (CBP, 2014).

Trusted Traveler Program: Program that provides expedited security screening travel for pre-approved, low risk travelers through dedicated lanes and kiosks (CBP, 2014.)

Significance of the Study

The study is significant because it allows DHS agencies to explore various options when planning to adopt biometrics into the expedited screening procedures across commercial airports in the United States and its territories, as it relates to matters of privacy. The study makes it contribution to the literature by specifically addressing privacy in Trusted Traveler programs as it relates to expedited security screening and the adoption of biometric technologies in commercial airports (Merlano, 2014, p. 1).

Assumptions

In this study, I assumed that travelers enrolled in Trusted Traveler programs under DHS agencies enjoyed the benefits of having a faster security experience through the checkpoints in the United States and its territories. However, some researchers have raised questions about the effectiveness of biometric systems into security systems based on the capture and verification rates of current technology developments (NSTC, 2006a). The Subcommittee on Biometrics and Identity Management under the NSTC reported in 2006 that the "effectiveness of a particular biometric technology is dependent on how and where the technology is used" (p.5).

To avoid any bias about the benefits of Trusted Traveler programs, I explored the arguments of privacy advocates and those organizations that state that an individual should not give up their right to privacy, or release personal information to have a faster security screening experience; to draw a broad picture about the adoption of biometrics into the expedited screening process in a commercial airport environment.

I also assumed that the participants in the archival complaints submitted to the DHS Privacy Office that were used in this study answered truthfully and provided honest answers to the questions on the complaint forms. I tried to account for the effect of this assumption by analyzing different privacy annual reports and GAO reports on privacy assessments that revealed various points of view (data triangulation).

Another assumption was that the data collected from the complaints and archival documents were comprehensive and gathered the relevant information needed to answer the questions of the study. A data collection form was developed to summarize the data that was collected from all the documents, which helped me to compile and analyzed the findings.

The final assumption was that responses to the study questions truthfully reflected the assessments of legal experts. The legal system has not yet included new advances in technology into its legal interpretation; therefore, balancing an individual's right to privacy had not been addressed in this regard. I tried to reach a group of specialists dealing with legal matters under the subject of national security. I did this in an attempt to provide various points of view on effective and efficient security measures while remaining compliant with laws pertaining to privacy and the traveling public.

Scope of the Study

The implementation of Trusted Traveler Programs was an initiative by the DHS to free resources as a result of budget reductions. The programs created a risk-based model in security screening where it classified travelers into categories in which the government had known or little information of individuals. The scope of the study was to extend an assessment of the effects of Trusted Traveler programs and the potential to adopt biometric systems to be implemented into the expedited security screening of travelers in a commercial airport environment. The study involved the views of specialists from national and international organizations, as well as individual's enrolled into a Trusted Traveler Program that had knowledge about the enrollment process and the benefits of the current programs as describe by the GAO and the DHS Privacy Office.

Limitations and Delimitations

This research was about the privacy concerns related to the use of biometric technology in Trusted Traveler programs specifically applied to the commercial airport environment. The overall research design was an explanatory case study that included a document review analysis. The review of primary documents (number of enrollees, institution’s reports, and agency data) was complemented with the selection of secondary data (journal articles, newspaper articles, and social media reactions) to see the extent of the use of Trusted Traveler programs in public policy.

The study results will be disseminated to countries looking to implement these types of risk-based security programs. The purpose is to allow countries to consider when possible, the results of the study in developing or implementing Trusted Traveler programs to free up resources and develop security standards based on intelligence driven data. Yet, the creation of a set of suggestions that may work for all countries is not within the scope of this study because each country has specific set conditions, and what works in the United States might not be applicable to other countries. Thus, in future studies, this topic might be worthy of examination for other countries engaged in national security policies.

Implications for Social Change

By placing this study within the body of the research on social and political change, the results may be used to enhance the discussion for the U.S Supreme Court to bring about a clear interpretation of the fourth amendment and the U.S. Patriot Act of 2001. This research contributes to the deficiency in the literature as it addresses the privacy aspect through legal matters as it relates to advances in information technology. This study may give authorities, scholars, and specialists the opportunity to determine which actions should be implemented in their policies.

The implementation of Trusted Traveler programs in American civil society has already impacted the traveling public and commerce in commercial airports (Neyland, 2009). The American people will have to make the decision to give up their personal privacy in order to receive the benefits of expedited security during the screening process or not participate in such programs and continue to get standard screening in commercial airports. Yet, Trusted Traveler programs are not just limited to the airport environment, but those of border crossings and marine time entry within the U.S for the import and export of commerce.

The goal of such research was to make a contribution to the existing body of knowledge on the subject, so that individuals and civil society in the U.S. could better understand issues and problems; propose and arrive at solutions, and foster the continuation of change-oriented debate in public policy.

The implementation of Trusted Traveler programs with the adoption of biometric technologies into the expedited screening process may interest other countries with similar characteristics to those of the U.S. to implement programs of the same nature (Neyland, 2009). It is hoped that this research will provide a platform for other researchers to build on and conduct further studies on the subject.

Chapter Summary

The main purpose of this research was to explore and explain the relationship between the privacy concerns of travelers and the adoption of biometrics into the expedited screening process of outgoing travelers in Trusted Traveler programs. Furthermore, the relationship between privacy, the adoption and use of biometrics is to include the role of different stakeholders, local, state, and national legislation, and explore and explain whether the traveler is accepting of the technology that would be incorporated as it relates to privacy. For this research, a mixed method approach design was chosen. Two research questions guided the study. The questions were answered through quantitative and qualitative methods to understand technology acceptance.

In Chapter 2, I presented a review of the literature about the concept of expedited screening, the use of biometric technology as it relates to expedited screening and how privacy provisions must be addressed for its implementations on political and social change. I specifically focus on Davis' (1989) model on technology acceptance as the selected framework for the study. I reviewed recent studies to set the contextual background for the possible use of biometrics into the expedited screening of passengers. Details of the research design are presented in Chapter 3, including the data collection and data analysis methods. In Chapter 4, I presented the results of the documents reviewed to answer the research questions. Chapter 5 included the interpretation of the findings, recommendations for the application of the findings, implications for social change, and recommendations for further studies.

Chapter 2: Literature Review

Introduction

In this literature review, I focused on the concept of privacy and its importance to the adoption and use of biometric systems in Trusted Traveler programs administered by the U.S. Department of Homeland Security. Specifically, I discussed Davis' (1989) TAM as a selected theoretical framework for the study based on the findings of Morosan (2012). Additionally, I presented a critical evaluation of the TAM model and provided examples of its application in various contexts.

Furthermore, the debate between an individual's right to privacy and the government's responsibility to develop security programs for its national security needs creates challenges to civil rights and liberties. I presented background information regarding Trusted Traveler programs in an attempt to understand the existing literature written related to an individual's right to privacy and the use of biometric technologies for expedited screening. I incorporated and highlighted the studies on social, political, and economic change, as well as the approaches and theories used: and the limitations of these studies.

The literature for the review came from various scholarly sources in the Walden University library. The following databases were searched: PROQUEST, EBSCO, JSTOR, Naval Graduate Academy, and SAGE found in the Walden Library. The databases were searched using the following keywords: *Trusted Traveler Program, registered traveler program, risk-based security, expedited screening, TSA Pre-Check,* *Global Entry, privacy in trusted traveler programs, biometrics, biometric systems, biometric technologies, low-risk passenger, aviation security, and privacy concerns.*

Other keywords used included *ease of use biometric technology* and privacy requirements based on the federal definitions in the Privacy Act of 1974 and how the TAM model would provide an integrated model for the adoption of biometric technology into the expedited screening of passengers.

The Concept of Expedited Screening

The TSA uses the term expedited screening as a screening process that is more convenient and efficient to screen individuals that the agency has gathered sufficient background information classifying them as low-risk, compared to those receiving standardize screening as no information is known beforehand (TSA, 2014). Passengers qualifying for expedited screening no longer have to remove their shoes, can keep permitted small liquids, gels, and laptops inside of their carry-on bag; and are allowed to keep on their jackets and belts while passing through the walk through metal detectors through security screening checkpoints (TSA, 2014). If the passenger has an alarm, those items must be removed for alarm resolution (TSA, 2014).

Global Entry, NEXUS, SENTRI, and FAST are Trusted Traveler programs that expedite the security screening of low-risk passengers and shipments across the border through lanes and kiosks dedicated to Trusted Travelers at Ports of Entry (CBP, 2013). TSA Pre-Check was implemented in October 2011 and is a Trusted Traveler Program that allow Trusted Travelers to receive expedited screening at security checkpoints in commercial airports (GAO, 2014a, p.4). Trusted Travelers registered under programs with CBP are automatically eligible to received TSA Pre-Check at commercial airports in the United States.

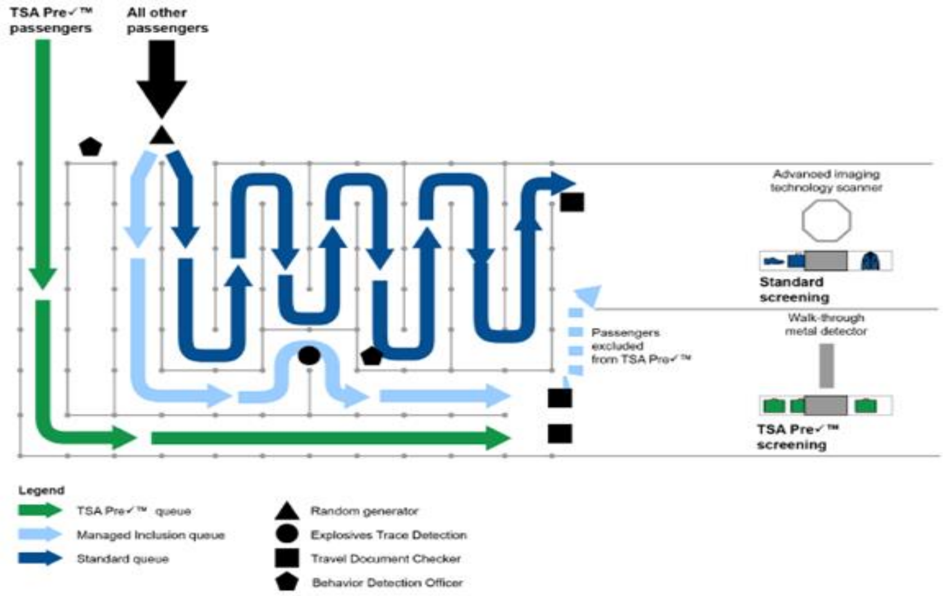
The purpose of Trusted Traveler programs is for participants to receive expedited travel benefits through dedicated lanes and kiosks at checkpoints and ports of entry throughout the United States. All Trusted Traveler programs rely on the vetting of travelers who voluntarily applied for membership by providing personal information and paying a fee to either CBP or TSA (GAO, 2014a, p.12). Those travelers are granted Trusted Traveler status and are considered low-risk compared to others as a result of the vetting process that CBP and TSA conduct during the enrollment process and afterwards (GAO, 2014a, p.12).

Trusted Traveler Programs allow program participants to go through the same screening procedures as regular travelers with the exception that Trusted Travelers have a special identification card that is compliant with the Western Hemisphere Travel Initiative (WHTI) and requires the submission of biometrics (GAO, 2014a, p.12). The card automatically notifies CBP through its computer system at primary inspection booths of an individual's trusted status. If a Trusted Traveler is referred to secondary inspection, he or she would be moved to the front of the line because of its Trusted Traveler status (GAO, 2014a, p.12).

When lanes and kiosks dedicated to Trusted Travelers become long, CBP and TSA implement a technique called active lane management to ensure that Trusted Travelers' wait times are lower compare to regular travelers at ports of entry and screening checkpoints (GAO, 2014a, p.13). The CBP uses active lane management by switching regular traffic lanes to Trusted Traveler lanes when wait times become too long for Trusted Travelers (GAO, 2014a, p.13). If there are few Trusted Travelers in the dedicated lanes, those lanes get converted to regular travelers to maintain low wait-times and faster processing (GAO, 2014b. p.5).

The TSA employs a similar concept named Managed Inclusion for its Pre-Check program at commercial airport checkpoints who have dedicated Pre-Check lanes that are under use when wait-times are too long in the standard lane using a criterion based on risk assessments and low-risk eligibility (GAO, 2014a, p.13). Managed Inclusion enables the risk assessment of passengers in real-time to determine their risk-level through the use of randomization procedures, behavior detection officers (BDOs), canine screening teams, and explosive trace detection (ETD) devices (GAO, 2014b, p.5).

In November 2015, the TSA reduced the use of Managed Inclusion with the use of BDOs and ETDs in commercial airports as a result of audits conducted by the Homeland Security Office of Inspector General (OIG). OIG stated that the agency had not tested the effectiveness of the Managed Inclusion process (GAO, 2016, p.1). The OIG report stated that TSA's behavior detection and analysis program, had not demonstrated that behavioral indicators can be used to effectively and reliably identify passengers who many pose a threat to aviation security (Improve Oversight, 2016, p.10). The presented form of Managed Inclusion implemented by the agency is with the use of canine screening teams (GAO, 2016, p. 2).

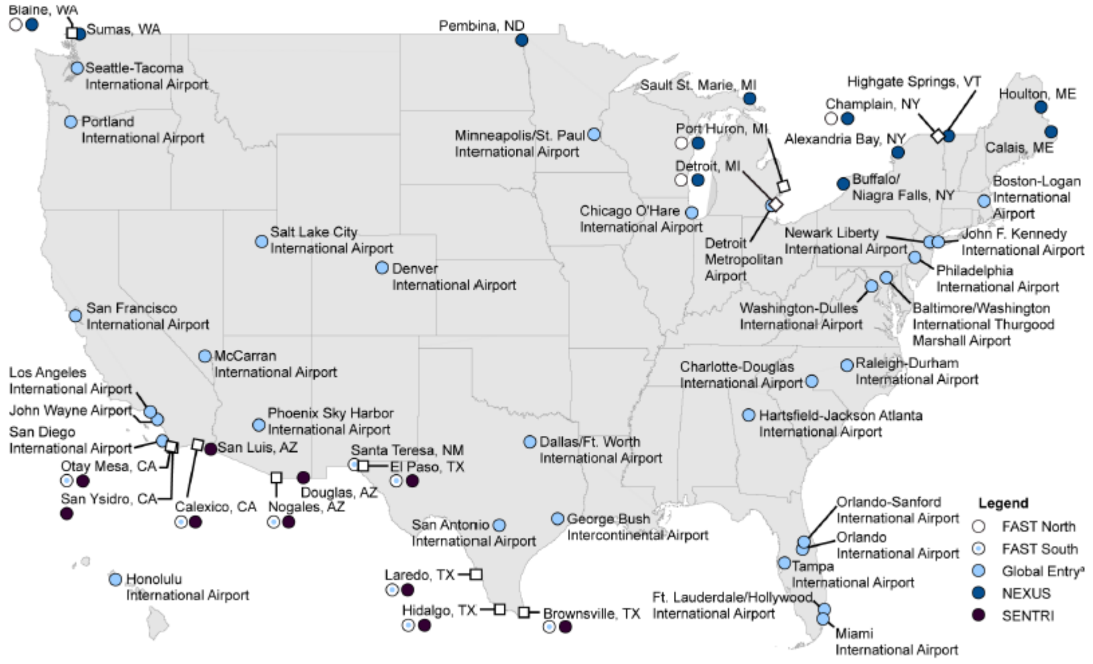


Source: GAO analysis of TSA information. | GAO-15-150

Figure 1: How the TSA operates managed inclusion with ETD devices

The expedited travel benefits for Trusted Travelers through CBP allows those with Trusted Traveler status to enter at point of entries, by just scanning their passports at dedicated kiosks and progressing through primary inspection booth without meeting a CBP officer (GAO, 2014b, p.10). At the kiosk, Trusted Travelers submit their passports, answer a series of questions, have their picture taken, and submit their fingerprint to verify their identity (CBP, 2013).

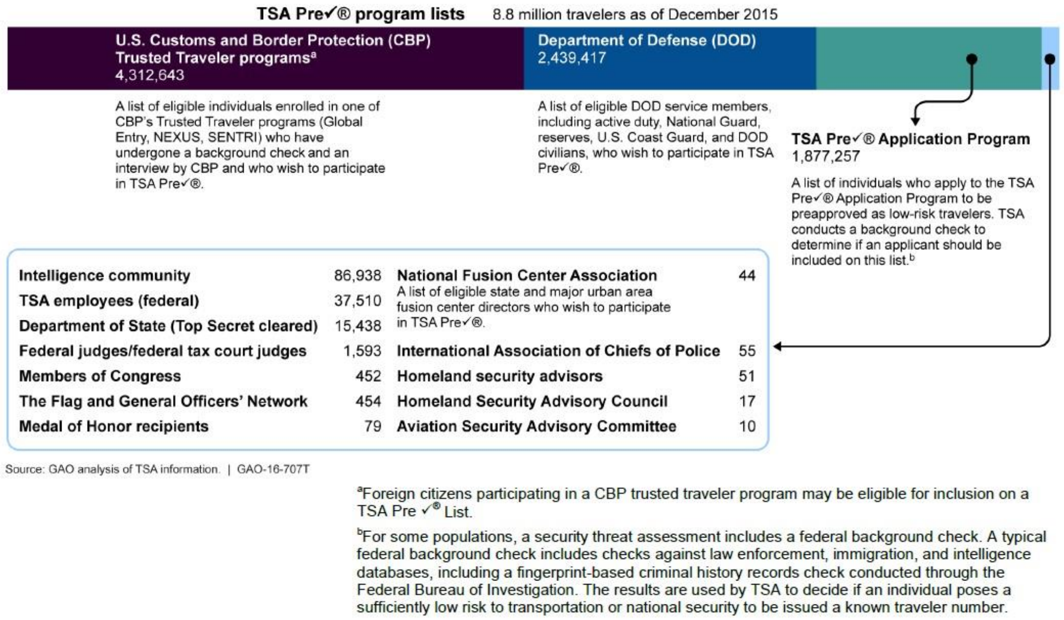
The kiosk notifies the traveler that they have been cleared to enter the country, or are being referred to secondary inspection (GAO, 2014b, p.10). When cleared to enter the country, the Trusted Traveler shows their passport and their receipt from the kiosk to ensure the receipt is valid and matches the passenger (GAO, 2014b, p.10). If the receipt is clear, the passenger is allowed into the country. If the receipt has a large X on it, the passenger is referred to secondary inspection (CBP, 2013).


Blaine, WA
Sumas, WA
Pembina, ND
Seattle-Tacoma International Airport
Portland International Airport
Sault St. Marie, MI
Highgate Springs, VT
Champlain, NY
Houlton, ME
Minneapolis/St. Paul International Airport
Port Huron, MI
Alexandria Bay, NY
Calais, ME
Detroit, MI
Buffalo/ Niagra Falls, NY
Boston-Logan International Airport
Chicago O'Hare International Airport
Salt Lake City International Airport
Detroit Metropolitan Airport
Newark Liberty International Airport
John F. Kennedy International Airport
Denver International Airport
Philadelphia International Airport
Washington-Dulles International Airport
Baltimore/Washington International Thurgood Marshall Airport
San Francisco International Airport
McCarran International Airport
Charlotte-Douglas International Airport
Raleigh-Durham International Airport
Los Angeles International Airport
John Wayne Airport
Phoenix Sky Harbor International Airport
Hartsfield-Jackson Atlanta International Airport
San Diego International Airport
San Luis, AZ
Santa Teresa, NM
El Paso, TX
Dallas/Ft. Worth International Airport
Otay Mesa, CA
San Ysidro, CA
Douglas, AZ
Calexico, CA
Nogales, AZ
San Antonio International Airport
George Bush Intercontinental Airport
Orlando-Sanford International Airport
Orlando International Airport
Tampa International Airport
Legend
○ FAST North
◎ FAST South
● Global Entry^a
● NEXUS
● SENTRI
Honolulu International Airport
Laredo, TX
Hidalgo, TX
Brownsville, TX
Ft. Lauderdale/Hollywood International Airport
Miami International Airport

Source: GAO analysis of U.S. Customs and Border Protection data.

Figure 2: Trusted Traveler POEs by program.

In the case of TSA, its expedited airport screening is based on low-risk populations and "Trusted Traveler or Known Traveler" status – those who have volunteered personal information to TSA, so that the TSA can confirmed those "Trusted or Known Travelers" are low risk (TSA, 2013). The TSA Pre-Check program allows for the expedited screening of low- risk populations such as children 12 years and younger, 75 and older adults, known crew members, Trusted Traveler programs through CBP, frequent flyers choosing to opt-in through their air carriers, and through TSA Pre-Check membership (GAO, 2014b, pp.8-9).



TSA Pre✓® program lists 8.8 million travelers as of December 2015

U.S. Customs and Border Protection (CBP) Trusted Traveler programs[a] 4,312,643

A list of eligible individuals enrolled in one of CBP's Trusted Traveler programs (Global Entry, NEXUS, SENTRI) who have undergone a background check and an interview by CBP and who wish to participate in TSA Pre✓®.

Department of Defense (DOD) 2,439,417

A list of eligible DOD service members, including active duty, National Guard, reserves, U.S. Coast Guard, and DOD civilians, who wish to participate in TSA Pre✓®.

TSA Pre✓® Application Program 1,877,257

A list of individuals who apply to the TSA Pre✓® Application Program to be preapproved as low-risk travelers. TSA conducts a background check to determine if an applicant should be included on this list.[b]

Intelligence community	86,938	**National Fusion Center Association** A list of eligible state and major urban area fusion center directors who wish to participate in TSA Pre✓®.	44
TSA employees (federal)	37,510		
Department of State (Top Secret cleared)	15,438		
Federal judges/federal tax court judges	1,593	**International Association of Chiefs of Police**	55
Members of Congress	452	**Homeland security advisors**	51
The Flag and General Officers' Network	454	**Homeland Security Advisory Council**	17
Medal of Honor recipients	79	**Aviation Security Advisory Committee**	10

Source: GAO analysis of TSA information. | GAO-16-707T

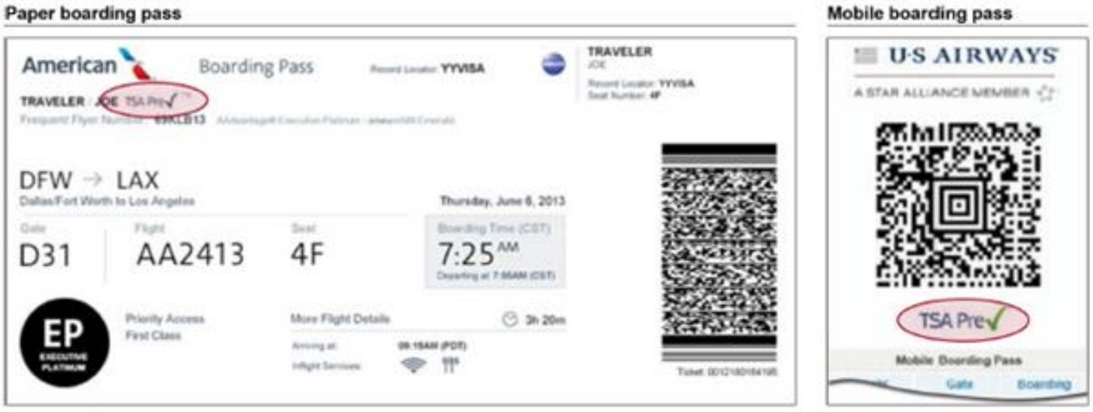
[a] Foreign citizens participating in a CBP trusted traveler program may be eligible for inclusion on a TSA Pre ✓® List.

[b] For some populations, a security threat assessment includes a federal background check. A typical federal background check includes checks against law enforcement, immigration, and intelligence databases, including a fingerprint-based criminal history records check conducted through the Federal Bureau of Investigation. The results are used by TSA to decide if an individual poses a sufficiently low risk to transportation or national security to be issued a known traveler number.

Figure 3: TSA Pre-✓ lists

In December 2015, TSA officials announced that the branches of the U.S. armed forces including those on Reserve and National Guard personnel were eligible to participate (GAO, 2016, p.5). In addition, members of the intelligence community, TSA employees, Department of State (Top Secret Cleared) employees, and foreign citizens participating in CBP Trusted Traveler Programs were eligible to participate (GAO, 2016, p.6).

TSA Pre-Check enables the participating air carriers to technologically send the necessary passenger information to Secure Flight for vetting against federal government watch lists and print the low-risk designation in the encrypted boarding pass bar code and the TSA Pre-Check designation on the boarding pass (GAO, 2014a, p.13).



Source: TSA | GAO-15-150

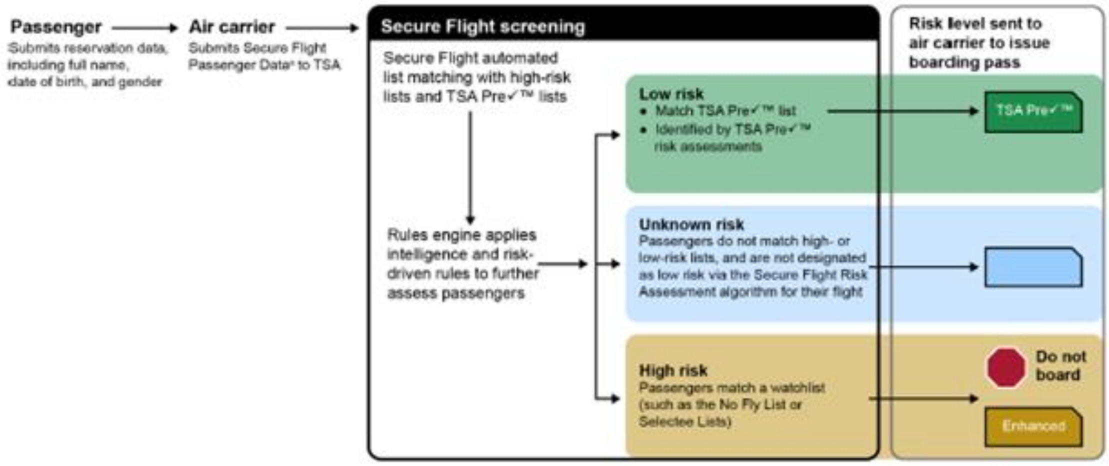
Figure 4: Examples of boarding passes with the TSA Pre-✓ Designation

The process to apply for TSA Pre-Check membership includes visiting a enrollment center, where individual’s must provide their biographic information such as name, date of birth, address, citizenship documentation, a second source of identification, and fingerprints to undergo a security threat assessment (TSA, 2013).

As a result of previous programs implemented by the TSA such as Transportation Worker Identification Credential (TWIC), the agency was able to leverage existing capabilities into their enrollment process and threat assessments from program applicants (GAO, 2014, p.18). In order to be eligible to participate in TSA Pre-Check, applicants must be a U.S. citizen, U.S. national or a lawful permanent resident and must not have been convicted of certain crimes (GAO, 2014a, P.18).

The system of Secure Flight is used at commercial airports to automatically match a traveler’s information that has been collected by the air carriers to screen against the various watch lists (No Fly and Selectee Lists) 72 hours before a travelers’ scheduled departure (GAO, 2010, p.3). Once the verification is completed through the watch lists, Secure Flight indicates the air carriers to mark a traveler's boarding pass for expedited screening, enhance screening, standard screening or is prohibited from boarding the aircraft (GAO, 2010, p.5).).

The same system is used to identify travelers who are eligible for expedited screening at commercial airports by utilizing the same information collected by the air carriers and vetting that information through the low-risk lists (GAO, 2014a, p.29). Afterwards, the TSA notifies the traveler of their eligibility by informing the air carriers to mark the boarding pass with the TSA Pre-Check designation (GAO, 2014a, p.19).


Passenger
Submits reservation data, including full name, date of birth, and gender
Air carrier
Submits Secure Flight Passenger Data[a] to TSA
Secure Flight screening
Secure Flight automated list matching with high-risk lists and TSA Pre✓™ lists
Rules engine applies intelligence and risk-driven rules to further assess passengers
Low risk
• Match TSA Pre✓™ list
• Identified by TSA Pre✓™ risk assessments
Unknown risk
Passengers do not match high- or low-risk lists, and are not designated as low risk via the Secure Flight Risk Assessment algorithm for their flight
High risk
Passengers match a watchlist (such as the No Fly List or Selectee Lists)
Risk level sent to air carrier to issue boarding pass
TSA Pre✓™
Do not board
Enhanced

Source: GAO analysis of TSA information. | GAO-15-150

Note: Passengers of unknown risk do not have screening-related markings on their boarding pass.

[a]Secure Flight passenger data include personally identifiable information, such as full name, gender, date of birth, passport information (if available), and certain nonpersonally identifiable information, such as itinerary information and the unique number associated with a travel record (e.g., record locator number). See 49 C.F.R. §1560.3 (defining "secure flight passenger data").

Figure 5: TSA Secure Flight screening process

For some commercial airports, the TSA has dedicated TSA Pre-Check expedited screening lanes for those travelers having the TSA Pre-Check designation on their boarding pass (TSA, 2014). The participation into the program is completely voluntary and a traveler who has been designated as eligible for TSA Pre-Check expedited screening may elect not to use the dedicated lanes according to TSA officials (TSA, 2014). Not all commercial airports can afford to have dedicated TSA Pre-Check expedited screening lanes due to space restrictions and low volume of passengers with Pre-Check designation that do not warrant a dedicated lane (GAO, 2014a, p.19).

In those commercial airports where Pre-Check dedicated lanes are unavailable, travelers with the TSA Pre-Check designation can still experience expedited screening of "their person" (ex: does not remove shoes, belts, and light jackets) but must divest their permitted liquids, and laptops from their carry-on baggage, since the screening process used in standard lanes are different from those in expedited screening lanes (GAO, 2014a, p.19).

The selection in which the TSA determines who is eligible for expedited screening is based on three risk assessment methods. The first method is verifying an individual's name through the TSA Pre-Check List of known travelers (GAO, 2014, p.9). The second method is the designation of a traveler's identification as low-risk under the TSA's Risk Assessment Algorithm (GAO, 2014b, p.9). The third method is the real time assessment of a traveler at the airport under the Managed Inclusion Process (GAO, 2014, p.9).

The concept to use expedited screening through Trusted Traveler Programs was proposed by Northwest CEO Richard Anderson in 2002. He stated "Trusted Traveler Programs is one example of how industry, working with government, can quickly bring to market programs that would relieve some of the burden on aviation security" (Melnik, 2002).

Foundations for a Risk-Based Security System

The development of Trusted Traveler Programs came from the idea that not all travelers present the same security threat level. This idea expanded in the creation of a risk-based approach to aviation security. Countries such as Israel and the European Union focus their security resources on identifying risky travelers enabling them to match their resources to those risks, rather than screening everyone the same (GAO, 2002, p.3) The risk-based model approach provides security officials the ability to direct more resources and obtained better screening equipment for travelers exposing a higher risk to security. Therefore, the model allows for the improvement in detection and increase deterrence compared to the one-size fit all approach (GAO, 2002, p.8).

Trusted Traveler Programs serve as a risk management tool as it chooses the appropriate level of screening for a traveler depending on a prior assessment of their personal background and the individual's threat to security. These programs decrease the inconveniences and uncertainties of the amount of time and the level of security, travelers would experience as they pass through a security checkpoint in a commercial airport (GAO, 2002, p.3).

The President and CEO of the U.S. Travel Association Roger Dow stated “These programs would encourage travelers, especially business travelers to fly more often, therefore, improving the economic health of the United States” (U.S. Travel Association, 2010). Additionally, other related industries would also benefit from these programs such as tourism, aviation-related manufacturers, transportation workers and commerce creating a healthy economy (U.S. Travel Association, 2010).

Dow (2010) highlighted that Trusted Traveler programs should be the centerpiece for an enhanced air travel security system by screening passengers for security risks prior to entering the checkpoints (p.3). The programs pre-screens the individual before arriving at the airport and this risk assessment reduces the line in the airport and allows security resources to be used for individuals presenting a higher risk level (p.3).

Additionally, these programs have the ability to deter potential threats as they create an effective and efficient approach to security that alleviates congestion at security checkpoint, as a congestive atmosphere becomes attractive to potential terrorists (p.3). Furthermore, according to Dow (2010) these programs protect the privacy and civil liberties by eliminating physical security measures for those enrolled into the program by strengthening public trust as the federal government works on balancing privacy, civil liberties, efficiency and security, as those travelers are deem low-risk (Dow, 2010).

Based on the views and influence of various stakeholders in the aviation industry, the TSA in 2002 introduced a pilot for a registered traveler type program for transportation workers. The program called Transportation Worker Identity Credential (TWIC) provides a tamper-resistant biometric credential for maritime workers giving them unescorted access to secure areas into port facilities, outer continental self-facilities, and vessels regulated under the Maritime Transportation Security Act of 2002 and the U.S. Coast Guard (TWIC, 2013).

The application process for the TWIC card requires for applicants to submit biographic and biometric information to include fingerprints, sit for a digital photograph, and pass a security threat assessment (TWIC, 2013). Once accepted into the program, the card issued has a computer chip, known as an Integrated Circuit Chip (ICC) storing the holders' biometric and personal information (TWIC, 2013).

Furthermore, stakeholders such as airport managers, airlines, and law enforcement entities found that such programs could contribute to enhanced customer service, expedited check-in at airports, track frequent flier miles, collect information obtained during background checks to help identify individuals wanted by the police, or tracking the movement of citizens who might pose criminal risks (GAO, 2002, p.8). Since Trusted Traveler programs are voluntary, passengers choose to participate in these programs. This model assumes that a background check would accept all members of the non-terrorist public who apply and are granted Trusted Traveler status, while rejecting all terrorists (Chan, Jackson, & Latourrette, 2012).

According to Chan et al. (2012) some fraction of the non-terrorist population will apply and be rejected incorrectly, as some fraction of terrorists will be accepted incorrectly into the program (p.3). However, CBP and TSA maintained that Trusted Traveler Programs are voluntary and participants may have less possibility for an appeal, than they would in a government entitlement program since participation is guaranteed by statue (GAO, 2002, p.6)

However, many stakeholders expressed that Trusted Traveler Programs need to provide accurate data verification about travelers, function well in a commercial airport environment, and safeguard information against fraud (Chan et al., 2012). The concept of biometrics and its technologies is being used in Trusted Traveler Programs for those under CBP, but TSA has not adopted the used of this technology in its commercial airport security screening procedures.

The Concept of Biometrics and its Technologies

Government programs apply the concept of biometrics and its various technologies as a means for identifying and verifying of a person's identity by analyzing and measuring an individual's characteristics. The scientifically measurement of a person's physiological characteristics produces a unique data that enables a biometric to clearly identify or verify an individual (NTSC, 2006a, p. 2).

The adoption of the use of biometrics for security and identification related matters are not uncommon in the private sector. The tourism and banking industry use this concept to control fraud and accessibility (Moroson, 2012). The U.S. government continues to look into the adoption and use of this technology for its Trusted Traveler Programs, but must be able to incorporate privacy provisions, as the law requires it (NTSC, 2006a, p.2).

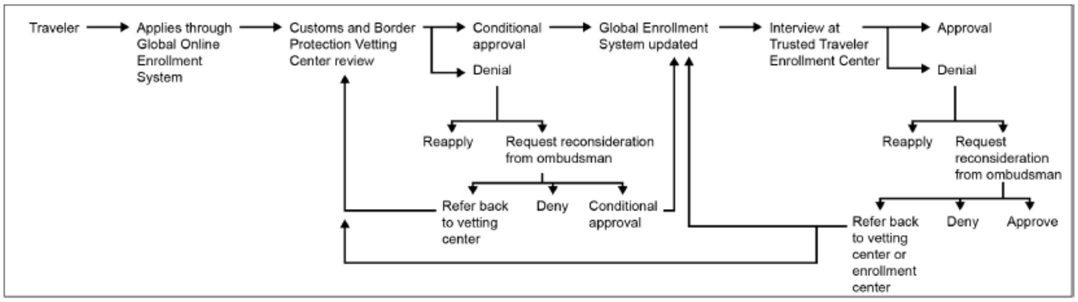
The use of biometric technologies to measure and analyze an individual's personal characteristics can come in various forms, measuring body parts such as the eyes, hand, fingerprints, and face (GAO, 2010, p.3). Acquisition devices such as recordings, cameras to take pictures, and scanning devices as known as biometric identification systems; that recognize patterns that are extracted, encoded, stored, and compared depending on the computer hardware and software capabilities (GAO, 2004, p.3).

The process for biometric identification systems is usually automated and the decision-making process is fast within seconds. Based on the format of the system and its use, it can be for identification or verification purposes (GAO, 2002, p.3).

Enrollment

In the enrollment process, the biometric system is specifically set to identify the identity of the person. For this to take place, the person must provide an identity card, which will act as an identifier (GAO, 2010, p.3). Afterwards, the system links the biometric to confirm the identity that is stored in the identification document.

Later, the individual places its unique biometric (ex: face, hand, fingerprints, or eye) in the acquisition device for identification (GAO, 2010, p.3). Those distinctive features are turned into samples which are taken, encrypted, and stored as future templates for comparisons in the future (GAO, 2010, p.3). If the identification document does not match a person's real identity, the template that is used as a template will be connected to a false identity (GAO, 2004, p.4).


Traveler
Applies through Global Online Enrollment System
Customs and Border Protection Vetting Center review
Conditional approval
Denial
Global Enrollment System updated
Interview at Trusted Traveler Enrollment Center
Approval
Denial
Reapply
Request reconsideration from ombudsman
Refer back to vetting center
Deny
Conditional approval
Reapply
Request reconsideration from ombudsman
Refer back to vetting center or enrollment center
Deny
Approve

Source: GAO analysis of U.S. Customs and Border Protection information.

Figure 6: CBP Trusted Traveler enrollment process

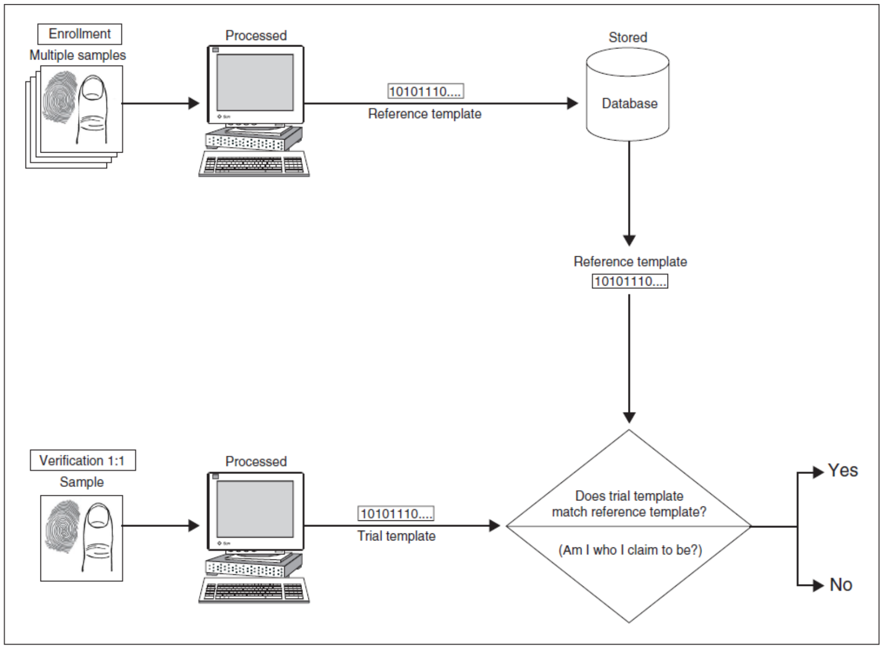
Depending on the technology, the biometric system extraction, encoding and storage information inside the template is exclusive to the vendor's proprietary algorithms (GAO, 2010, p.3). The same considerations are given to template sizes as templates can be stored remotely in a central database or inside a biometric reader device, such as smart cards and tokens (GAO, 2002, p.4). Specific factors such as changes in position, distance, pressure, and environment can change the template. Therefore, every time the biometric of an individual is taken, it is a unique template (p.4).

During the enrollment process, an individual may be asked to provide several samples of biometric data as part of the enrollment process, these samples are reference templates that are captured and stored for future comparisons (NSTC, 2006, p.3). The quality of the templates is important as it depends on the response of the biometric systems in order for it to accurately perform (NSTC, 2006, p.3). Since an individual's biometric data over time can change, an individual will have to resubmit into the enrollment process to update their reference template, unless the technology being use updates itself during matching operations (GAO, 2004, p.4).

Verification

After the enrollment process is verification. Verification is to verify that an individual is who they claim to be (ex: enrollee in the system) (GAO, 2010, p.4). Once the individual gives an identifier and the biometrics are collected, the biometric system process the biometrics, which generates a trial template according to the vendor's algorithm (GAO, 2010, p.4). Afterwards, the system compares the trial biometrics with the person's reference template already stored in the system and determines, if the individual's trial and stored template match each other (GAO, 2002, p.8).

Biometric systems that perform verification functions contain databases that range from dozens to millions of enrolled templates. There function is to always predict the matching of an individual's biometric against his or hers reference template (GAO, 2002, p.8). Most verification systems render a match to no match result in less than a second and require employees to confirm their identities to gain access to secured computers and buildings (GAO, 2002, p.9).



Source: GAO.

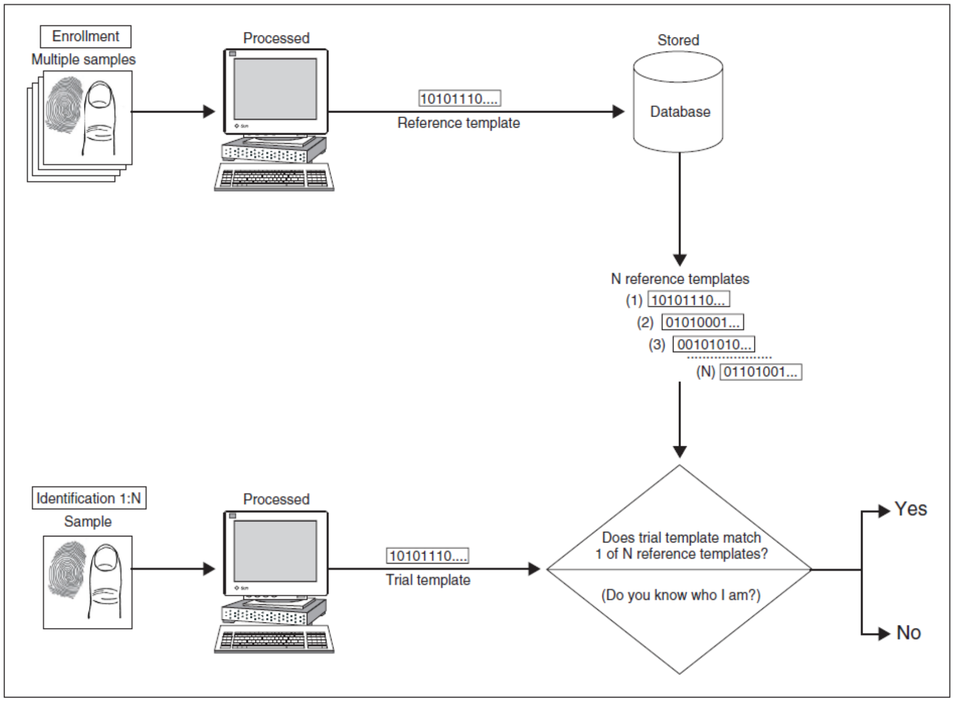
Figure 7: The biometric verification process

Identification

An additional step after the enrollment process is identifying who the person is. Identification systems are different as no identifier is needed to provide a match (GAO, 2010, p.8). In these systems, the captured biometric is compared with a stored template alongside all of the individuals enrolled in the system with the anticipation that a match will be provided based on the search (GAO, 2010, p.8).

In positive identification systems, access to secure buildings and computers are conducted by cross-checking everyone in the database that all enrollees are enrolled in (GAO, 2002, p.10). The purpose of these systems is to find whether a person seeking access can be identified as being enrolled in the system (GAO, 2002, p.10). However, in negative identification systems, a person's biometric information is not stored inside a database leading to a non-match result (GAO, 2002, p.10).

For example, the comparison of a person's biometric information in a database of those that have registered in a public program can verify that a person may be "double dipping" with the use of fraudulent documents using multiple identities (GAO, 2002, p.10). A watch list system is an example of a negative identification system as it is designed to identify people who match the list and alert authorities for appropriate action. The system will check for those individuals that are not on the list and allowed them to travel (GAO, 2002, p. 10)



Source: GAO.

Figure 8: The biometric identification process

Individuals' biometrics in the database of identification systems may have been placed in the system involuntarily. For example, in systems of surveillance, biometrics may be face captures from mug shots given by a law enforcement agency (GAO, 2013, p.12). For verification and identification systems, a no match is perfect since each time a biometric is taken; the template is different (GAO, 2013, p.12). As a result, biometric systems can be formatted to make a match or no-match decision on a number that has been preset and/or program threshold establishing a degree of acceptability between the captured template and the stored templates of those enrolled (NSTC, 2006b, pp.12-13).

Once the comparison is conducted, a score will be produced with the degree of acceptability and that score is than compared to the established threshold to make a decision (GAO, 2002, p.13). Depending on the setting of the threshold, it can have several reference templates be considered matches to the trial template; resulting in better scores leading to better matches (GAO, 2002, p.13). The International Biometrics Group (IBG) considers four types of biometric identifiers to be effective for Trusted Traveler Programs especially for aviation security. These identifiers include fingerprint recognition, iris recognition, hand geometry, and facial recognition.

Types of Biometric Technologies

Fingerprint Recognition

This is the most commonly used and best-known technologies, as it is the easily acceptable among private industries. This technology extracts impressions made up of specific ridges in the fingertips. Fingerprints may be collected by rolling the finger or by placing it on a flat surface (Biometrics, 2010). A flat print collects the impression of the central area of the fingertip and the rolling print collects the ridges of the finger from both sides (Biometrics, 2010).

An image of the fingerprint is collected by a scanner, converted, and then enhanced, to become a template. Scanner technologies may be ultrasound, silicon, or optical (GAO, 2002, p.47). Ultrasound is considered the most accurate, but optical scanners are the ones commonly used. During enhancement procedures, “noise” is a result of things such as scars, cuts, dirt, and creases, or worn fingerprints is reduced, making the ridges of the fingers more visible (GAO, 2002, p.47). About 80% of vendors format their proprietary algorithms on the collection of miniature points that relate to breaks in the ridges of the fingerprints, while others extract ridge patterns (GAO, 2002, p.47).

Iris Recognition

This technology centers on the color ring surrounding the pupil of the eye. The iris that is part of the eye is made of elastic connective tissue and is considered extremely rich in biometric data (GAO, 2002, p.47). The iris has 266 distinctive characteristics to include trabecular meshwork, rings, furrows, freckles and a corona allowing for extensive biometric data (GAO, 2002, p.47). Iris recognition utilizes a small, high-quality camera to collect a white and black, high-resolution picture of the iris and then selects the boundaries establishing a coordinate system over the iris. Afterwards, the specific zones are analyzed within that coordinate system (Biometrics, 2010). The iris tends to remain stable over the lifetime of the individual except if an injury would occur (GAO, 200, p.47).

Hand Geometry

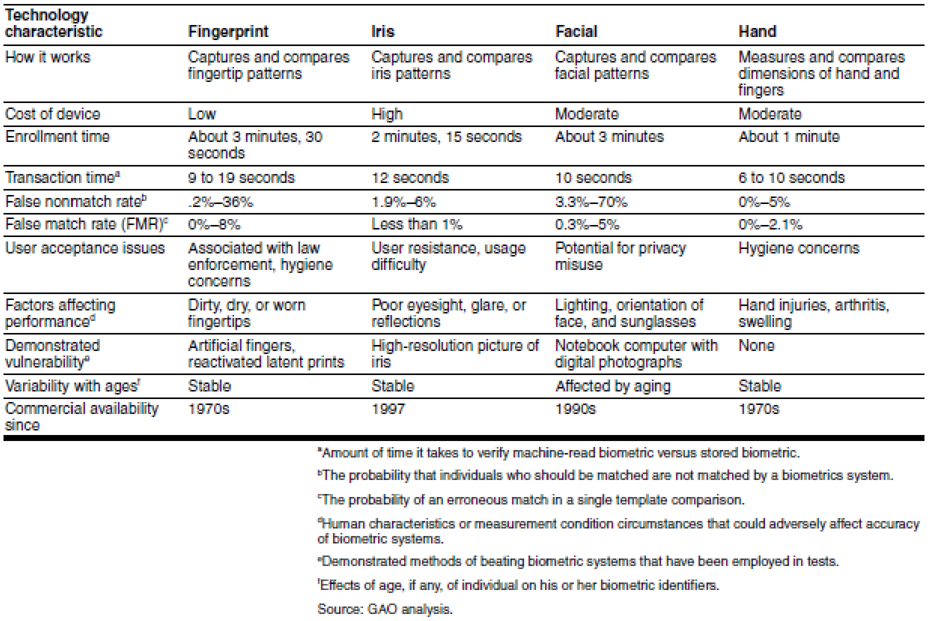
Hand Geometry utilizes an optical scanner that emits light-diodes with reflectors and mirrors capturing a three-dimensional image of the sides and back of the hand (Biometrics, 2010). Its purpose is to measure the width, length of fingers, joints, distance, between the joints, shapes of the knuckles, and height. These systems have been used for more than 10 years for access control at facilities from day care centers to nuclear power plants (Biometrics, 2010). This technology from its images can produce 96 measurements of extraction and as the shape of an individual's hand remains the same over time, natural and environmental factors can result in changes (GAO, 2002, p.47).

Facial Recognition

Facial Recognition compares a live facial picture with a reference template and can be used to analyze static images as a digitized passport photos (Biometrics, 2010). This technology identifies an individual by areas of the face – the upper outlines of the eyes, cheekbones, and mouth. These types of systems can be used as identification and verification purposes. Furthermore, since facial pictures can be captured from video cameras, facial recognition is the only biometric technology that can be used for surveillance purposes (Biometrics, 2010). Facial recognition depends on two algorithms: the Local Feature Analysis (LFA) and the Eigen Face method. The LFA breaks into pieces the face by the nose, eyes, mouth, and cheeks creating smaller size templates (GAO, 2002.p. 46). The Eigen Face method looks at the entire face using it at the set template (GAO, 2002, p. 46).

Table 1

Leading biometric technologies for aviation security



Technology characteristic	Fingerprint	Iris	Facial	Hand
How it works	Captures and compares fingertip patterns	Captures and compares iris patterns	Captures and compares facial patterns	Measures and compares dimensions of hand and fingers
Cost of device	Low	High	Moderate	Moderate
Enrollment time	About 3 minutes, 30 seconds	2 minutes, 15 seconds	About 3 minutes	About 1 minute
Transaction time[a]	9 to 19 seconds	12 seconds	10 seconds	6 to 10 seconds
False nonmatch rate[b]	.2%–36%	1.9%–6%	3.3%–70%	0%–5%
False match rate (FMR)[c]	0%–8%	Less than 1%	0.3%–5%	0%–2.1%
User acceptance issues	Associated with law enforcement, hygiene concerns	User resistance, usage difficulty	Potential for privacy misuse	Hygiene concerns
Factors affecting performance[d]	Dirty, dry, or worn fingertips	Poor eyesight, glare, or reflections	Lighting, orientation of face, and sunglasses	Hand injuries, arthritis, swelling
Demonstrated vulnerability[e]	Artificial fingers, reactivated latent prints	High-resolution picture of iris	Notebook computer with digital photographs	None
Variability with ages[f]	Stable	Stable	Affected by aging	Stable
Commercial availability since	1970s	1997	1990s	1970s

[a] Amount of time it takes to verify machine-read biometric versus stored biometric.

[b] The probability that individuals who should be matched are not matched by a biometrics system.

[c] The probability of an erroneous match in a single template comparison.

[d] Human characteristics or measurement condition circumstances that could adversely affect accuracy of biometric systems.

[e] Demonstrated methods of beating biometric systems that have been employed in tests.

[f] Effects of age, if any, of individual on his or her biometric identifiers.

Source: GAO analysis.

There are other biometric technologies that are commonly used, but are not applied to aviation security such as:

Retina Recognition

Retina Recognition collects and analyzes the blood vessels patterns from the thin nerve of the back of the eyeball from the light entering through the pupil (Biometrics, 2010). Each eye has its unique pattern of blood vessels, each pattern stays stable throughout a person's lifetime, but such diseases such as glaucoma, diabetes, high blood pressure, and autoimmune deficiency syndrome can affect it (Biometrics, 2010). In retina recognition, the individual has to place the eye closely to the lens of the scanning device and remain completely still while focusing on a revolving light while a small camera scans the retina through the pupil, since the retina is small and can be difficult to measure, the collection of its image makes it hard in relation to other biometric technologies (GAO, 2002, p.48).

This technology the most reliable and accurate of the technologies currently used, but any slight movement can interfere with the collection process and restarting can cause time during the enrollment and verification process. At the moment, government and military environments use this technology for access control requiring very high security levels such research sites and nuclear weapons locations levels (GAO, 2002, p.48). However, as a result of the high degree of cooperation and effort required of its users, it is also one of the least deployable technologies in terms of biometrics (GAO, 2002, p.48).

Signature Recognition

Signature Recognition confirms the identity of the individual by the measurement of signatures that are hand written. Then, the signature through a series of movements is analyzed to reflect an individual's rhythm, pressure flow, and acceleration (GAO, 2002, p.48). Electronic signature captures the signature and treats it as a graphic image compare to signature recognition in which measures how a signature is signed (GAO, 2002, p.48).

In signature recognition, the capture consists of the individual signing his or her signature on a digitized personal assistant or graphic tablet. Then, the system will analyze the signature based on the dynamics of stroke count, pressure, speed, and stroke order, as well as, track an individual's natural signature fluctuations over time (GAO, 2002, p.49).

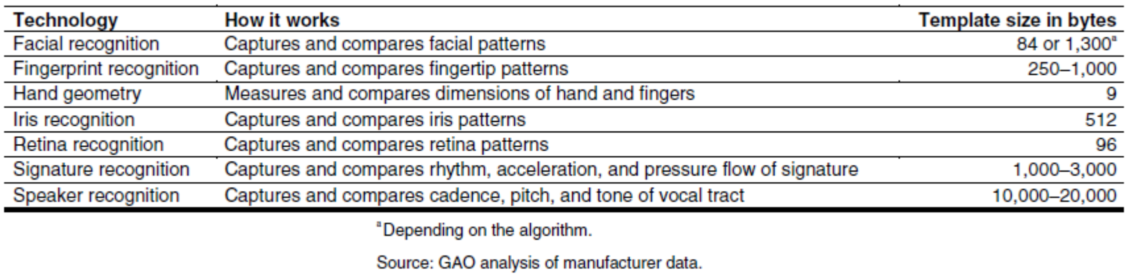
Speaker Recognition

Speaker Recognition uses the individual's sound of voice combine with differences in physiological as in learned speaking habits and the shape of vocal tracts (Biometrics, 2010). In the enrollment process, this technology captures samples of individual's speech by having him or her speak predetermined information into a telephone number or a microphone several times to capture the template (Biometrics, 2010).

The predetermined information can be a name, birth month, birth city, a sequence of numbers, or a favorite color. Afterwards, that information is change from analog to digital format and the distinctive vocal characteristics such as cadence, tone, and pitch are collected and a model of the speaker is composed (Biometrics, 2010). Then, a template is developed and saved for future matching. This technology can be used to verify and identify a person’s identity, however, the biometric identifier is through telephone or call centers (GAO, 2002, p.49).

Table 2

Leading biometrics technologies and their template size



Technology	How it works	Template size in bytes
Facial recognition	Captures and compares facial patterns	84 or 1,300[a]
Fingerprint recognition	Captures and compares fingertip patterns	250–1,000
Hand geometry	Measures and compares dimensions of hand and fingers	9
Iris recognition	Captures and compares iris patterns	512
Retina recognition	Captures and compares retina patterns	96
Signature recognition	Captures and compares rhythm, acceleration, and pressure flow of signature	1,000–3,000
Speaker recognition	Captures and compares cadence, pitch, and tone of vocal tract	10,000–20,000

[a] Depending on the algorithm.

Source: GAO analysis of manufacturer data.

Emerging Biometric Technologies

New biometric technologies are under development to recognize behavioral and physiological characteristics. Some of these technologies are commercially available while others still have years from implementation (Biometrics, 2010). Each technologies technique’s performance can change, depending on how it is used and the environment where is being used (Biometrics, 2010).

Vein Scan

This biometric technology automatically identifies a person from the patterns of the blood vessels in the back of the hand. It uses near-infrared light to detect vein vessel patterns (GAO, 2002, p. 50). Vein patterns are different between twins and even between a person’s right and left hand. This technology is highly stable and robust, and the vein pattern only changes throughout a person’s lifetime in size. It is not intrusive and works on the hand even if it is not clean (GAO, 2002, p. 50).

Facial Thermography

Facial Thermography detects patterns of heat created by the branching of blood vessels emitted from the skin. The patterns name thermo grams are highly distinctive that identical twins have different ones. Facial thermography works much like facial recognition, except that infrared cameras are used to capture the images (GAO, 2002, p.50).

This technology is not intrusive and no physical contact is required, as every person can present a usable image that can be collected in an instant. In addition, infrared systems work in dim light or in total darkness. The problem with this technology is that the manufacturing costs of the system are extremely expensive (Biometrics, 2010).

DNA Matching

Is a biometric technology that uses physiological traits for personal identification, it is considered the ultimate technology as it can produce a proof positive identification of a person, except for identical twins (GAO, 2002, p.51). The difference between DNA matching from standard biometrics is that it compares actual samples rather than templates generated by samples.

In addition, DNA comparisons cannot be automated and so comparisons cannot be made in real time. This technology is only use for identification in forensic applications and it has many years for its implementation as its extremely intrusive (GAO, 2002, p.51).

Odor Sensing

Odor sensing is the measuring of body odor. This technology would allow the use of an odor-sensing instrument to capture the volatile chemicals that the skin pores all over the body as it emits an individual's smell (GAO, 2002, p.51). The development of this type of technology is complex as odor can change based on an individual's diet, medications, perfumes, and deodorants (GAO, 2002, p.51).

Blood Pulse Measurement

Blood Pulse Measurement is the technology that measures the blood pulse on a finger with infrared sensors. This technology is in its experimental stages and has a high false match rate, which is impractical for personal identification purposes (Biometrics, 2010).

Skin Pattern Recognition

Skin Pattern Recognition measures the characteristic spectrum of an individual's skin. Each individual's skin is different as it relates to thickness and the interfaces between the layers that have various pigmentation, undulations, collagen fibers, and proteins changes in the density beneath the skin (GAO, 2002, p. 51). This technology uses a light sensor that lights up a small patch with a beam of visible and near-infrared light and then measures with a spectroscope after being scattered by the skin (GAO, 2002, p.51). Afterwards, the measurements are analyzed and an optical pattern is extracted (GAO, 2002, p.51).

Nailbed Identification

Nailbed Identification is the identification of the distinct tongue-in-grove spatial arrangement of the epidermal structure directly under the fingernail. An interferometer is used to detect phase changes in back-scattered light shone on the fingernail and once the distinctive dimensions are reconstructed, a map is generated (GAO, 2002, p. 51).

Gait Recognition

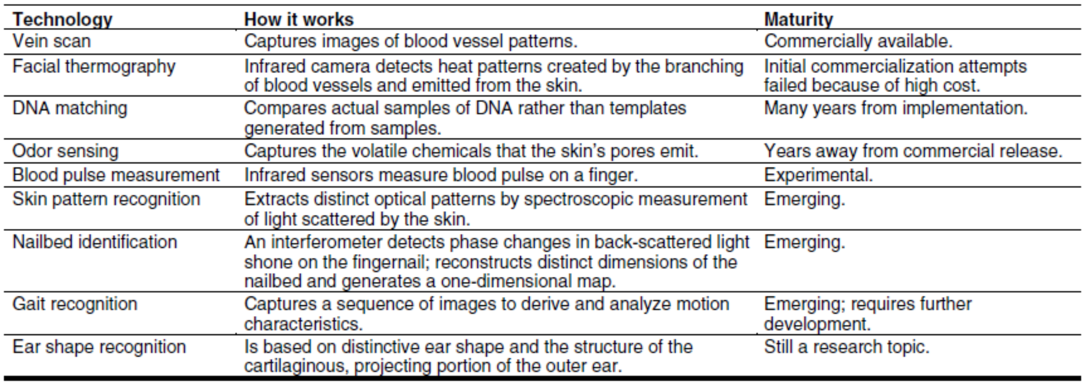
Gait recognition is based on the concept of recognizing individuals by their walk. An individual's gait may be difficult to hide since an individual's musculature prevents the variation of movement and needs contact with that individual. This technology would capture a pattern of pictures to analyze the characteristics based on movement (GAO, 2002, p.52). Experimental results have confirmed that there is potential for this technology and further testing is needed to determine advantages, limitations, and performance (GAO, 2002, p.52).

Ear Shape Recognition

Ear Shape Recognition is currently under development and it is the concept of measuring and analyzing the specific shape and size of each individual's ears and its structure is based on the cartilaginous part of the outer ear. There are no commercial systems available for this presently (GAO, 2002, p.52).

Table 3

Emerging Biometric Technologies and Their Maturity



Technology	How it works	Maturity
Vein scan	Captures images of blood vessel patterns.	Commercially available.
Facial thermography	Infrared camera detects heat patterns created by the branching of blood vessels and emitted from the skin.	Initial commercialization attempts failed because of high cost.
DNA matching	Compares actual samples of DNA rather than templates generated from samples.	Many years from implementation.
Odor sensing	Captures the volatile chemicals that the skin's pores emit.	Years away from commercial release.
Blood pulse measurement	Infrared sensors measure blood pulse on a finger.	Experimental.
Skin pattern recognition	Extracts distinct optical patterns by spectroscopic measurement of light scattered by the skin.	Emerging.
Nailbed identification	An interferometer detects phase changes in back-scattered light shone on the fingernail; reconstructs distinct dimensions of the nailbed and generates a one-dimensional map.	Emerging.
Gait recognition	Captures a sequence of images to derive and analyze motion characteristics.	Emerging; requires further development.
Ear shape recognition	Is based on distinctive ear shape and the structure of the cartilaginous, projecting portion of the outer ear.	Still a research topic.

Source: GAO analysis.

Accuracy of Biometric Technologies

The accuracy of biometric technologies is based on three key performance metrics the False Match Rate (FMR), False Non-Match Rate (FNMR) and the Failure to Enroll Rate (FTER) (GAO, 2004, p.11).

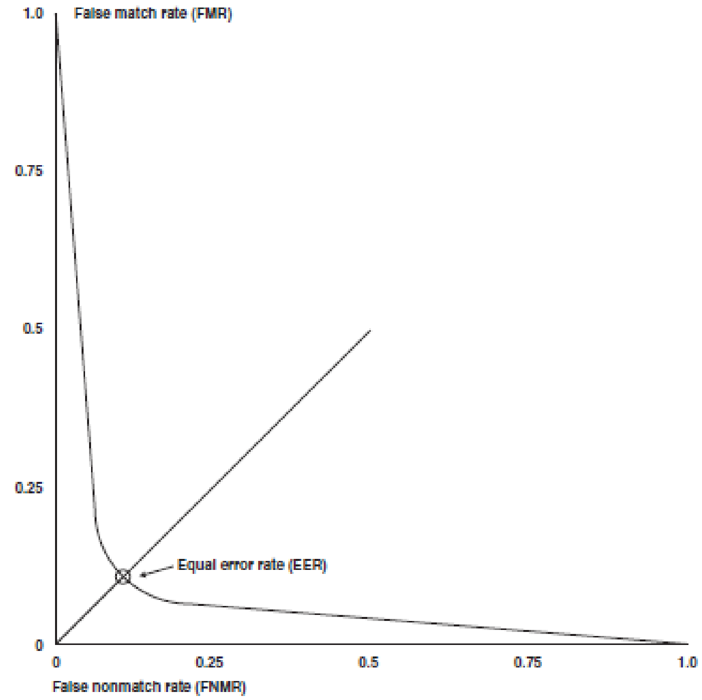
The *false match rate* happens when a biometric system matches incorrectly an identity, and that the individuals have been wrongly matched (GAO, 2004, p.11). In positive identification and verification system, unauthorized people may be granted access to resources and facilities because of incorrect matches. In negative identification systems, the result of a false match can be to deny access (GAO, 2004, p.11). For example, an applicant may be denied access to benefits to a government benefits program, if it is falsely matched to a person that has previously enrolled in the program and is registered under a different identity (GAO, 2004, p.11).

The *false non-match rate* happens when a biometric system rejects a valid identity and is the probability of valid individuals being wrongly not matched (GAO, 2004, p.11).

In positive identification and verification systems, people can be denied access to resources and facilities as the system may fail to make a correct match (GAO, 2004, p.11). In negative identification systems, a false non-match can grant access to resources that should be denied to the individual. For example, if an applicant has enrolled in a government benefits program under another identity and is not matched correctly, he or she will gain access to benefits (GAO, 2004, p.11).

The high similarity between two individuals' traits can produce false matches; while having a low similarity between two individuals during enrollment can be affected by various conditions is what causes false non-matches. It is important to consider that an individual's biometric data will change through time based on aging and sometimes injuries (Biometrics, 2010). If both the error rates are zero, it would make the biometric system perfect, but biometric systems cannot identify individuals by 100 percent accuracy and therefore a trade-off has to exist within the two (GAO, 2004, p.11).

False non-match and false match are related as they must be assessed towards the levels of risk that are acceptable. These risk levels must be balanced with the limitations of inconvenience (GAO, 2004, p.11). For example, in access control environments, perfect security would require denying access to everyone and granting access to everyone would result in denying access to no one. Neither extreme is reasonable, and biometric systems must operate somewhere between the two (GAO, 2004, p.11).



Source: GAO.

Note: Equal error rate is the point at which FMR equals FNMR.

Figure 9: The relationship between FMR and FNMR

An additional metric is derived from false match rate and false non-match rates that vendors used as the equal error rate to demonstrate the accuracy of their biometric systems. The equal error rate is the point where the false match rate equals the false non-match rate (GAO, 2004, p.15). When a biometric system is at a threshold that is at its equal error rate; an individual that is falsely matched, is the same as an individual that is falsely non-matched (GAO, 2004, p.15). However, this statistic explanation tends to over simplify the balance between the false match rate and the false non-match rate because in the real world, few applications the need for security is identical to the need for convenience (GAO, 2004, p.15).

The *failure to enroll rate* measures the probability that an individual will be unable to enroll. This may come from not having a unique biometric sample or the system design makes it hard for an individual to give biometric data (GAO, 2004, p.15). For example, the people who work manual labor extensively, their fingerprints are too worn to be captured and in retina recognition systems a high number of individuals are unable to enroll because of the precision it requires (Biometrics, 2010).

Furthermore, people who cannot speak are unable to use voice recognition systems and people without fingers or hands from injuries, congenital disease, and surgery amputation cannot use hand geometry and fingerprint systems (Biometrics, 2010). 1 and 3 percent of the population cannot use any one biometric system as they do not have the required body part needed; and so are not counted into the system's failure to enroll rate (GAO, 2004, p.15).

In order to meet performance requirements, vendors of biometrics systems are incorporating two or more biometrics systems, as one biometric capture system may have high failure to enroll rates (Biometrics, 2010). Depending on how the biometric system is programmed, it can operate for either identification or identification purposes. Recent studies have demonstrated through experimental results that the identities established by systems that incorporate more than one biometric are more reliable, can be applied to large target populations, and improve response times (Biometrics, 2010).

Criticisms of Biometrics

Besides the important benefits over security measures that biometric technologies may provide, there are issues and concerns. Government agencies and organizations realize the significant advantages that biometric technologies have in improving and monitoring identity identification and verification, yet, a major concern is tracking and data management (Bocozk, Buster, Fitzgerald et al, 2005). According to the International Biometrics Group (2008) the most negative part of biometric identification systems is their ability to locate and track people. Many surveillance systems seem to track and locate people and biometric systems are used because of their high level of accuracy (p.4).

The loss of privacy is another serious concern surrounding the use of biometrics (Archarya, 2006; Baird, 2002; Cavoukian 1999; European Commission, 2005; Jain, Ross, & Prabhkar, 2004). The global implementation of the use of biometric systems has increased and the concern for privacy and an individual's right to that privacy have increased as well. "In the United States, the freedom of the individual is perceived to be closely related to his or her ability to operate somewhat autonomously and anonymously in the eyes of the states, as well as, other organizations that collect data from individuals without permission" (Woodward, Webb, Newton, Bradley, & Rubenson, 2001, p.22).

According to Cavoukian (1999) privacy is what an individual does in their own space and whom they choose to interact "with trust, sense of freedom and openness, or with distrust, sense of insecurity and fear" (p.29). Furthermore, an individual's interest and autonomy usually will rise when the person feels like their privacy is threatened by others (NSTC, 2006d). According to privacy rights advocates, biometric technology will violate the individual’s right to privacy and invade confidentiality (Vollmer, 2006). A biometric per say is not considered good or bad, it depends on how the biometric system is designed, developed, and implemented (Pilgrim, 2007). The biometric industry and organizations are apprehensive about privacy, as it a significant problem in regards to the collection of personal information (ANSI, 2005).

The majority of apprehensions related to privacy are based on the rights of the individual, data mining, and the managing of biometric data by an organization (Allan, 2002). Discussions related to privacy concerns focused on individuals, as they do not have power over the managing of their personal data that could easily be misused and abused (Allan, 2002). The different forms of privacy by Tiresias (2008) are:

- Privacy protective: Is a system used to limit access or protect personal information providing a form for the individual can established a trusted identity.
- Privacy sympathetic: Is a system that limits the access and the usage of personal data by making decision by design related towards the transmission and storage of biometric data.
- Privacy neutral: Is a system where privacy is not an issue and its potential impact to privacy is light. These systems are hard to misuse from a privacy point of view as it does not protect personal privacy.
- Privacy invasive: Is a system that enables and facilitates the use of personal data in an unstructured matter allowing for privacy principles acceptance (p.8).

Privacy rights advocates do not accept the use of biometrics and other forms of verification for capturing information about individuals for the fear of having a "surveillance society or police state" where private companies and governments collect large quantities of personal information without justification (Archarya, 2005, p.8). Therefore, the adoption of biometrics becomes an issue of physical privacy, creating greater anxiety of state watching in the blanket term for national security (Archarya, 2005; ANSI, 2005; Rand, 2001; Woodward et al., 2001).

In addition, the elevation of the trepidation of physical privacy can lead to stigmatization, hygiene, and actual harm (ANSI, 2005; Woodward et al., 2001). Additionally, the disapproval of biometric technology is the function creep. The term function creep refers to data collected for one reason and then is used for another unintended purpose without justification and to take advantage of the authorization of data subjects (Archarya, 2005). According to Tiresias (2008) function creeps are a direct violation of privacy principles.

The use of the Social Security Number (SSN) is an example of the function creep in the society of the United States. The original social security cards had the label "Not for Identification", then, by 1961, the Internal Revenue Service (IRS) began using social security numbers for purposes of tax identification (Lease, 2005, p.57). In 2002, employment, credit, insurance transactions, and state driver's licenses require the social security number, even though it is not needed to complete the transaction (Lease, 2005, p.57). Furthermore, a controversial concern surrounding the use of biometrics is data catalogued though the collection of personal information. Data catalogued is a reduction of the individual unique identifiers in association with committed crimes (Watkins, 2007).

Biometric data is not easy to modify as once the digital identifier is compromised, it cannot be used for identification and verification into the records of the system's database (Watkins, 2007). Under the use of this technology, automatic recognition is controversial because its purpose is to have human errors prevented. However, when the system does not respond properly, there is no one to correct those mistakes and that becomes the cost for implementing such technology (Watkins, 2007).

Another concern for the resistance of biometric technology is health and hygiene. Users of the technology may experience anxiety based on the cleanliness of the sensors used to collect data from irises, fingerprints, and facial scans (Bocozk et al, 2005). Presently, there are no studies demonstrating of any health concerns associated with the use of biometrics. However, the idea may produce fear in users or discourage them from enrolling or accepting the verification process of biometric technologies (Bocozk et al, 2005).

Those health concerns would have to be investigated by health professionals, subject matter experts and vendors of biometric technologies. The religious concern towards the use of biometric technology can come from societal emphasis and legal opinions as respect to religious beliefs (Bocozk et al, 2005).

Besides all of the concerns regarding the use of biometric technologies, Lease (2005) stated, "supporters of biometric authentication systems argued that properly deployed and equipped with adequate best practice controls, biometric systems can actually function to enhance and protect privacy" (p.57). Experts in biometric technology stated that the potential for this technology is tremendous, but the need for privacy principles and the ability to protect users from unauthorized intrusion is important (Cavoukian, 1999).

As the government continues to adopt and implement this technology quickly, the right to privacy of the individual is being threatened (Vollmer, 2006). The government must implement safeguards that need to be incorporated into the technology, so that the individual's intrusion of privacy is minimal and public safety and protection are maximized (Vollmer, 2006). The bottom line is that the system's design, deployment, personnel training, and use must have protections for personal privacy (Lease, 2005).

Privacy provisions are not subject to just government institutions, businesses need to accept responsibility for protecting consumer data and their privacy. According to Cavoukain (1999) the use of biometric information must balance effectively and appropriately a customer's right to privacy and must be for legitimate business purposes as organizations should deployed and adopt requirements for the promotion of fair information practices (p.44). The purpose of fair information requirements and practices is to reduce and avoid unauthorized data collection that is unreasonable, unnecessary, and unauthorized use, and disclosures (Cavoukian, 1999).

Biometric application through the privacy enhancing of privacy technologies (PETs) is a solution offered by ANSI (2005). PETs are systems of information and communication technology (ICT) measuring privacy protection through the reduction and elimination of personal data and through the prevention of undesired processing without losing the functionality of the data system (ANSI, 2005). Privacy watchdogs have already protested the use of biometrics to verify and identify individuals, but it is important to incorporate safeguards and privacy principles in the protection of an individual's security and to lessen the compromise of consumer data (ANSI, 2005). By implementing those items, individuals have the peace of mind that their information is secured and controlled; and not sold to third-party vendors (Nwatu, 2011). Organizations will be trusted more by the public if their systems and data are viewed as protecting privacy and enhancing security (Nwatu, 2011).

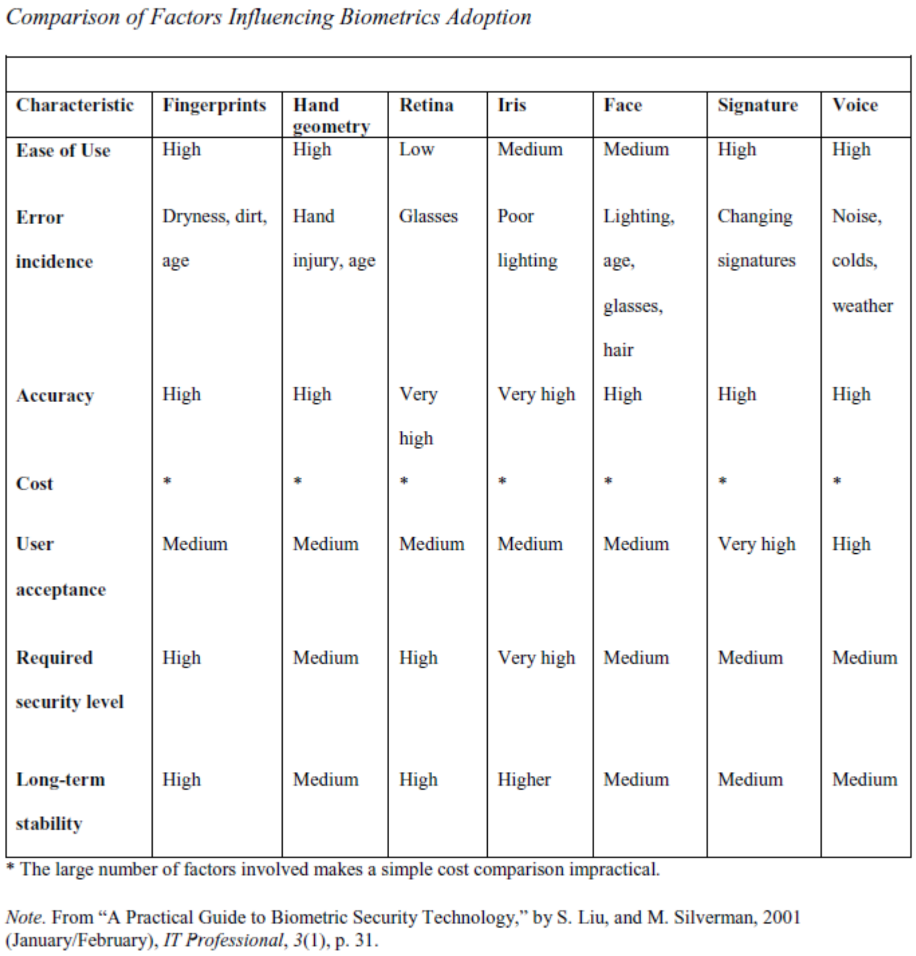
Technology Acceptance Model by Davis (1989)

The incorporation of any biometric system in any government program cannot neglect the TAM model and its usage on how large populations may perceive the use of recent technologies. Davis (1989) model provided a valid and reliable measure that predicts the acceptance or adoption of new technologies by end-users and is used to measure technology acceptance (King & He, 2006).

According to Liu and Silverman (2001) several factors affect the adoption and acceptance of biometric systems to include accuracy, costs, user acceptance, error incidence, required security level, and long-term stability affect in whether a biometric system will be deployed or not. Additionally, Rajchel (2007) stated "that the lifestyle of the system, invasiveness, hygiene and health, religion, culture and ethics would affect implementation". Table 4 illustrates the different factors impacting the adoption of biometric technologies (Liu & Silverman, 2001). The TAM plays an important part in the implementation toward the adoption of biometric systems and although, the authors of the model may have various viewpoints, analyzing the need to make the decision to adopt, is based on financial resources, the type of biometric technology to use and the availability of experienced personnel.

Table 4

Comparison of Factors Influencing Biometrics Adoption



Comparison of Factors Influencing Biometrics Adoption

Characteristic	Fingerprints	Hand geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very high	Very high	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
Required security level	High	Medium	High	Very high	Medium	Medium	Medium
Long-term stability	High	Medium	High	Higher	Medium	Medium	Medium

* The large number of factors involved makes a simple cost comparison impractical.

Note. From "A Practical Guide to Biometric Security Technology," by S. Liu, and M. Silverman, 2001 (January/February), *IT Professional*, *3*(1), p. 31.

The TAM is the theoretical framework that allows for the understanding of how perceived ease of use and perceived usefulness will influence an individual's behavior and attitudes towards the adoption of the use of the technology being implemented (Klopping & McKinney, 2004; Nqugi, 2005; Wahid, 2007). When understanding the various factors that will affect the implementation of technological systems, the model enables the improvement of the system's design, deployment and adoption strategies, and user acceptance (Shen, Laffey, Lin & Huang, 2006). The literature related to this model has been receptive and popular as it continues to be used to clarify the various influences that can determine the acceptance of technology in organizational environments (Mahinda & Whitworth, 2005).

The model uses the factors of perceived usefulness and perceived ease of use in order to determine the possible technology adoption, acceptance, and usage (Shen, Laffey, Lin, & Huang, 2006). The author of the model concluded that perceived usefulness (PU) and perceived ease of use (PEOU) affected attitudes and behavioral reactions toward the usage of technologies such as biometrics (Shen et al., 2006). For example, individuals using the technology may believe that it will be useful, easy to use, and reliable in identifying people and an enhancement to their personal security (Shen et al., 2006).

These beliefs would generate attitude or behavioral reactions furthering an interest in the use of the technology. Furthermore, if users believed that the system is complex and does not have reliable performance, then the behaviors toward the system will be negative impacting the adoption of the technology. External variables such as the characteristics of the system's design, available training, interest, awareness, and documentation will heavily impact the usage of the technology (Wahid, 2007).

Biometric technology vendors find it hard to incorporate the model operationally as it goes under the implementation level (Ngugi, 2005). As the model has been employed to describe factors that will influence the adoption, the model becomes deficient in reliability, flexibility, and extendibility (Mahinda &Whitworth, 2005). Furthermore, the model is criticized for being incomplete as it does not include other variables that impact the adoption such as privacy, security, and trust (Brydie, 2008; Josua & Koshy 2009, Shen et al., 2006).

In a study conducted by Joshua and Koshy (2009) it concluded that perceived ease of use and security helped determine the attitudes toward the acceptance of technological systems. Afterwards, Kim (2006) realized that physical security was a variable that affected the acceptance of the system by hotel guests; and that reliability and trust were also reasons for adoption (Brydie, 2008). The studies conducted that the acknowledgment of these variables would affect the implementation of the technological systems, by improving the design, deployment and adoption strategies to gain user acceptance (Wahid, 2007).

The model in Figure 10 illustrates the relationship between ease of use, usefulness, and external variables such as those of security, privacy, and trust towards attitude formation toward the acceptance of biometric technologies (Joshua & Koshy, 2009). According to Joshua & Koshy (2009), "the original model that Davis (1989) developed did not include security as a variable. Over the years, researchers argued that other factors would affect the attitudes and behavioral reactions to use technology besides perceived ease of use and perceived usefulness" (Cowen, 2009, Joshua & Koshy, 2009, Jahagir & Begum, 2008; Shen, Laffey, Lin & Huang, 2006).

Ease of Use

Is the extent that an individual would accept at no cost using a method (Jahangir & Begum, 2008; Joshua & Koshy, 2009). According to Jahangir and Begum (2008), "perceived ease of use is the user's awareness that the use of biometrics will be of minimal effort, if an individual understands the technology, it leads to adoption and this is important as it would generate positive attitudes towards acceptance of the system" (p.34).

Perceived Usefulness

Refers to an individual's perception of the outcome of the experience when using a new piece of technology (Jahangir & Begum, 2008). If an individual believes that biometric systems are helpful and effective to protect individual security, and privacy, they will likely accept its use. However, if the individual does not realize the usefulness, it will also affect the adoption (Jahangir & Begum, 2008; Joshua & Koshy, 2009).

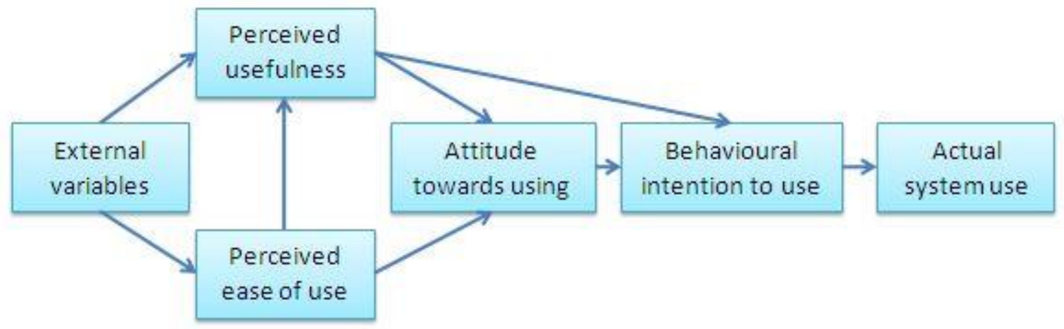


Figure 10: Davis (1989) technology acceptance model

Security

Is the need for preventative measures and identity protection towards unnecessary risks (Jahangir & Begum, 2008). When users perceived that there is reliability and security in the use of the technology, their attitudes towards the technology would be positive (Jahangir & Begum, 2008). Moreover, the sense of loss of safety and unreliability of the system would increase attitudes towards the system to be negative.

Awareness

The level of awareness of the technology would impact its implementation as well as a person's age (Asfaw, 2006; Norris, 2001). Various factors would add an important role in the adoption, implementation, and usability of biometric technologies.

- Awareness of the benefits and effects of the technology to incorporate identity management and fight against identity fraud.
- Awareness of accessibility and availability, and
- Awareness of the daily use of biometrics as a part of life.

The issue of implementation is determined by various factors that could impact the acceptance in the long-term as it could bring change in attitudes and behaviors. High levels of awareness may not always impact the adoption and usability of biometrics, but it is a factor that should be considered in its adoption and implementation strategies (Asfaw, 2006; Norris, 2001).

Attitude

According to Alrafi (2005) behaviors could be negative or positive and the way an individual perceives that experience it what gives such attitude. Attitude is the individual's society, as he or she believes it to be. Behaviors determined an implicit response that is:

1. Considered significant in the individual's society,
2. Based on patterns learned through discrimination and generalization,
3. Self-cueing and drive-producing, and,
4. Anticipatory and mediating in reference to patterns of overt responses (p.4).

If an individual has a positive attitude towards the technology, it is most likely to approve and accept it as a part of life. However, a disapproving feeling would lead to a negative mindset towards any biometric system based on their perceived ease of use, perceived usefulness, awareness, security, privacy, and level of interest of the individual (Joshua & Koshy, 2009; Jahangir & Begum, 2008).

Past research suggested that individuals are not likely to perceive information practices as invasive to privacy when (1) the information used or collected is related to a transaction and (2) the information they believe would be used to draw reliable and valid inferences about them (Baker, 1991; Clarke, 1988; Stone & Stone, 1990; Stone et al., 1983; Tolchinsky et al., 1981; Woodman et al., 1982). As privacy is considered to be the most highly prized rights, it becomes secondary when it comes to threats of physical harm and street crimes (Vidmar & Flaherty, 1985, as cited in Katz & Tassone, 1990).

In the use of Davis (1989) TAM Model, biometrics is an information technology tool that would have to incorporate cultural, gender and demographic differences, as well as, social influence and attitudes towards technology; in order to see if the target population would accept or reject the use of biometric devices (Malhotra & Galletta, 1999). Moreover, the current research points out that understanding specifically who the user is can have an important influence on the technology's acceptability to that user, in this case, it would be the Trusted Traveler who voluntarily participates in the program.

Additionally, the effects of the change in behaviors and attitudes is described in the Cognitive Dissonance Theory, where the use of a product may change one's perceptions, attitudes, and needs when the product has been used. For example, a frequent flyer may experience various trip conditions such as the commute to the airport, airline check-in, security screening, and gate boarding differently versus a non-frequent flyer (Pranic, Roehl, &West, 2008). However, the introduction of a new experience may change the common knowledge of the frequent flyer that could result in altering the perceptions of the frequent flyer into accepting the new security procedures (Pranic, Roehl, &West, 2008).

The Concept of Privacy

According to Warren and Brandeis (1890) “Privacy” is the claim that an individual interest usually arises as an assertion against other individuals or organizations to prevent interference from the individual’s autonomy. It is the desire of each individual for physical space, as he or she can be free of interruption, intrusion, embarrassment, and accountability; it is the attempt to control the manner of disclosures of personal information” (Warren & Brandeis, 1890).

The birthplace of privacy in the United States comes from the article “The Right to Privacy” by Samuel Warren and Louis Brandeis (1890) which provided the example of the conceptual transition from physical place to information space. For instance, in the last fifty years, the Supreme Court used the right to privacy to protect the right to purchase and use contraceptives, the right to have an abortion, and the right to engage in private and consensual homosexual activity (Chemerinsky, 2006, p. 644).

However, the main concern of Warren and Brandeis was with the media that was interested in gossip and revealing personal things about individuals without their consent (Chemerinsky, 2006, p.644). For example, Warren and Brandeis (1890) stated that “photography is an information technology that enabled the collection of information about an individual independent of his or her actual control; creating the capability to use the collected information for any purpose without further involvement or agreement from the individual” (Warren & Brandeis, 1890).

As of current date, the Supreme Court has not clearly articulated or protected the right to informational privacy. In his article in 1960, William Prosser described how privacy came to be established in tort law and the various torts that fit within to include torts for intrusion, public disclosure of private facts, and placing a person in a false light (Chemerinsky, 2006, p. 645). Privacy is about freedom from government intrusion into an individual's home or to an individual's person.

Brandeis made an argument that the Fourth Amendment should apply because people have a reasonable expectation of privacy for their conversations and the unjustified intrusion by the government is a means of infringing on this expectation and deem a violation of the Fourth Amendment (Warren & Brandeis, 1890). Privacy is used in constitutional law to protect aspects of autonomy in which the person has the right to make certain crucial personal decisions.

The present concern is on data aggregation, electronic surveillance, identity theft, identity management, biometrics, warehousing and breaches. The Warren and Brandeis (1890) concern led to specific questions in the field of privacy and to the legal aspects in U.S. Society such as: (1) "What effect should privacy protection have on technology?" (2) "What is the appropriate use of personal information?" and (3) "Should personal information be collected and for what particular purpose or application?"

The National Science & Technology Council (NSTC) broke down the complex term of privacy to make it relevant to the technological advances to today's society.

Decisional

Concerns related to a person's authority to make life decisions that affect the person's life and body and those of the person's family members in end of life issues (NSTC, 2006d).

Spatial

Concerns related to physical spaces to include a person's bedroom, home, car, etc. These issues usually concentrate on the authority of the person to decide who may enter or observe the items and activities that happen in that specific place (NSTC, 2006d).

Intentional

Concerns related to characteristics that are publicly visible or intimate activities. These concerns concentrate on the authority that the person has to bar further communication of an observable feature or event (NSTC, 2006d).Examples are claims against conversations being repeated that happen in public and the publishing of photographs without authorization and unintended nudity (NSTC, 2006d).

Informational

Concerns related to the use of information that pertains to the person. Issues usually concentrate on the extent of the person's authority to control how that information is used (by whom and for what purpose) and the responsibility of the corresponding individuals and organizations to include the person in the decision-making process that would drive the subsequent use (NTSC, 2006d).

The concept of informational would apply to the adoption of biometrics into Trusted Traveler programs as the main focus would be that government organizations would use the biometric data and convert it into electronic data and then make a decision for individuals to be able to access expedited screening. This is the reason why privacy assessments must be made before adoption and implementation of biometric systems (Solove, Rotenburg & Schwartz, 2006).

The term "privacy" is not in the text of the United States Constitution, but the living document does have provisions that incorporate privacy protection. Those provisions are in the First Amendment, protecting against the disclosure of group membership (National Archives, 2013). The Third Amendment protects an individual's home from government intrusion (National Archives, 2013). The Fourth Amendment protects against unreasonable searches of personal spaces, possessions, and body from the government (National Archives, 2013). Last, the Fifth Amendment is the protection against forced disclosure of self-information (National Archives, 2013).

For instance, the Fourth Amendment main focus is on unreasonable search and seizures, which includes a review of the expectation of privacy for the individual (National Archives, 2013). The individual must have an actual expectation of privacy and that expectation must be reasonable in the given circumstances (Solove, Rotenburg & Schwartz, 2006). For example, biometric systems must considered and inform the individual of the development, operation, and its implementation (Morosan, 2012).

Just like the privacy provisions in the U.S. Constitution, Privacy Torts are additional sources of privacy protection. In civil law, torts are civil injuries that an individual could be compensated. There is a possibility that an individual could file a claim related to the use of biometric data, at which point the details of what does or does not qualify, and the measure of the injury would become the focus (Prosser, 1960). According to Prosser (1960), these privacy torts are categorized as "(1) Interfering with an individual's private affairs, (2) Sharing embarrassing information about the individual, and (3) Using someone's name or image for personal gain"(Richards & Solove, 2010, p.9).

As the U.S. Constitution has privacy provisions, states laws have also been in place to protect the individual's right to privacy extending those of federal jurisdictions. As a result, each biometric system that is use exists only within the legal jurisdiction of the tribal, local, state, and federal laws (NSTC, 2006d). Therefore, the laws of each place must be reviewed and incorporated into the strategy and design of the biometric system in order to operate and be administrated in (NSTC, 2006d).

The legal jurisdiction to biometric systems does not just extend to those in the United States, but also into international governments. International agreements with the European Union (EU) and the Asia Pacific Economic Cooperation (APEC) created frameworks in the sharing of fair privacy principles when dealing with personal information (NSTC, 2006d). The framework encourages participation of the individual granting them the right to know what is the personal information being collected, the right to request a copy of the information, and the right to appeal the accuracy of the data including the chance to have it erased (NSTC, 2006c.)

In the case of the adoption of biometrics into Trusted Traveler programs for the use of expedited security screening, it would exist in multiple jurisdictions within the United States and would cross international boundaries (NSTC, 2006c.) International connections would exist through the physical equipment used by the system, the information in the system, the individuals using the system, and the individuals' information in the system (NSTC, 2006c)

The real concern relating to the privacy of information is its ability to connect to the interest of the individual. This connection is personal information as any information could be used to identify the individual in any way. Not all data may look like personal information, but can be through its use (Commerce, 2000). For example, if data is use in combination with other data and results in the identification of the individual either intentional or unintentional the data becomes personal information and privacy issues become a concern (NTSC, 2006d).

The privacy impact of combining data for the purpose of identifying individuals' reaches to the point; to the intent to identify is the reason biometric information justifies as personal information through its content and its use (GAO, 2010, p. 21). Where there is the use of biometric information, there is personal information involved and privacy concerns need to be addressed to determine the impact of the use of the data, and how it relates to the individual's privacy interests (NSTC, 2006).

Legal Authority and Privacy Provisions

The law and the legitimate public policy that governs biometric systems must be clearly articulated, previously disclosed, and related to its original purpose. The collection and use of personal information is based on a legal authority through an agreement or law. An individual decides to participate in a system or program based on the individual understanding of what he or she is giving and what he or she is getting in return (NTSC, 2006c).

According to Moroson (2012):

> “The privacy assessment of a biometric system should explain the context and authority to the user. It should further explain the original collection of biometric information and illustrate that all system functions; including information sharing, the grounds to its legal authority and the details are articulated and available to the individual, before personal information is collected” (p.440).

The use of biometric systems could be modified through time and privacy protections must be applied. The most important privacy consideration to keep is the ongoing management of biometric systems on the bases of information privacy. Private industries have different requirements for the use of biometric systems, in regards to medical, financial, and minor children. However, government institutions have three laws that must be incorporated in their protocols (Morosan, 2012).

The collection and use of personal information by the government is controlled under (a) The Freedom of Information Act of 1966, which provides access to any government record to anyone for any purpose with the exception to include the protection of personal privacy, (b) The Privacy Act of 1974 that has a set of fair information principles to govern the government’s collection, use, and maintenance of PII contained in a system of records; and (c) The Government Act of 2002 which requires government agencies to conduct assessments of the use of information technology and its potential impact that use could have on privacy (Nelson, 2004).

It is essential to understand the individual’s concern towards privacy protection, as it is threatened, especially when information used by the system is based on health, financial status, or used by the government for other means that are clearly not disclosed

(Neyland, 2009, pp.135-136). The biometric system must be clear in its design and implementation strategies to address the concerns of the individual and illustrate that the information collected would be used only for such functions and nothing else, preventing the *function creep* (NSTC, 2006a).

Privacy advocates argued that these national databases would operate on a presumption of accuracy, but who would be responsible for those amendments, costs, and the process it would involve. Furthermore, privacy advocates suggest that the national ID scheme offers the chance for favored companies to win lucrative government contracts expanding their self-interests (Neyland, 2009, pp. 145).

Nevertheless, misidentification, problems with confirming identification, and others using or manipulating identity information, could lead to problems for a broader constituency (Neyland, 2009, pp. 145). Therefore, the politics built into the technology include inclusion boundaries (good to almost everyone) and exclusion boundaries (those to be targeted), would be depended on the terms of “feasible” and “reasonable” arguments that would depend on the ability to successfully manage these boundaries (Neyland, 2009, pp. 145)

According to Neyland (2009), National ID policies such as those of the Real ID Act of 2005 involve claims regarding the advantages and disadvantages of large-scale databases, connecting each other with regards to millions of people. The advantages in using biometrics under National ID policies are (a) fights against illegal working by preventing employers from employing staff without having the proper documentation, (b) prevent immigration abuse by making the country less attractive for asylum seekers, (c) prevent the use of false and multiple identities' by terrorists and criminals, (d) ensures that free public services are only used by those entitled to them, preventing the abuse of health tourism, and (e) help to protect people from identity theft where victims have their identities stolen by others who may use the identity for financial or some other gain (Neyland, 2009, pp 15-16).

However, Neyland (2009) mentioned the disadvantages on posing set policies on the use of biometrics based on organizations against National ID policies, as these National IDs are unreasonable, unnecessary, and technology is not feasible. Those claims are based on the following arguments: (a) terrorism is not based on issues of identity, but tied to various political situations around the world, (b) benefit fraud is committed through the under or lack of reporting of income (not identity) and, (c) identity theft may increase through the ID card scheme with criminals, by registering their own biometrics under another name and gaining access to computer records (Neyland, 2009, p.15-16).

Nevertheless, Neyland (2009) suggested that a series of privacy concerns are subject to the flexibility of the interpretation of legislation. Therefore, depending on the interpretation, governments would use the technology for (a) impose fines and imprisonment for failure to enroll or obtain a national ID, (b) decide to share information with third parties, (c) limit powers to protect the population, (d) not all interpretation of legislation would fit international organization compliance requirements, and (e) cards with chips would produce audit trails that are not clear for what and who it would be useful (Neyland, 2009, p.16).

The Use of Biometrics for Aviation Security

The DHS and its agencies have been exploring the use of biometrics in aviation security in these areas:

- The verification of the identity of airport employees to ensure that access to secured areas are restricted to authorized personnel only;
- The protection of public areas surrounding airports with the use of surveillance systems;
- Verification of passengers when boarding aircrafts; and
- Verification of flight crew before and during a flight (GAO, 2004, p.20).

Purchasing airline tickets to travel and border crossings are the focus for expressing concerns regarding privacy and forms of surveillance in the light of new technological developments. Airport managers have expressed the use of biometric systems in their airports based on reducing the speed of security checks in favor of increasing profit from the retail properties inside of airports.

For example, the use of facial scans for more rapid security checks would save time on the passenger, therefore, the passenger would spend extra time on shopping (Neyland, 2009, pp.136). Furthermore, the use of a chip in storage cards would allow airport managers to know who was who and their location in the airport as a means to enhance security by stopping access into prohibited areas, as well as, for passengers who had check-in but did not made their flight (Neyland, 2009, pp.136).

According to Neyland (2009) airport managers expressed mass problems that a biometric device might generate based on problematic identity claims and airports might not want to diminish their security records (Neyland, 2009, p.151). In developing the biometric technology for the use in airports, it has to be measured in an airport environment and the views of stakeholders have to be considered. Vendors have to take into account what those technologies might be able to do, which ones to build, and who would be the beneficiaries of the technology.

Airport managers have to consider the potential for increased security, enhanced information regarding passenger movement, and increased shopping revenue against possible problems in identity confirmation and constant problems with security delays and security lapses (Neyland, 2009, p.151).

Challenges and Issues to the Adoption of Biometrics Technologies

The limitation of technology has to be taken into account in the security process. For example, exception-processing procedures must be planned carefully as not all people can be enrolled in the biometric system. However, exception-processing that is not appropriate when primary is biometric processing could be a vulnerability to security, as it could be exploited and directly affect the performance of the technology (GAO, 2004, p.18).

In a study conducted by the General Accountability Office (GAO) for border security, it was concluded that recognition of the fingerprint is the most developed of all current biometric technologies in the market (GAO, 2004, p.19). Fingerprint recognition is the longest in used and with databases containing up to 40 million entries, enables it to be constantly expanding (GAO, 2004, p.19). The issuing process of credentials must be considered into the process in any form of identity management system (GAO, 2004, p.19).

Biometrics help to ensure that people presenting themselves before the security system is the same as the person enrolled in the system (GAO, 2003, p.10). The purpose of the biometric is to identify and verify an identity, so to establish multiple identities could be a very difficult task as the system is to have one true identity. Therefore, biometrics cannot connect a person to his or her unique identity, if it was connected to a false identity from the beginning (GAO, 2004, p.10).

The selection to incorporate the use of biometrics as a security solution must consider the costs and benefits and its potential effects on privacy and convenience. The investment into a biometric system and its benefits, as well as, costs needs to be assessed and analyzed before its incorporation (GAO, 2003, p.20). An organization's goals must take into consideration the desired objectives of the system as to the matching of identities on a watch list or the verification of identities as to verify that individual is who he or she is. Particular performance requirements must be described, as the time it would take to verify a person's identity, and the maximum number that the system can hold (GAO, 2003, p.20).

Once the system performance requirements are set, a cost analysis could be created. The costs of the technology must be taken into consideration, as well as, the target population that it would affect (GAO, 2003, p.10). Initial costs must include efforts in engineering of the design, testing, system implementation; personnel training, network infrastructure, hardware and software, and additional facilities for the enrollment of people in the biometric system (GAO, 2004, p.15).

Recurring costs factors include software and hardware system maintenance, hardware acquirement, training personnel, and program management (GAO, 2004, p.18). Additionally, other costs include hiring personnel for the enrollment process of people in the biometric system and purchasing identification documents for biometric storage. The consequence of performance issues such as accuracy problems, and their effect on the process, and people are important in selecting the right biometric solution (GAO, 2004, p.18).

Effects on Privacy and Convenience of Use

Federal agencies are limited on the disclosure of personal information as it relates to collection, storage, and usage of biometric information of fingerprints and photographs by the Privacy Act of 1974 (GAO, 2003, p.20). However, the act does include exemptions for national security and law enforcement purposes; and representatives of privacy and civil liberties groups have raised concerns related to (1) the adequate security protections put in place to handled identify theft, data sharing, and uses for biometric data, and (2) secondary uses also known as function creeps (GAO, 2004, p.20). Those concerns are related under the current law, as the legal system in the United States has not addressed the large-scale of data handling by a biometric system (GAO, 2010, p.10).

The broad exemption of the Privacy Act of 1974 does not provide guidance on its appropriate use for biometric information as it relates to national security or law enforcement purposes (GAO, 2004, p.20). Since there are no general consensuses, or criteria on the appropriate use of data sharing on the usage of biometric technologies, there must be a balance between matters of security and privacy as it pertains to biometric system usage (GAO, 2004, p.21). Discussions on policy decisions are required as the current legal system has a range of unresolved policies, suggesting that the use of biometric technologies is based on management and technical policies (GAO, 2004, p.21)

Furthermore, consideration must be applied in the use of biometrics and its convenience would impact the government's ability to achieve its goals. Some individuals could find the use of biometric technologies difficult and could resist it based on the personal beliefs of being uncomfortable to use, offensive, or intrusive (GAO, 2004, p.21). A biometric system's performance and adoption in commercial airports could be affected by an individual's lack of cooperation and resistance, as the process could be lengthy or erroneous.

This could negatively affect the ability of the biometric system to operate and fulfill the government's mission (GAO, 2004, p.21). The concern to adopt and use biometric technologies into the expedited screening of passengers in a commercial airport environment is based on the speed it would take to process each passenger and the accuracy of the verification rate that the technology would produce when deployed at airports (GAO, 2006, p.24).

Cavoukian, Chibba, & Stoianov (2012) in their research focused on having encryption into the biometric template of a person for the protection of privacy and use a numerical sequence to verify the individual. The government through its research through the GAO has not provided that solution in its biometric systems deployed in facilities and for further use in other areas (GAO, 2010, p.26). Furthermore, security cannot be based on technology alone, but through ATSA it did encouraged the adoption of biometric technologies to enhance security systems. Additionally, presidential directives have been signed to adopt biometric technologies, but agencies with a mission in national security have yet to implement such systems into aviation security.

Even though, the use of biometric systems is not 100% accurate in security systems, it does allow for some accuracy when it comes to the identification of an individual as required by the 9/11 Commission Report. Additionally, the privacy rights of the individual must be protect by federal law, but since Trusted Traveler programs are voluntary, the individual provides consent to have its privacy rights waived in an exchange for a faster security experience.

Summary of the Literature Review

The focus of the comprehensive literature review in this study was conducted to discuss expedited screening in Trusted Traveler programs within the DHS agencies dealing with aviation security, the adoption of biometric systems as a layer of security in commercial airports and its privacy provisions. An example of the use of biometric systems for identity verification was use to illustrate how the TSA uses the technology for its TWIC program. A description of biometric systems and the different types was used to provide examples of positive and negative outcomes of the various acquisition devices.

Davis' (1989) TAM was presented to illustrate how an individual perceived ease of use and perceived usefulness affects the individual's attitudes towards the acceptance of the technology that would be adopted into commercial airports. A descriptive of the accuracy of the various biometric technologies reflects the positive and negatives outcomes when being integrated into the verification process of travelers in expedited screening. Furthermore, the description of the concept of privacy by Warren and Brandeis (1890) and by legal experts under tort laws illustrates a modern day approach to what is considered a person's individual right to privacy.

Risk-based security was the foundation for the Trusted Traveler programs and for DHS agencies to apply their resources to become more efficient and effective as an organization. Examples of how biometric systems and their positive and negative effects were reflected on government assistance benefits programs to demonstrate the use of biometrics as a government statue.

The legal authority was presented to illustrate how legal jurisdictions subsequently affect the adoption and implementation of biometric systems and their compliance with federal, state, local, and international agreements. Lastly, the challenges and issues on the adoption of biometrics takes into account that biometric technology has its limitations and not all members of the population could enroll in such programs. Limitations such as congenital diseases, injuries, or the aging process, and the performance of the technology, must be kept to be relevant through time.

Additionally, the effects on privacy and convenience were presented to describe the trade-offs of personal privacy for modern day convenience of faster security checks. The information provided in Chapter 3 described the methodology that was used to conduct this study.

Chapter 3: Research Method

Introduction

The purpose of this study was to investigate and explore if privacy concerns of travelers would be a factor in the adoption of biometric technologies in expedited screening procedures in commercial airports. In addition, does ease of use, usefulness, awareness of the technology, and security contributed to the adoption of biometric technologies in the expedited screening process at commercial airports as it related to Trusted Traveler Programs.

Chapter 1 introduced the study and the problem statement and Chapter 2 illustrated the relevant literature on expedited screening, risked-based security, biometric technologies, and the concept of privacy. It also addressed legal authorities, and privacy provisions; and the use of the TAM that created the theoretical foundation for this study. Chapter 3 explains the research approach that was utilized for this mixed-method investigation.

Research Design and Approach

In this mixed-method research study, the research questions were the foundation for the approaches that were used. The perception of privacy and the experiences of travelers using biometric systems reported to the DHS Privacy Office provided the attitudes and behaviors determining that the data would be of a qualitative nature.

The case study approach was used as it involved developing an in-depth analysis of multiple cases (Teddlie & Tashakkori, 1998, p.25). The data collection for a case study approach involves various sources that include quantitative data relevant to the overall research design (Teddlie & Tashakkori, 1998, p.25). This study used a purposive sampling method as it selected a small sample of units because of the valuable information to the research questions (Teddlie & Tashakkori, 1998, p.25). Contextual (holistic) strategies were used to interpret data in the context of a whole to include interconnections among all of the elements. The entire study was of a inductive-deductive cycle as at some points it would move towards a grounded result (facts and observations) as an inductive inference to a general inference (TAM) through the deductive inference of similar predictions (Teddlie & Tashakkori, 1998, p.26).

Data Collection

The data collection consisted in a document review of previous peer reviewed journals, articles, and studies conducted on the effectiveness of biometric technologies and the attitudes and behaviors that could be generated if the technology would be implemented. The evaluation of privacy had to be considered, but it could not be based on the perception of an individual, as the federal government defines the concept of privacy based on the Privacy Act of 1974. The DHS Privacy Office collected and reported the privacy complaints of Trusted Travelers during the enrollment process or while experiencing the use of biometric technologies at ports of entry. These privacy reports are reported to Congress on a semiannual basis and are distributed without the disclosure of PII.

The DHS Privacy Office collects privacy complaints base on a set criteria that the federal government has categorized as violations based on the Privacy Act of 1974. These complaints are formal and DHS must take action to resolve the issue within a seven to ten day period (DHS Privacy Office, 2012). I went to the DHS Privacy Office public website under archived annual privacy reports from (2011-2014) that provided the data that would answer the first research question in regards to privacy.

Secondly, the TSA made available the numbers of Trusted Travelers processed through expedited screening and those enrolled in TSA Pre-Check, public information through a study conducted by the GAO. I used those numbers and features to confirm them through the TSA databases, but could not disclose additional information as these databases are sensitive security information (SSI). The quantitative features provided the data as to demonstrate how expedited screening was deployed at commercial airports.

Additionally, I gathered public information through social media networks with the #TSAprecheck, #GlobalEntry and #TrustedTraveler to get a higher sample size than those obtained by the DHS Privacy Office (2011-2014). The information on social media networks provided more detailed information into the reactions of the population participating in Trusted Traveler programs and their experiences with biometric technologies and expedited screening at airports.

Variables: Independent and Dependent Variables

In this study, the variables determine the findings and outcomes of the research conducted. I decided to have multiple variables that would create various outcomes. For example, a variable can take different values according to treatment, scenario, and other factors. In this study, I referred to independent variables as what has determined the outcome of a dependent variable (Creswell, 2007, P.152). For instance, in this study privacy, ease of use, usefulness, security, and awareness of the technology are independent variables that could affect the outcome, which is the dependent variable if biometric technologies would be used and adopted into the expedited screening procedures at commercial airports. I wanted to explore the relationship among the variables and its effects on the possibility of biometric technologies be deployed as a security measure, if the technology was to be expanded as other agencies had.

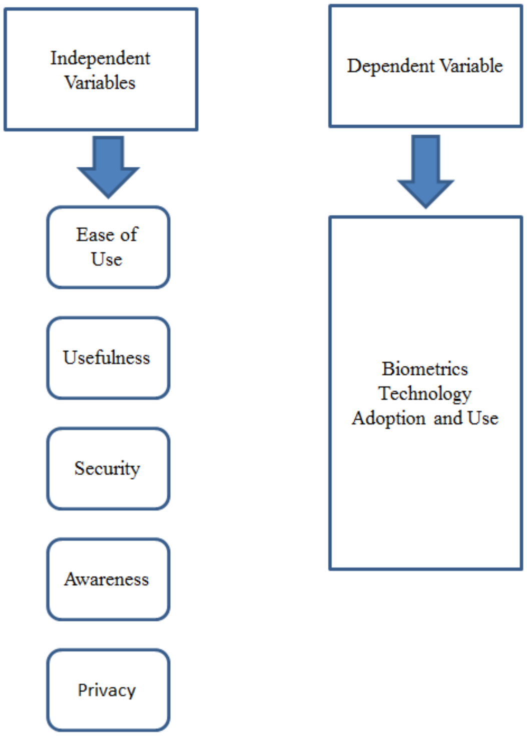


Figure 11. A graphic representation illustrating the independent variables and the dependent variable.

Setting

The TSA is responsible for implementing security screening procedures in 450 airports in the United States and its territories for outgoing travelers through aviation security. The CBP is responsible for the screening of incoming travelers into the United

States from aboard. Currently, 121 commercial airports have expedited screening through the participation of Trusted Traveler Programs. These airports have on-site enrollment centers for those wanting to enroll in the program after viewing the process through prior security experiences. The archived data of this study was obtained from airports providing expedited screening specifically to Trusted Traveler program participants.

Databases

Publicly available GAO and OIG vetted data (reviewed and redacted), was used in this study. The information is based on actually Trusted Traveler program participants reported into the Performance Measurement Information System (PMIS), an application that assists authorized users throughout the TSA to report and track all of the Trusted Travelers processed through security screening checkpoints on a daily basis. The system keeps a running total of all of the Trusted Traveler participants processing in all 450 airports, as other airports have expedited screening of the individual, but not of their belongings.

In addition, the Performance Information Management System (PIMS) allows those who have access the capability of generating a variety of reports for viewing based on set parameters (e.g. date range, region, busiest time, etc.) when required. Reports could be made to illustrate Trusted Traveler expedited screening by an airport, lane, busiest time, and date. The information is based on Trusted Traveler processing by the categorization of “LLLL” documented and reported into PMIS by all of the TSA airports.

The TSA offers expedited screening in seven categories (Appendix B) in the PMIS database, and this research study only focused on expedited screening for travelers enrolled in a Trusted Traveler Programs administrated by a DHS agency. Data was collected from several audits and reports gathered from commercial airports and point of entries implementing expedited screening by the GAO and OIG. Those reports illustrate the process and security assessments of biometric technologies in border and aviation security. The information contained within the assessments and those analyses are considered public.

Research Questions and Hypotheses

Research Question 1: Do privacy concerns of travelers affect the adoption of biometric technology into the expedited screening procedures at commercial airports?

This question was answered by the analysis of the qualitative data that was obtained from the formal complaints of the DHS privacy reports. The data was analyzed based on a case study approach. The case study approach allowed me to conduct a qualitative analysis based on a specific way of collecting, organizing, and analyzing the data based on analyzing a process (Patton, 2002, p.447). This method allowed for a thematic analysis that allowed for pattern recognition (Patton, 2002, p.452)

Research Question 2: Do ease of use, usefulness, awareness of the technology, and security affect the adoption of biometric technology into the expedited screening procedures at commercial airports?

This question was answered through a deductive analysis based on TAM. Data triangulation was used to conduct a content analysis from previous document reviews. Data collected from social media sites was based on analytic induction to verify that the analysis was similar to those of the TAM. Lastly, the quantitative data collected from the

GAO reports illustrated the airport capabilities and the number of passengers receiving expedited screening at commercial airports. Afterwards, through the purpose of descriptive statistics, I illustrated through pie charts the perceptions of Trusted Travelers experiences using biometric technologies, and receiving expedited screening at commercial airports (Trochim, 2008).

Data Analysis

The data analysis for this research is based on a content analysis. Content analysis refers to the researching of recurring words and themes (Patton, 2002, p.452). In this study, I analyzed documents from the GAO, privacy complaints, social media postings, and studies for recurrent patterns. The first part of the study that pertain to privacy concerns was based on an inductive analysis as the process was to discover patterns, themes, and categories in the data.

The second part of the study that dealt with variables that could impact the acceptance of biometric technologies in the expedited screening procedures was based on a deductive analysis, as the data was analyzed to the existing theoretical framework of Morosan (2012) and Davis' (1989) TAM. A minimal sample of descriptive statistics was used for the data interpretation of the attitudes and behaviors of Trusted Travelers and commercial airports providing expedited screening and its capabilities.

Protection of Participant's Rights

There are no participants or subjects used in this study. I requested permission from the Committee on Ethical Standards in Research for the Institutional Review Board (IRB) at Walden University. The entire data was collected and used as secondary data within this study. The information provided from the GAO, OIG, and DHS Privacy Office is publicly available online at each agency's official websites. The audits and surveys were vetted and redacted (reviewed and cleared) are considered public information and did not require permission from the DHS and TSA Office of Public Affairs for use. The use of public information reduces the possibility of disclosing SSI and protects the security assessments of both DHS agencies.

I could not collect or use the data from the databases based on SSI procedures. I only used the databases to confirm previously released information made to the public through the GAO. As a covered employee under the TSA SSI Policies and Procedures Handbook (SSI Program, 2012) guidance on usage, I could reviewed the data to support the research based on the assessments conducted by the GAO (2014) regarding the usage of biometrics into the expedited screening process in commercial airports.

According to the TSA SSI Handbook Section 6.0 (2012) records containing SSI are not available for public inspection or copying and the TSA does not release records containing SSI to covered or non-covered persons who do not have a need to know. As written in the TSA SSI Handbook Section 6.1 (2012), a covered person is an individual or entity that has transportation or transportation security-related responsibilities to include, but not limited to, (a) anyone who is permanently or temporarily assigned, detailed to, attached employed by, or under contract with DHS, (b) regulated parties such as federal, state, local, and tribal government employees, contractors and grantees, as well as TSA stakeholders and industry partners; (c) committees of Congress; (d) other persons with a need to know as defined in Title 49 code of federal regulations (2012) Section 1520.11; and (e) persons receiving SSI pursuant to other conditional disclosures.

Moreover, the specific data could not be approved for public disclosure as it contains information that if released publicly would be detrimental to transportation security. Furthermore, the use of PMIS and PIMS was solely used to support specific assessments conducted by the GAO (2014) and OIG (2012) regarding the number of Trusted Travelers receiving expedited screening at commercial airports.

Summary

The primary focus of the research method in this study was to provide an extensive explanation of the process used to describe the research design and approach. The research method described the purposive sample and setting which consisted of current U.S. commercial airports providing expedited screening. The instruments and materials within this research study were collected from past OIG, GAO, and DHS Privacy Office Annual Reports to provide an overview of privacy concerns reported by travelers, biometric technologies used and tested, DHS agencies process of expedited screening at commercial airports, and its enrollment rates since the implementation of Trusted Traveler programs. The data collection provided the methods on how the data was collected. The research questions described how what methods were used to have them answered.

The databases identify the system used for tracking Trusted Traveler expedited screening at commercial airports administered by the TSA. The data analysis explained the reason for the selection of specific methods of analysis to explore an in-depth explanation of the two research questions. The protection of participants' rights is addressed within the study to safeguard that any information gathered from a group or individual had been provided in advance and that full consent to use the information in this study was granted. Ethical issues within this study were presented to receive approval from the Committee on Ethical Standards in Research for the Institutional Review Board (IRB) at Walden University prior to conducting research.

Chapter 4: Results

Introduction

In order for biometric technologies to be adopted into the expedited screening procedures for the TSA Pre-Check Trusted Traveler program in commercial airports, DHS must address privacy requirements based on the Privacy Act of 1974. DHS has to consider the differences in individuals' perspectives, attitudes, and acceptance of the technology; as the "user" would be affected by the collection and use of the technology if adopted into the expedited security procedures.

The results of this study would help the DHS and TSA understand the position of multiple entities that have an interest in the incorporation of such technology for stronger security measures. Entities include national governments, airport managers, airlines, industry experts, and the traveling public. Chapter 4 describes the process used to answer the two research questions that dominated the study.

The first question framing the research addressed what the United States federal government classification of a formal privacy complaint under the Privacy Act of 1974. The complaints filed with the DHS Privacy Office have to be addressed and reported to Congress on a semi-annual basis.

The research questions were: 1) Do privacy concerns of travelers affect the adoption of biometric technology into the expedited screening procedures at commercial airports? And 2) Do ease of use, usefulness, awareness of the technology, and security affect the adoption of biometric technology into the expedited screening procedures at commercial airports?

The document review of the privacy complaints of travelers was analyzed for content to determine what privacy concerns were reported as it related to the use of biometric technologies. The reports reviewed were from 2009-2014. Although, Trusted Traveler programs began in 2009 through Global Entry by CBP, DHS had used biometric technologies under its program US-VISIT (United States Visitor and Immigration Status Indicator Technology) to control foreign travelers entering the United States. Under the US-VISIT program, DHS collects the ten fingerprints and digital photographs of most non-U.S. citizens while obtaining the US Visa and entering the United States (OBIM, 2015).

This process provides biometric identification services to state, local, and federal government officials helping immigration officers to determine if a particular person is eligible to receive a visa to enter the U.S (OBIM, 2015). The collection of biometrics is used to prevent identity fraud that can occur with documents used for identification and verification, unlike with biometrics as each is unique and impossible to forge (OBIM, 2015). The program helps the U.S. government prevent people from using fraudulent documents to enter the country or have stayed after visa expiration (OBIM, 2015). In March 2013, the name of the program was changed to the Office of Biometric Identity Management (OBIM).

DHS did not have information regarding formal complaints regarding Trusted Traveler Programs until 2013 with the official implementation of TSA Pre-Check in 121 airports, so I had to review and collect data from formal complaints under the program of US-VISIT to determine the privacy concerns in regards to the use of biometric technologies. Using a categorical strategy by breaking down the narrative of the data after reviewing 20 pages of privacy complaints, I did a context analysis and used the software of QSR International Nvivo 11 to code based on the three surrounding themes:

1. Privacy concerns based on biometric technology experience through port of entries.
2. Privacy concerns based on personal information inputted into databases.
3. Privacy concerns based on interactions with government officials.

The categorization into the three areas was done to show the accurate position of the federal government to accept these complaints as valid based on the requirements of the Privacy Act of 1974. Therefore, when someone from the traveling public would file a formal complaint it had to belong to the following categories to have a resolution from a government official from the DHS Privacy Office. This Chapter further includes descriptive statistics to reflect the various factors to include the expansion of expedited screening in airports based on Pre-Check enrollment, participating airlines, third party vendors, and increase participation into other Trusted Traveler Programs run by CBP.

Data Collection

This mixed method design with an overall case study approach was based on the quantitative data that was released by the GAO in regards to the number of travelers receiving expedited screening from 2011 to 2014. This information was made public and was reviewed during the literature review to show stakeholders' role of participation in Trusted Traveler Programs. Upon approval of the Institutional Review Board (IRB) with number 06-17-0269550, the study met ethical considerations, as no participants were used.

I received consent from the agency to be able to verify the accuracy of the numbers released to the GAO regarding the number of travelers receiving expedited screening in airports nationwide. I did not disclose SSI as the information did not mentioned a location, time, and technologies that would create a security risk. Once the numbers for expedited screening compared to the Trusted Traveler status eligible passengers was confirmed through the databases was correct. The public information of the quantitative data was placed into a Microsoft Excel Spreadsheet categorized by year and compared to the Trusted Traveler's enrollment compared to passengers receiving expedited screening at commercial airports.

The purpose was to understand if privacy concerns were a factor in the adoption of biometric technologies if it would be used for expedited screening in commercial airports. The concept of privacy on a personal level was subjective and does not fit into the criteria of those underlined by the Privacy Act of 1974. Therefore, interviewing members of the traveling public would not have been a reliable source of data, as it would produce inconsistencies and not subject to government review. I went to the DHS Privacy Office and collected the reports that were presented to Congress regarding privacy complaints from 2009 - 2014.

The reports provided the qualitative data that was used to analyze what exactly were the privacy complaints that the government took into consideration in regards to biometrics and Trusted Traveler Programs. Afterwards, the data was imported into Nivo 11 and through a content analysis was categorized into the three most important categories previously stated to understand how the federal government determined privacy violations. In addition, social media posts from Facebook between the years of 2011-2014 of a sample size of 325 with the #TSAprecheck and #globalentry were gathered to determine the traveling public reactions regarding experiences using Trusted Traveler Programs. The information obtained from social media sites was collected to enhance and answer the second research question, as the information is considered public and accessible to anyone.

Data Analysis

Research Question 1: Do privacy concerns of travelers affect the adoption of biometric technology into the expedited screening procedures at commercial airports?

The qualitative data from the 50 privacy complaints from the annual reports was reviewed through a content analysis. I reviewed all 50 complaints for themes, patterns, and words. Through inductive analysis, I discovered that privacy concerns were reported based on the overall experience of the use of biometric technologies, errors inputted into databases, and interactions with government officials. I used Nvivo 11 to code the recurrent themes and was categorized into three categories:

1. Privacy concerns based on biometric technology experience through port of entries,

2. Privacy concerns based on personal information inputted into databases, and

3. Privacy concerns based on interactions with government officials.

The coding of the data was done through a content analysis of the privacy complaint. A sample of a privacy complaint and the agency's disposition is in Appendix G. The privacy data was analyzed under these categories as it was the best form to answer the first research question. Under the complaints received by the DHS Privacy Office, I wanted to know the submissions based on the type of privacy violations that occurred and how it would impact the study.

The themes were based on reactions towards the use of biometric technologies at ports of entry, these includes ports, airports, and border crossings. I also was interested into the various complaints that the traveler would experience after submitting themselves to the biometric technology process and errors were done at no fault of the passenger, but of personal information captured incorrectly. The last category was created as various complaints were having a repetitive theme that government officials were the cause of the traveler's dissatisfaction while undergoing security screening.

Using Nivo 11, I reviewed the privacy complaints and highlighted the complaint into one of the three categories placing references through pattern recognition and thematic analysis. From the 50 formal complaints received from the DHS Privacy Office regarding to Trusted Traveler programs or individual's having interactions with biometric technologies the results are as follows:

The 5 (10%) complaints in the area of experience with biometric technologies through ports of entry had nothing to do with biometric technology. The complaints were done because the traveler did not understand why he or she was referred to secondary screening as they had registered for a Trusted Traveler Program and had willing paid the fee of $100 dollars. Therefore, the complaints were filed to receive clarification and vent about the experience during secondary screening selection. In the area of privacy concerns based on personal information inputted into databases 20 (40%) complaints were regarding the errors during enrollment/or processing. Errors included placing fingerprints with incorrect names, dates of births, fingerprint captures, and poor quality of fingerprints taken.

The last area of privacy concerns was based on interactions with public officials as the highest with 25 (50%) complaints. In this area, the common themes were mistreatment of government officials based on tone of voice, comments, and procedures not understood by the traveler. The passenger's use of the term "violation of privacy" was based on searches conducted during secondary screening when during primary screening an alarmed had occurred that enabled government officials to conduct a more thorough investigation. Additionally, these complaints expressed many sentiments of the traveler while experiencing secondary screening such as "Feeling like a Criminal" "Feeling Uncomfortable", "Feeling Violated", "Questions Were Personal and Intrusive", "Feeling Angry", and "Treated Unprofessionally."

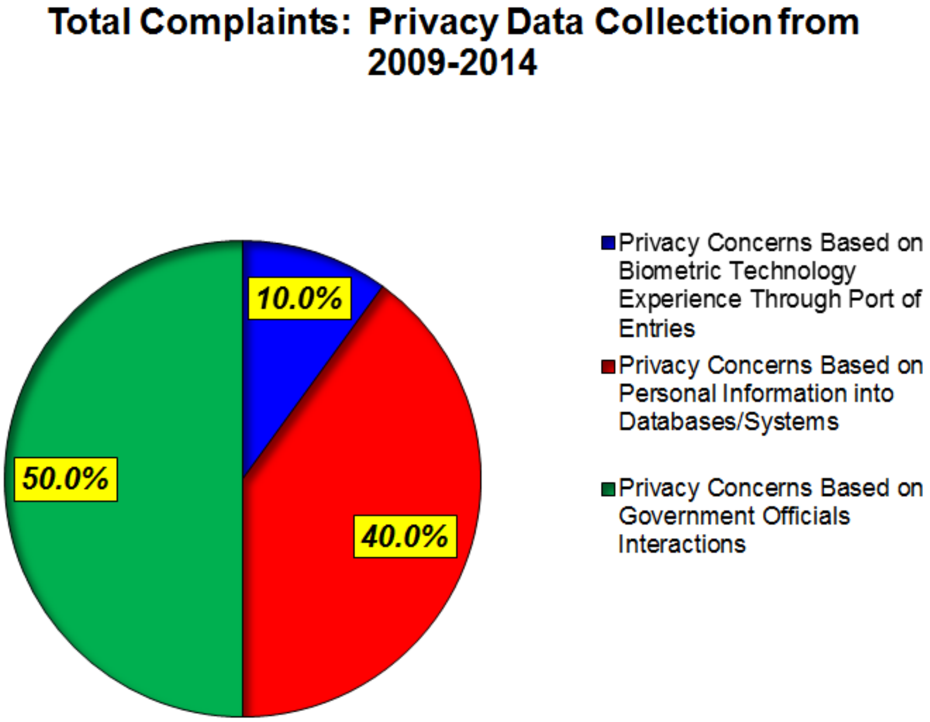


Figure 12: Total percentage of privacy complaints from 2009- 2014

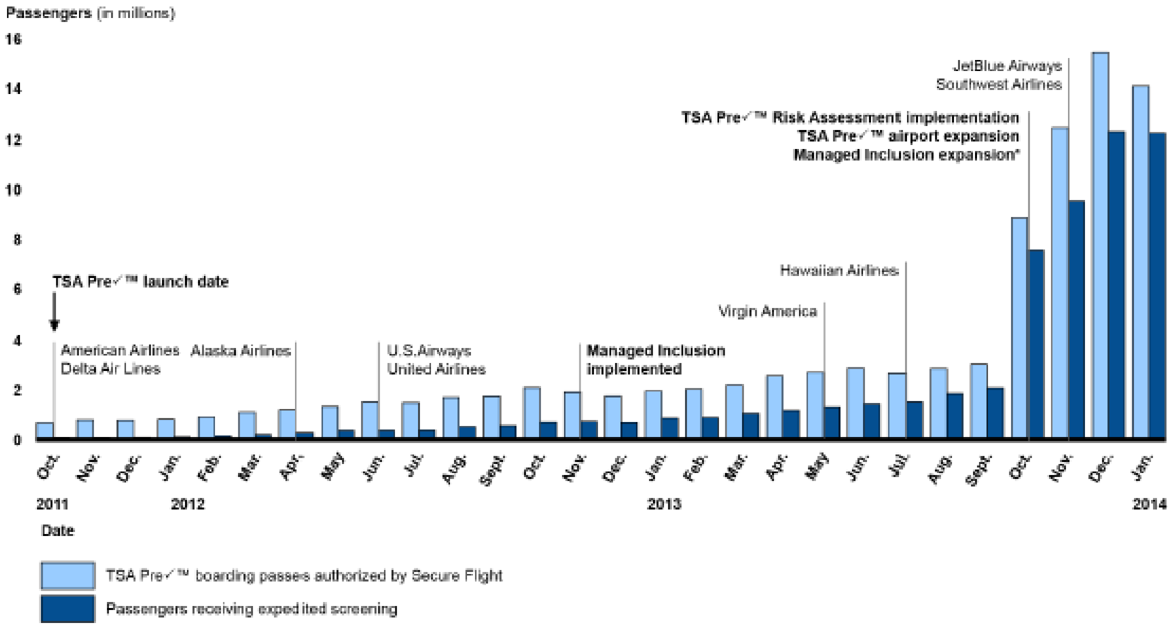
After the data was analyzed and coded under the numerical form, each number was divided by 50 and then multiplied by 100 to obtain a percentage; afterwards, it was placed into Microsoft Excel to create the detailed graph showed above illustrating the results of the analysis.

The results of the analysis for the first research question demonstrated that privacy concerns do not have an impact on the adoption of biometric technologies into the expedited screening process. Based on the analysis, the traveler would not object to submitting to biometric technologies as long as they are treated with respect and the process of biometric capture is not intrusive and done correctly during the enrollment and security screening process.

Research Question 2: Do ease of use, usefulness, awareness of the technology, and security affect the adoption of biometric technology into the expedited screening procedures at commercial airports?

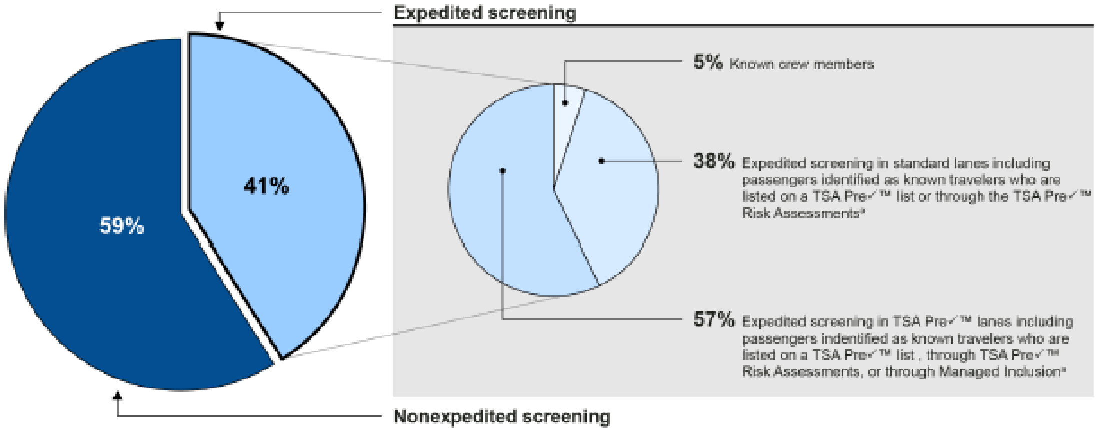
This part of the research was based on a deductive analysis as the data was analyzed based on the theoretical framework of the TAM and Morosan (2012) research. The numerical data of expedited screening was collected by the TSA from October 2011 through January 2014 and was released to the GAO in 2015. The content analysis shows in millions, the differences in the Secure Flight system producing TSA Pre-Check designated boarding passes compared to the actual number of passengers receiving expedited screening. The numbers beginning from October 2011 showing by each month are small for Pre-Check designation as only four airports were piloting the program. Delta Airlines was the first airline to provide the service to its frequent flyers, but expedited screening at the airports was not implemented until January 2012.

Multiple airlines such as Alaska Airlines, U.S. Airways, American and United Airlines joined TSA Pre-Check to have passengers eligible for expedited screening. TSA began processing passengers through expedited screening in only 30 airports. In November 2012, to increase expedited screening into Pre-Check designated lanes, the TSA incorporated the Managed Inclusion program to allow passengers without Pre-Check designation and with the use of a randomizer, experience the benefits of expedited screening without registration into the Pre-Check program. By October 2013, the TSA expanded the Pre-Check program designated lanes in 121 airports nationwide and Virgin America, Hawaiian Airlines, JetBlue Airways and Southwest Airlines were added to the expedited screening numbers. The addition of those airlines expanded the generation of Trusted Traveler designation into the Secure Flight program giving the boarding pass of passengers the Pre-Check status.



Source: GAO analysis of TSA data. | GAO-15-150

Figure 13. Expansion of TSA expedited screening from October 2011- January 2014



Source: GAO analysis of Transportation Security Administration (TSA) data. | GAO-15-150

Figure 14. Percentage of passengers screening by type from May 11, 2014 – May 18, 2014

The content analysis underlines the comparison of when Secure Flight designates the boarding passes with the Pre-Check designation and when the TSA began implementing expedited screening at commercial airports. The data shows that the system would over-designate boarding passes with the Trusted Traveler status, but commercial airports did not have the expedited screening capabilities to sustain the large volume of Pre-Check designation the Secure Flight system was producing.

During the period of May 11, 2014, through May 18, 2014, the TSA implemented the programs of Managed Inclusion, Known Crew Traveler, and its risk assessment algorithms. 41% of the traveling public received expedited screening at the 121 participating commercial airports compared to the 59% received standard screening. The long-term objective of the agency is to provide 100% expedited screening and a wait time of fewer than 5 minutes for Pre-Check participants and to increase voluntary enrollment (TSA, 2016).

However, the agency does not understand that the program may not be suitable for all members of the traveling public because some may travel once a year. Hence, for passengers traveling once a year would not a benefit in enrolling into a Trusted Traveler program. Therefore, the data will always be evolving as the relationship between expedited screening, and the airport resources and capabilities are changing based on the agency's senior leadership objectives, additional airline participation, and financial budget.

Additionally, private companies such as CLEAR and IDENTOGO are providing the service of enrollment with a fee for identity verification bypassing the travel document checker personnel at selected airports. Customers can skip the line but Trusted Traveler program enrollment is required to receive expedited screening at commercial airports or sporting events. These third-party vendors have conducted the research and dedicated resources in understanding that individual members of the traveling public would pay any fee, and have their biometric information collected and verified to reap the benefits of shorter and faster lines while traveling (INDENTOGO, 2016).

An analytic induction was conducted based on a content analysis with documents from the literature review and previous studies. A sample of 325 social media posts were analyzed to capture the attitudes, perceptions, and concerns of the traveling public regarding their experiences with Trusted Traveler Programs, biometric technologies, and expedited screening. The data obtained from the DHS Privacy Office was not sufficient to make a generalization regarding the TAM and attitudes of Trusted Traveler participants.

The TAM could not be applied in this study based that I did not have access to the actual design of the biometric technologies being used by CBP at ports of entry. In addition, I did not conduct actual interviews of those that did have experience with those technologies as it would null the data of the privacy reports. However, the 325 social media postings provided an indication of how ease of use and usefulness are influential in the attitudes and behaviors towards biometric technologies (Shen et al., 2006).

Based on the content analysis, the traveler feels ease to use the biometric technologies as it would provide an extended benefit, if it is non-intrusive and enhances security (Josha & Koshy, 2009). In the area of usefulness, passengers would accept submitting to biometric technologies as long as they are aware of its purpose. Individuals who choose to enroll in a Trusted Traveler program are made aware of the technologies being used and its purpose in the terms and conditions policies during the enrollment process.

During the data analysis with the use of Nvivo 11, I created three categories and coded the social media posts based on the recurrent themes of (a) Shorter/faster lines; (b) Experience was enjoyable, easy, and pleasant, and (c) Frustration with the process during airport screening. I read all of the 325 posts and coded them based on the frequency of the themes experienced by travelers. The data was analyzed and coded under a numerical form; each number was divided by 325 and then multiplied by 100 to obtain a percentage. Then, it was placed in Microsoft Excel creating the detailed graph illustrating the results.

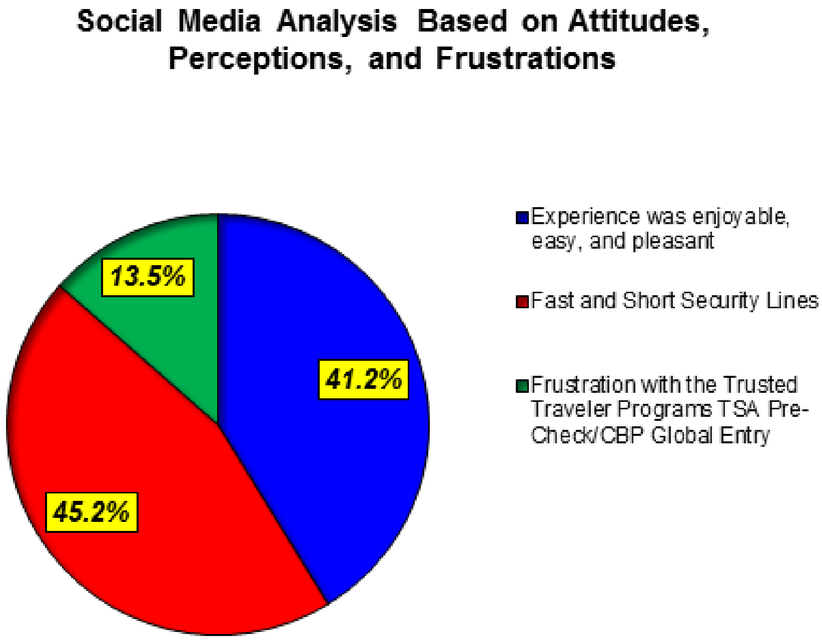


Figure 15: Social media analysis based on attitudes, perceptions, and frustrations.

The analysis revealed the majority 147 (45.2%) of those experiencing Trusted Traveler status favored the shorter and faster lines. Third-Party vendors have explored the concept of shorter lines with the use of biometric technologies during screening for identity verification with positive results. 134 (41.2%) enjoyed the experience of the expedited screening process due to not removing shoes, electronics, liquids from carry-on bags, and belts. 44 (13.5%) experience frustration with the Trusted Traveler Program.

Furthermore, I explored in-depth the themes causing frustration among travelers experiencing expedited screening at airports and ports of entry. Using the same process as previously with the 325 media posts, the number used to determine the frustrations of travelers experiences with expedited screening at airports is 44. The data was analyzed and coded under a numerical form; each number was divided by 44 and then multiplied by 100 to obtain a percentage. Then, it was placed in Microsoft Excel creating the detailed graph illustrating the results.

Out of the 44, 22 (50.0%) felt cheated about paying for the program because their boarding pass was not designated the Trusted Traveler status, non-enrollees were being placed into Trusted Traveler designated lines that did not know the divestiture process for expedited screening. 13 (29.5%) stated that Trusted Traveler designated lanes are longer than standard lanes. 9 (20.5%) were selected for additional or secondary screening while having Trusted Traveler status.

Out of the 44, 22 (50.0%) felt cheated about paying for the program because their boarding pass was not designated the Trusted Traveler status, non-enrollees were being placed into Trusted Traveler designated lines that did not know the divestiture process towards expedited screening, 13 (29.5%) stated that Trusted Traveler designated lanes are longer than those at the standard lanes, and 9 (20.5%) were selected for additional or secondary screening while having Trusted Traveler status.

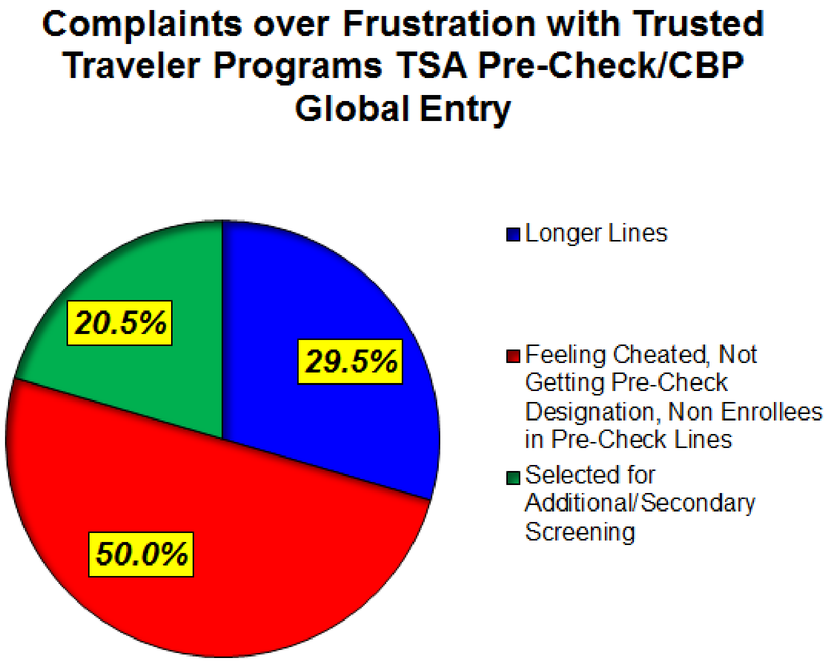


Figure 16: Social media analysis based on frustration with Trusted Traveler Programs.

Therefore, the adoption of biometric technologies into the expedited screening process at commercial airports would be affected based on the common theme of wait time during the security screening process and not the technology. The analysis concluded that the traveling public would prefer to have security be efficient and fast without the process being intrusive to their person.

Summary

In Chapter 4, I presented the results of the data analysis from the document review of the formal complaints obtained from the DHS Privacy Office from 2009-2014. I explained by the TAM could not be tested based on the lack of accessibility to the system design. The social media analysis provided additional content into the behaviors and attitudes of travelers experiencing expedited screening in commercial airports. The analysis was conducted based on the data released by the TSA to the GAO and confirmed through its databases of PMIS and PIMS. The GAO and OIG provided the information of Secure Flight and the amount of passengers that received expedited screening at commercial airports. The data demonstrated that commercial airports do not have the full capabilities to increase the volume of expedited screening based on resources.

Therefore, consideration must be made that the amount of passengers receiving expedited screening would constantly change as more commercial airports would add Pre-Check lanes and resources to support program participants. However, Secure Flight is over producing the Trusted Traveler designation on boarding passes, but commercial airports do not have the capabilities to process the high amount through expedited screening.

During the time frame of this research, only 121 airports out of the 450 offer expedited screening for Trusted Traveler status designation. It does not account for additional airports that have implemented expedited screening, additional airline participation, and the removal of the Managed Inclusion program as it was used as a wait-time management tool. Therefore, the amount of passengers receiving expedited screening is related to the airport having lanes designated for Pre-Check processing or standard lanes being converted into expedited screening and the resources to maintain them.

The analysis and interpretation of the data in this mixed-method case study expressed that privacy was based on the definition provided by the Privacy Act of 1974 and would not influence the adoption and usability of biometric technology in regards to expedited screening procedures in commercial airports. The attitudes and behaviors of the traveler are towards wait times and shorter/faster security lines, and not the use of biometric technologies for the identification and verification process as a security measure for expedited screening. A discussion of the results is presented in Chapter 5 with its conclusions and recommendations for further study.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

This chapter begins with a summary of the study and discusses the findings based on the theoretical frameworks by Morosan (2012) and Davis' (1989) TAM. The focus was whether did privacy concerns would affect the adoption of biometric technologies in the expedited screening process at commercial airports. In addition, I explored other variables such as those of ease to use, usefulness, security, and awareness of the technology to understand their effects on the adoption of biometric technologies into the expedited screening procedures as a security measure at commercial airports.

Furthermore, this chapter discusses the limitations of this study and provides recommendations for future research and actions. The conclusion of this chapter finalizes with the implications for positive social change and what methods were implemented to date in regards to enhancing expedited screening in commercial airports.

Summary

The study focused on privacy as a variable into the adoption of biometric technologies into the expedited screening process at commercial airports. Furthermore, the study explored the attitudes, perceptions, and concerns regarding the ease of use, usefulness, and awareness of the biometric technology, and how its adoption would be affected as an enhancement of the expedited screening procedures at commercial airports.

The research questions all surrounded on the theoretical concept of the TAM and provided new information to technology manufacturers of biometrics devices, government agencies, businesses, scholars, and public policy decision makers to decide on the adoption of biometric technology as a security measure for the identity and verification process of those going through expedited screening at commercial airports. Such data would help the government agencies with the mission of national security to be able to reach a balance between the individual's right to privacy and safeguarding the country.

In this study, I applied a mixed methodology approach with a focus of case study that involved a small about descriptive statistics (graphs) and a content analysis of secondary data from both quantitative and qualitative sources. During the numerical data sets, the data revealed that the internal system of Secure Flight was over producing the Trusted Traveler status designation more than the airport's capabilities and resources allowed.

As a result, there are increased wait-times or enrollees not screened through expedited screening procedures as required. The qualitative data through privacy complaints and social media posts were used as secondary data to enhanced and provided and in-depth view of the traveler's experience with Trusted Traveler Programs at commercial airports and ports of entry.

Interpretation of the Findings

The use of biometric technologies has increased as a tool for identification, authentication, authorization, and accountability purposes. The literature review provided the information and the reasoning for the use of the technology as a security measure for identity identification and verification. For government agencies, biometric technology implementation in its programs is for national security interests and record management into national databases. In the use of aviation security, many variables must be taken into account before the adoption of biometric technology can be implemented, such as airport size, personnel executing the program, databases maintenance, airline participation, technology manufacturers, and airport managers. In this mixed methodology study, I investigated the variables that would influence the adoption of biometric technology for use as a security measure for the expedited screening procedures at commercial airports in the United States.

Findings for Research Question 1

The data analysis demonstrated that privacy concerns do not have an impact on the adoption of biometric technologies into the expedited screening procedures. The traveler would consent to their right to privacy to receive a benefit, or for the convenience of having a faster security line. Additionally, the biometric device capture has to be quick and non-invasive. The travelers referred the majority of the privacy concerns (50%) were based on the treatment of government officials during secondary security screening rather than concerns regarding the collection of their personal information through biometric technologies.

Findings for Research Question 2

The TAM could not be applied as I did not have access to the actual design of the biometric technologies used by CBP at ports of entry. However, a 325 purpose sample of posts on social media sites provided an indication of how ease of use and usefulness influences the attitudes and behaviors towards biometric technologies. The analysis revealed that the data provided by the TSA showed that the internal system of Secure

Flight had over produced the Trusted Traveler status designation, but not all 450 commercial airports were offering expedited screening procedures or had Pre-Check designated lanes.

Therefore, the commercial airports do not have the capabilities to provide expedited screening to the large volume of travelers having the Trusted Traveler status produced by Secure Flight. In addition, to capture the attitudes, perceptions, and behaviors of the traveling public, a purposeful sample of 325 was analyzed to determine that 45.2% of the traveling public preferred Trusted Traveler designated status because of the shorter and/or faster lanes.

41.2% enjoyed the experience of the expedited process as being easy and pleasant, and 13.5% were frustrated with the Trusted Traveler Program experience. I wanted to explore further the frustration of travelers regarding Trusted Traveler programs as it related to biometric technology. The results illustrated that 50.0% of Trusted Travelers felt cheated, as the status was not reflected on the boarding pass, or non-enrollees were being placed in Trusted Traveler lanes without knowing the divesture procedures. 29.5% of travelers stated that longer lines were in Trusted Traveler designated lanes, and 20.5% were because of additional and/or secondary screening.

Limitations of the Study

This study had no limitations. The investigation was based on how privacy concerns would affect the adoption of biometric technology into the expedited screening process at commercial airports. Additionally, I also explored if awareness, ease of use, security, and usefulness of the technology would affect the adoption of biometric technology into the expedited screening procedures. If the study had included actual interviews of participants regarding their sentiments about privacy, the answers to the research questions would have been different and results would not be those reflected in the study.

The results based on the content analysis from the information obtained from the DHS Privacy Office illustrated that not many people filed privacy complaints or that the government discard them as it did not met the federal government's definition of privacy. Therefore, government agencies are required to abide by the law, and are not subjective as individuals and corporations could. The Privacy Act of 1974 only applies to government programs and private companies are regulated through their own terms of service.

The small sample size of 50 privacy complaints obtained by the DHS Privacy Office (2009-2014) demonstrated that the agency had not collected enough data or it collected enough to meet the required minimum reporting requirements. The small sample size collected over the years was used to make general assumptions of privacy complaints in all of the United States and its territories, and not a specific region, state, or city.

Additionally, the information obtained from the privacy complaints that was analyzed was not enough and other secondary sources were needed. I was able to get a wider perspective of the feelings of travelers through social media sites as they shared their experiences with Trusted Traveler Programs and expedited screening at commercial airports.

Additionally, I was not allowed to disclose information that was not made public by the TSA previously. Under its SSI program, I was only allowed to verify information, but could not disclose other information that would have had major contributions to this study, if accessible. Therefore, the initial plan to compare and categorize commercial airports based on their enplanements, personnel resources, technology, and wait-times based on expedited screening was not possible. The non-disclosure of information created a limitation because the research questions had to be answered through the limited data that the agency had already released two years prior.

Discussion

According to TSA records, biometric security measures are being piloted to include retinal scans that enable identification of passengers based on a unique set of identifiers such as iris scans and fingerprints (TSA, 2012). Aviation security experts suggested that security should be categorized into three parts: Items (Threats), Identity (Passengers/Travelers), and Intent (Purpose). The TSA has made improvements in the area of implementing the IATA version of the checkpoint of the future, but has concentrated in the area of fraudulent boarding passes, instead of identifying and verifying the traveler's true identity (TSA, 2012).

Jackson, Chan, & Latourette (2011) argued about the consequences a Trusted Traveler Program presents to the advantages of terrorists wanting to evade security measures. First, a terrorist could apply for and be granted Trusted Traveler status, providing them "authorized access" to that particular line (Jackson et al., 2011, p.3). Second, terrorist could identify members of the public who are Trusted Travelers and force them into carrying weapons through the Trusted Traveler line (Jackson et al., 2011, p.3). Lastly, members of the public that are Trusted Travelers could become terrorists (either by recruitment or by self-radicalization) and stage an attack before their changed risk level was discovered and their Trusted Traveler status was revoked (Jackson et al. 2011, p.3).

Furthermore, Jackson et al. (2011) stated that the reasoning for the limited expansion of Trusted Traveler Programs in the United States is because if terrorists can gain access based on the three forms stated previously, it would reduce the benefits of such programs. They suggested that some fraction of the terrorists will apply, and some may be accepted as Trusted Travelers depending on the nature of their background check and the rates of false positives (incorrectly flagging an innocent person as a threat) or a false negative (misidentifying a terrorist as a nonthreat) (Jackson et al. 2011, p.5). However, the baseline probability of detection is the most important factor in aviation security standards as all passengers, regardless of status would be receiving x-ray screening of their property and a walk through metal detector of their person (Jackson et al. 2011, p.5).

The quality of the background checks also plays a significant role in the acceptance and implementation into the Trusted Traveler Program by reducing the rates of false positives and false negatives, allowing for security to be more efficient and using its resources for travelers where information is limited or unknown (Jackson et al. 2011, p.15). However, terrorists could already use population that receives expedited screening as a condition of their employment to gain access through security checkpoints, such as pilots, airline crew, airport employees, and bribing security officials under existing security models (Jackson et al. 2011, p.15).

Jackson et al. (2011) made the correlation between the baseline of security performance and a terrorist ability to be able to gain Trusted Traveler status based on the quality of the background checks; making the programs a tool for terrorist to circumvent security screening. However, the RAND Corporation report (2011) stated that the TSA when it was created in 2001, provided the head of the agency the ability to establish a registered traveler program with the requirements that fliers must provide personal information, including biometrics, and submit to a background to verify, whether they present a threat to commercial aviation or not (RAND, 2011). Trusted Travelers would receive expedited security screening and a more convenient and comfortable travel experience, but security screeners would still reserve the right to increase the intensity of the screening, if the Trusted Traveler were suspicious or chosen randomly for secondary screening (RAND, 2011).

Airports managers and stakeholders argued that technology must be efficient, precise, and time-saving as too much time being spent in the security process could become a deterrent for those wanting to travel for either business or pleasure. However, since Trusted Traveler Programs are voluntary those choosing to enroll received the benefits of being pre-screened by the integration of biometrics; and can received a faster security experience as they are granted low-risk status allowing for more time to be spent on other things in the airport such a shopping and dining; while waiting for their flight increasing commerce and revenue for all stakeholders involved.

The introduction of biometric technology into the expedited security screening in commercial airports would create the balance in its desire to deter terrorist from applying into the program, while at the same time delivering clear benefits to innocent travelers who take the time to apply and pay the registration fee (RAND, 2011). Furthermore, the primary variable based on the report is how effective the background check would be. The reasoning behind it is what makes the program desirable to the flying public also makes it attractive to a terrorist (RAND, 2011).

In regards to matters of privacy, privacy advocates have identified privacy concerns with the use of facial recognition technology for its ability to recognize individuals in public environments without their consent, and collect their information, and then share their personal data (Facial, 2015, p. 13). One of the concerns is the reduction of anonymity that affects the privacy of a person when in a public environment, if choosing to be in public (Facial, 2015, p.13). However, the Center for Democracy & Technology stated: when most individuals are in public, there is an expectation that some business and people would recognize their faces, but only a few would make the connection between the name of the face especially in matters of internet behaviors and travel patterns (Facial, 2015, p.13).

Furthermore, privacy advocates stated: since being recognized in public settings becomes more common, some individual may not be comfortable shopping in specific establishments, gathering in public for a supporting cause, or visiting certain places (Facial, 2015, p.14). The Electronic Privacy Information Center (EPIC) stated that individuals lose control over their identity, if they do not have the option to want to remain anonymous in public settings. Facial technology adds additional privacy concerns as its use is not only to identify the individual, but also those they are with (Facial, 2015, p.14).

The World Privacy Forum stated that the majority of individuals may find it invasive to their privacy, if security cameras were used in the tracking of their movements for marketing strategies (Facial, 2015, p.14). An additional privacy concern is the identification or verification of the individual without its consent or knowledge. Unlike those of other biometric technologies, facial recognition can be utilized to capture the face at a distance with the individual knowing, and as the technology grows the option of opting out may be less feasible for the utilization of the technology (Facial, 2015, p.15).

The biggest privacy issues with the use of facial recognition are:

- Individual control over personal information: The matter that personal data is associated and collected with facial recognition could be shared, used, and sold without the person's consent (Facial, 2015, p.16).
- Data security: The data collected by the facial recognition technology can be subject to data breaches that could be exposed to unauthorized entities (Facial, 2015, p.16). The risk of theft of data could increase the possibilities of stalking, identity theft, and harassment (Facial, 2015, p.17). Industry experts believe that security concerns are mitigated, as present facial print algorithms are tailored to the vendor and, there is little use, if received through a breach (Facial, 2015, p.17).

- Misidentification: The matching of someone's image is captured and misidentified with the incorrect identification of an individual leading to long-term consequences without the knowledge of the individual (Facial, 2015, p.17).
- Disparate treatment: Individuals who may not have consented to facial recognition could be denied access to particular services and products. Therefore, the use of patterns of behavior and personal characteristics could be used to make generalization leading a person be discriminated based on certain groups (Facial, 2015, P.17).

Stakeholders have expressed that the technology does not present unusual privacy risks that already exist and could be reduced as the benefits would be weighed towards what the technology offers (Facial, 2015, p.17). They argued that:

- Individuals should not expect complete anonymity in public: It is contended that privacy and anonymity are not the same and that losing complete anonymity is not a surrender of privacy. The capturing of a facial image of a face print in public is not the same as removing a person's anonymity, as it does not reveal any personal information (Facial, 2015, p.18).
- Surveillance is already part of our daily life: Public places already have security cameras and facial recognition does not increase their use (Facial, 2015, p.18).
- Individuals have demonstrated a willingness to give up privacy for the benefits technology: Individuals have demonstrated their willingness to share personal information in public, by posting on social networking sites. Therefore, the trade-

offs between losing some privacy and the benefits of new technologies offer businesses opportunities for economic development (Facial, 2015, p.18).

- The need for consent should be based on the context: The need for individual consent should rely on the framework under which facial recognition technology is utilized. In matters of security, there may not be a requirement to ask for permission when using the technology compared to social networking sites which have repositories of facial images to identify individual on a boarder scale (Facial, 2015, p.19).

Privacy advocates expressed that the technology should have "privacy by design" which are the building of privacy protections at every stage of development. For example, manufacturers of biometric technologies could design into their systems that the data collected, be used for specified purposes, and then, erasing the data after used ensuring that repurposing of the data is disabled (Facial, 2015, p.25).

Conclusions

The current research makes the suggestion that travelers are willing to waive their privacy concerns regarding the use of biometric technology, if the process is short on time and that the security process is fast. The biometric technology that is used to implement CBP Trusted Traveler programs utilizes a multi-model of fingerprint and facial recognition for incoming passengers in port of entries in the United States and its territories. Therefore, if the TSA would incorporate the same model, it could also address the issue of wait times as the traveler would have already verified their identity through dedicated kiosks minimizing the wait time in security lines. This concept has already been introduced in the private sector with the CLEAR Program.

The industry has added the product of Trust Traveler status to avoid the long security lines at commercial airports and sporting events. The CLEAR program has an annual enrollment cost of $179 and supports the argument that individuals are willing to pay such a fee for shorter lines (Crowley & Ross, 2009). However, CLEAR is not subject to the Privacy Act of 1974, but it is regulated by its own terms of service. CLEAR is available at 11 airports in the United States and works by passing through two steps: identity verification and security screening.

Travelers who enrolled in CLEAR have their separate lane for the first step, where they can utilize biometric authentication (Fingerprint or Iris Scan) at a kiosk rather than wait for a TSA agent to inspect their ID and scribble something on the boarding pass (Steele, 2015). After the identity has been verified, a CLEAR representative will escort the traveler to the actual security screening, bypassing everyone waiting in line (Steele, 2015).

CLEAR is utilized by passengers who have first enroll online, and then visit an airport location where their identity is verified, and biometrics are collected and recorded into the vendor’s system (Steele, 2015). The enrollment in CLEAR can be done at any CLEAR location with no appointment, and the card is shipped within 5 to 7 business days (Steele, 2015). However, enrolling in CLEAR does not mean that the traveler has Trusted Traveler status; it is just a program that allows individuals to skip the line and the identity verification of the TSA personnel (Steele, 2015).

Those who have enrolled in CLEAR must also enroll into a federal managed Trusted Traveler Program to receive its benefits for expedited screening as CLEAR only bypasses the identity verification portion of the screening as it is conducted by CLEAR Kiosks (Steele, 2015). Furthermore, the federal government must balance the individual's right to privacy under the Privacy Act of 1974 and those of national security.

The U.S Patriot Act of 2001 made it that the federal government does not have to follow restrictions of the Privacy Act of 1974 as issues of national security would take priority. In addition, national security interests are one of the twelve exceptions that the federal government has as a means to implement national security programs.

However, the Privacy Act of 1974 is the law that controls the federal government into having privacy impact assessments and offices at every department to safeguard itself from litigation. The U.S. Patriot Act of 2001 enables for multiple governmental agencies to share information and programs in the process to combat terrorism based on the attacks of September 11, 2001 (EPIC, 2016).

However, the balance between the interpretation of an individual's right to privacy and national security interests relies on the judicial system and which supreme justice would favor the federal government's position in fighting terrorism or the individual's right to privacy. The laws in the justice system have not been kept up with advances in technology in the digital age.

Implications for Social Change

The results of this study within the body of research on social and political change may be used to enhance the discussion for the U.S. Supreme Court to bring a clear interpretation of the fourth amendment and the U.S. Patriot Act of 2001. The study contributes to the deficiency in the literature as it addressed the privacy aspect of Trusted Traveler Programs and the purpose biometric technologies could serve in the enhancement of expedited screening procedures at commercial airports as a national security objective. This study could provide scholars, authorities, and industry experts' opportunities in deciding which actions should be implemented in their policies as it relates to Trusted Traveler Programs.

The study revealed that the traveling public is more concern with wait times and shorter or faster lines, and are willing to undergo any screening process that allows them to have a reduction in their time during security screening at commercial airports. The study illustrated that the traveling public is willing to consent to their right to privacy for the convenience of shorter and faster lines, as they can spend less time during security screening at commercial airports.

The objective of this research was to make a contribution to the existing body of knowledge to foster a continuation of a change-oriented debate in matters of public policy. The adoption of biometric technologies in Trusted Traveler Programs specifically for the TSA Pre-Check Program in the expedited screening process may interest other countries around the world with similar legal systems as those of the United States, into implementing biometric technologies in programs of the same nature (Neyland, 2009).

Recommendations

The DHS should combine all of its Trusted Traveler Programs into one database and in the same format for all of its components. The incorporation of having one database would reduce double efforts into creating different databases, maintenance, security patches, equipment, facilities, and training of personnel. The purpose of Trusted Traveler Programs is the same; regardless of the government agency that is overseeing its implementation. The overall focus is the continuation of a security model based on intelligence and risk assessments by allocating resources to individuals that are categorized at a higher risk.

As the TSA implements its Trusted Traveler Program through Secure Flight and its designation into the passenger's boarding pass, CBP employs radio frequency identification technology to allow pre-screened travelers expedited processing at designated port of entries (OIG, 2014, p.1). Radio frequency identification (RFID) is a form of automatic identification and data capture technology that uses radio frequencies to transmit information (OIG, 2014, p. 1). CBP attaches a RFID tag in each Trusted Traveler Program card and travelers who choose to participate in the program, voluntary submit PII through a web-based application system that CBP uses to handle the enrollment and vetting process (OIG, 2014, p.3).

Furthermore, CBP stores applicants' data (biographic data, facial photographs, and background investigation results) in a database. At ports of entry, RFID readers scan the Trusted Traveler cards and use the unique number embedded in each card to retrieve the passenger's data through an encrypted network (OIG, 2014, p. 3). The CBP Officer uses the passenger's information shown on the monitor to authenticate the traveler's identity (OIG, 2014, p.3).

The CBP uses the RFID technology for registered travelers for expedited border crossings and airports enrolled in their Trusted Traveler Programs. CBP maintains the integrity of these programs through a stringent screening process that includes automated searches against multiple law enforcement databases, 24-hour system checks to verify the status of enrolled travelers, and random selections of registered travelers for secondary inspection (OIG, 2014, p.4).

Additionally, CBP implemented a program to apply security patches to the servers and databases that support these programs and has created testing environments to see the effects of security patches before deploying its production systems (OIG, 2014, p.5). CBP does not store any PII on the Trusted Traveler Program cards, and only the unique identification number is present, this is done in the event that an attacker obtains the information to produce a duplicate card, CBP officers can mitigate the threat by verifying the travelers' PII and picture presented on their terminal (OIG, 2014, p.6).

The TSA should incorporate the same system of assigning cards and kiosks for those enrolled in Trusted Traveler Programs for the identity verification of the traveler using the same technologies and databases, instead of creating a different system as both agencies are under the DHS umbrella. The CLEAR program makes the concept workable and is deployed at 11 commercial airports and CBP has also deployed the technology for over two years and has had much success with the traveling public participating in Trusted Traveler Programs. Therefore, by combining resources and placing all Trusted Traveler Programs into one system, the concept would be easier to manage and would reduce operating expenses compared to having two agencies manage separate programs.

References

Abernathy, W., Lien, T., & Granger, S. (2006). Biometrics: Who's watching you? *Electronic Frontier Foundation*. Retrieved from http://www.eff.org/Privacy/Surveillance/biometrics/

Acharya, L. (2006). *Biometrics and government*. Parliamentary Information and Research Service. Retrieved from http://www.parl.gc.ca/information/library/PRBpubs/prb0630-e.pdf

AlBalawi, W. (2006). *Students' and instructors' attitudes toward using biometric technology as an identification method in online courses*. (Unpublished doctoral dissertation). West Virginia University, Morgantown.

Alrafi, A. (2005). *Technology acceptance model*. Retrieved from http://www.le edsmet.ac.uk/inn/RIP2005-4.pdf

Alonso-Fernandez, F, Bigun, J, Fierrez, J, & Ortega-Garcia, J. (2009). "Fingerprint Recognition." In *Guide to Biometric Reference Systems and Performance Evaluation*, edited by D. Petrovska- Delacrétaz, G. Chollet, and B. Dorizzi. London, England: Springer, pp. 51-88.

American National Standards Institute. (2007). *Cross-jurisdictional and societal aspects of implementation of biometric technologies, Part 1: Guide to the accessibility, privacy, and health and safety issues in the deployment of biometric systems for commercial applications*. New York, NY: International Standard Organization.

Baird, S. L. (2002). Biometrics "Security Technology": It is important for students to understand that technology can be used as part of a solution to a problem. *Technology Teacher, 61,* 1–6.

Barry, C. (2002). *Financial institutions give biometrics a thumbs up.* Retrieved from http://www.tmcnet.com/biomag/features/celnet.htm

Blackburn, D. M. (2004). *Biometrics 101*. Washington, DC: Federal Bureau of Investigation, Government Printing Office.

Blackburn, D., Coty, T., Cook, J., Dee, T., & Dunn, J. (2008). *Biometrics in government post-9/11: Advancing science, enhancing operations*. Washington, DC: Office of Science and Technology Policy.

Blackburn, D., Miles, C., & Wing, B. (2006). *The national biometrics challenge*. Washington, DC: National Science and Technology Council Subcommittee on Biometrics, Government Printing Office.

Bocozk, K, Buster, C. J., Fitzgerald III, S., Vacca, E. E., Welsh, J., & Wulf, T. (2005). *Biometrics: Networks and telecommunications in business*. Retrieved from http://www.kevingalls.com/biometrics/groupproject.doc

Boo, S. & Jones, D.L. (2009), Using a validation process to develop market segmentation based on travel motivation for major metropolitan areas, *Journal of Travel & Tourism Marketing,* Vol. 26 No. 1, pp. 60-79.

Brew, T. (2006). *European attitudes towards biometrics*. Hampstead, London: LogicaCMG.

Brydie, D. R. (2008). *Situational considerations in information security: Factors* *influencing perceived invasiveness toward biometrics*. (Unpublished doctoral dissertation). Capella University, Minneapolis.

Campbell, L. M. (2005). Rising government use of biometric technology: An analysis of the United States Visitor and Immigrant Status Indicator Technology Program. Retrieved from http://www.isrcl.org/Papers/2005/Campbell_L.pdf

Caslon Analytics Biometrics. (2006). *Biometrics, attitudes and responses*. Retrieved from http://www.caslon.com.au/biometricsnote12.html

Cavoukian, A. (1999). *Consumer biometric applications: A discussion paper*. Toronto, Ontario, Canada: Information and Privacy Commissioner.

Cavoukian, A., Chibba, M., & Stoianov, A. (2012). Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment. *Review of Policy Research*, *29*(1), 37-61. (2012, January 1).

Chan, S.L. (2002). Information Technology in Business Processes. Business Process Management Journal, vol.6 (3), pp. 224-237

Chirillo, J. & Blaul, S. (2003). *Implementing biometric security*. Indianapolis, IN: Wiley Publishing, Inc.

Clausen, S (2008) A Single-Line AC Capacitive Fingerprint Swipe Sensor. *In Advances in Biometrics Sensors*. London, England: Springer.

Coventry, L. (2005). *Usable biometrics offer a technological solution to the authentication of individuals*. Dundee, UK: Advanced Technology & Research, NCR Financial Solutions.

Cowen, J. B. (2009). The influence of perceived usefulness, perceived ease of use, and subjective norm on the use of computed radiography systems: A pilot study. Retrieved from https://kb.osu.edu/dspace/bitstream/1811/36983/1/FinalSubmitted.pdf.

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. Thousand Oaks, CA: Sage Publications.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Crowley P.J., & Ross, L. (2009) How to make the TSA (and airports) work better. http://www.americanprogress.org/ issues/2009/04/tsa_risk.html. Accessed July 7, 2016.

Customs and Border Protection. (2014). Trusted Traveler Programs, Global Entry, NEXUS, SENTRI

Retrieved from: http://www.cbp.gov/travel/trusted-traveler-programs

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Machine Studies, 38*, 475–487.

Davis F. D. (2001). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. Ann Arbor: Computer and Information Systems, Graduate School of Business Administration, University of Michigan.

Davis, S. G. (1994). Touching big brother: How biometric technology will fuse flesh and machine. *Information Technology & People, 7*(4), 1–9.

Electronic Frontier Foundation. (2006). Biometrics: Who's watching you? *Electronic*

Frontier Foundation. Retrieved from http://www.eff.org/wp/biometrics-whos-watching-you

Electronic Privacy Information Center (EPIC) (2016) Analysis of Specific US PATRIOT Act Provisions: Expanded Dissemination of Information Obtained in Criminal Investigations, https://epic.org Retrieved 20, July 2016.

European Commission. (2005). *Biometrics at the frontiers: Assessing the impact on society*. Spain: Joint Research Center, Institute of Prospective Technological Studies, Seville.

Hing, L., Jain, A. K., Pankanti, S., Prabhakar, S., Ross, A., & Wayman, J. L. (2004, August). Biometrics: A grand challenge. *The Proceedings of the International Conference on Pattern Recognition*, Cambridge, UK.

Hong, J. H., Yun, E. K., & Cho, S. B. (2005). A review of performance evaluation for biometrics systems. *International Journal of Image and Graphics, 5*(3), 501–536.

IdentoGO. (2016). Services. Retrieved from: https://www.indentogo.com/services

International Biometric Group. (2008). *Independent biometrics enterprise.* Retrieved from: http://www.biometricgroup.com/reports/public/market_report.html

Jackson, B., Chan, E. & LaTourrette, T. (2011) Assessing the security benefits of a trusted traveler program in the presence of attempted attacker exploitation and compromise. *RAND Corporation* 2011. DOI 10.1007/s12198-011-0077-0

Jahangir, N. & Begum, N. (2008). The role of perceived usefulness, perceived ease of use, Security and privacy, and customer attitude to engender customer adaptation in the context of electronic banking. *African Journal of Business Management,* Vol. 2, (1) pp. 032–040.

Jain, A. K., & Ross, A. (2008). Biometrics recognition: Techniques, applications and challenges. Retrieved from http://www.comp.hkbu.edu.hk/~icpr06/tutorials/Jain.html

Jain, A. K., Ross, A. and Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE, 14*(1), 1–29.

Joshua, A. J., & Koshy, M. P. (2009). Attitudes and behavioral intentions towards a technology based self-service banking delivery channel: The case of ATMs. *Erudition, Vol. 3 (1)*

Kim, J. (2006). *Biometrics in hotel industry: Issues that impact customers' acceptance.* (Unpublished master's thesis). University of Las Vegas, Las Vegas, Nevada.

Lazarick, R. & Cambier, J.L. (2008). Biometrics in the government sector, in Jain, A.K., Flynn, P. and Ross, A.A. (Eds), Handbook of Biometrics, Springer, Berlin, pp. 461-78.

Lease, D. R. (2005). *Factors influencing the adoption of biometric security technologies by decision making information technology and security managers.* (Unpublished doctoral dissertation). Capella University, Minneapolis.

Liu, S., Silverman, M. (2001). A practical guide to biometric security technology. *IT Professional,* Vol. 3 (1) 27–32. DOI: 10.1109/6294.899930

Liu, Y. (2008). Identifying legal concerns in the biometric context. *Journal of International Commercial Law and Technology, 3*(1), 45–54.

Mahinda, E., & Whitworth, B., (2005). The web of system performance: Extending the TAM model. *Information Systems Evaluation Track*. Americas Conference on Information Systems, Omaha, Nebraska.

Merlano, S (2014) Privacy Concerns Regarding the Use of Biometrics in Trusted Traveler Programs Prospectus, PP. 1-14

Mordini, E., & Petrini, C. (2007). Ethical and social implications of biometric identification technology. *Ann Ist Super Santa*, *43*(1), 5–11.

Morgan, D., & Krouse, W. (2005). Biometric identifiers and border security: 9/11 Commission recommendations and related issues. *Congressional Research Service*, Washington, DC.

Morosan, C (2012) Voluntary Step toward Air Travel Security: An Examination of Travelers' Attitudes and Intentions to Use Biometric Systems, *Journal of Travel Research*. Sage Publications, Inc. DOI: 10.1177/0047287511418368

National Science Technology Council. (2006a). *Biometrics glossary: Introduction*. Washington, DC: Government Printing Office.

National Science Technology Council. (2006b). *The national biometrics challenge*. Washington, DC: Government Printing Office.

National Science Technology Council. (2006c). *Subcommittee on biometrics and identity management committee on technology*. Washington, DC: Government Printing Office.

National Science Technology Council. (2006d). *Privacy and biometrics: Building a conceptual foundation*. Washington, DC: Government Printing Office.

Nelson, L. (2004). Privacy and Technology; Reconsidering a Crucial Public Policy Debate in the Post-September 11th Era. *Public Administration Review*. 64(3), 259-269.

Neyland, D. (2009). Who's Who?: The Biometric Future and the Politics of Identity. *European Journal of Criminology, 6*(135), 135-155.

Office of Biometric Identity Management. (2015). U.S. Department of Homeland Security. Retrieved from: https://www.dhs.gov/obim

Patton, M. Q. (2002) *Qualitative Research & Evaluation Methods:* 3rd Edition, Thousand Oaks, CA: Sage Publications.

Penna, S. & Kirby, S. (2009). Children and the ‘new bio politics of control’: identification, identity and social order. *The National Association for Youth Justice,* Vol. 9(2), Sage Publications, Inc, DOI: 10.1177/14732225409105493.

Pilgrim, T. (2007). *Biometrics and privacy*. Retrieved from http://www.privacy.gov.au/materials/types/speeches/view/6324

Rajchel, L. (2007). *Cross-jurisdictional and societal aspects of implementation of biometric technologies, part 1: Guide to the accessibility, privacy, and health and safety issues in the deployment of biometric systems for commercial applications*, New York, NY: International Standard Organization.

RAND Corporation. (2011) Trusted Traveler Program Should Result in Security Benefits https://sm.asisonline.org/Pages/rand-trusted-traveler-program-should-result-security-benefits-008568.aspx

Richards, N.M. & Solove, D.S (2010). Prosser's privacy law: a mixed legacy. *California Law Review*. Vol. 98 (6). DOI 10.15779/z3854IP

Sasse, A. M. (n.d). *Usability and user acceptance of biometrics*. London, England: University College.

Shen, D., Laffer, J., Lin, Yimei, & Huang, Xinxin. (2006, Winter). Social influence for perceived usefulness and ease-of-use of course delivery systems. *Journal of Interactive Online Learning, 5*(3), 270–282.

Singleton, R., & Straits, B. (2005). *Approaches to social research* (4th ed.). New York, NY: Oxford University Press.

Steele, J (2015) CLEAR Expedited Airport Security Program – Is it worth while? http://thepointsguy.com/2015/03/clear-expedited-airport-security-program-is-it-worthwhile/

Taneja, A., Wang, A., & Reja, M. K. (n.d). *Assessing the impact of concern for privacy and innovation characteristics in the adoption of biometrics technologies*. University of Texas at Arlington, TX.

Tashakkori, A. & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches.* Thousand Oaks, CA: Sage Publications.

The 9/11 Commission (2004). 9/11 Commission Report: The Final Report of the National Commission on Terrorist Attacks Upon the United States. Chaired by T.H. Kean New York; NY. W.W. Norton and Company.

Transportation Security Administration. (2008). *TSA registered traveler: Security, privacy and compliance standards for sponsoring entities and service providers,* *version 3.1*. Retrieved from http://www.tsa.gov/assets/pdf/rt_standards_v3.1.pdf

Transportation Security Administration. (2013). Trusted Traveler Program Pre-Check and Secure Flight, http://www.tsa.gov/secureflight

U.S. Department of Homeland Security, Office of Inspector General, Office of Information Technology. (2006). *CBP's trusted traveler systems using RFID technology require enhanced security (Redacted)*.

U.S. Department of Homeland Security, Office of Inspector General. (2008). *Letter report: DHS National Applications Office privacy stewardship*. Washington, DC:

U.S. Department of Homeland Security, Office of Inspector General. (2005). *Review of the Transportation Security Administration's role in the use and dissemination of airline passenger data (redacted)*. Washington, DC.

U.S. Department of Homeland Security, Office of Inspector General. (2014), *Enhancement in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs.* Washington, DC

United States General Accountability Office. (2002). *Aviation Security, Registered Traveler Program Policy and Implementation Issues,* Report to the Honorable Kay Bailey Hutchison, U.S. Senate. Retrieved from http://www.gao.gov/new.items/d03253.pdf (accessed February 22, 2010).

United States General Accountability Office. (2002). *Technology assessment: Using biometrics for border security*. Washington, D.C.

United States General Accountability Office. (2005). *Use of biometrics to improve aviation security: Hearing before the Subcommittee on Aviation of the Committee on Transportation and Infrastructure, House of Representatives, One Hundred Eight Congress, second session, May 19, 2004*. Washington: U.S. G.P.O.

United States General Accountability Office. (2014a). *Aviation security: rapid growth in expedited passenger screening highlights need to plan effective security assessments: report to congressional requesters*. Washington, D.C.

United States General Accountability Office. (2014b). *Trusted travelers: programs provide benefits, but enrollment processes could be strengthened: report to congressional requesters.* Washington, D.C.

United States. General Accounting Office. (2002). *Aviation security: Registered traveler program policy and implementation issues*. Washington, D.C.

United States. General Accounting Office. (2007). *Continuing attention to privacy concerns is needed as programs are developed*. Washington, DC.

United States General Accounting Office. (2015) *Facial Recognition Technology, Commerical Uses, Privacy Issues, and Applicable Federal Laws,* Washington, D.C.

Wahid, F. (2007). Using the technology adoption model to analyze internet adoption and use among men and women in Indonesia. *The Electronic Journal on Information Systems in Developing Countries, 32*(6), 1–8.

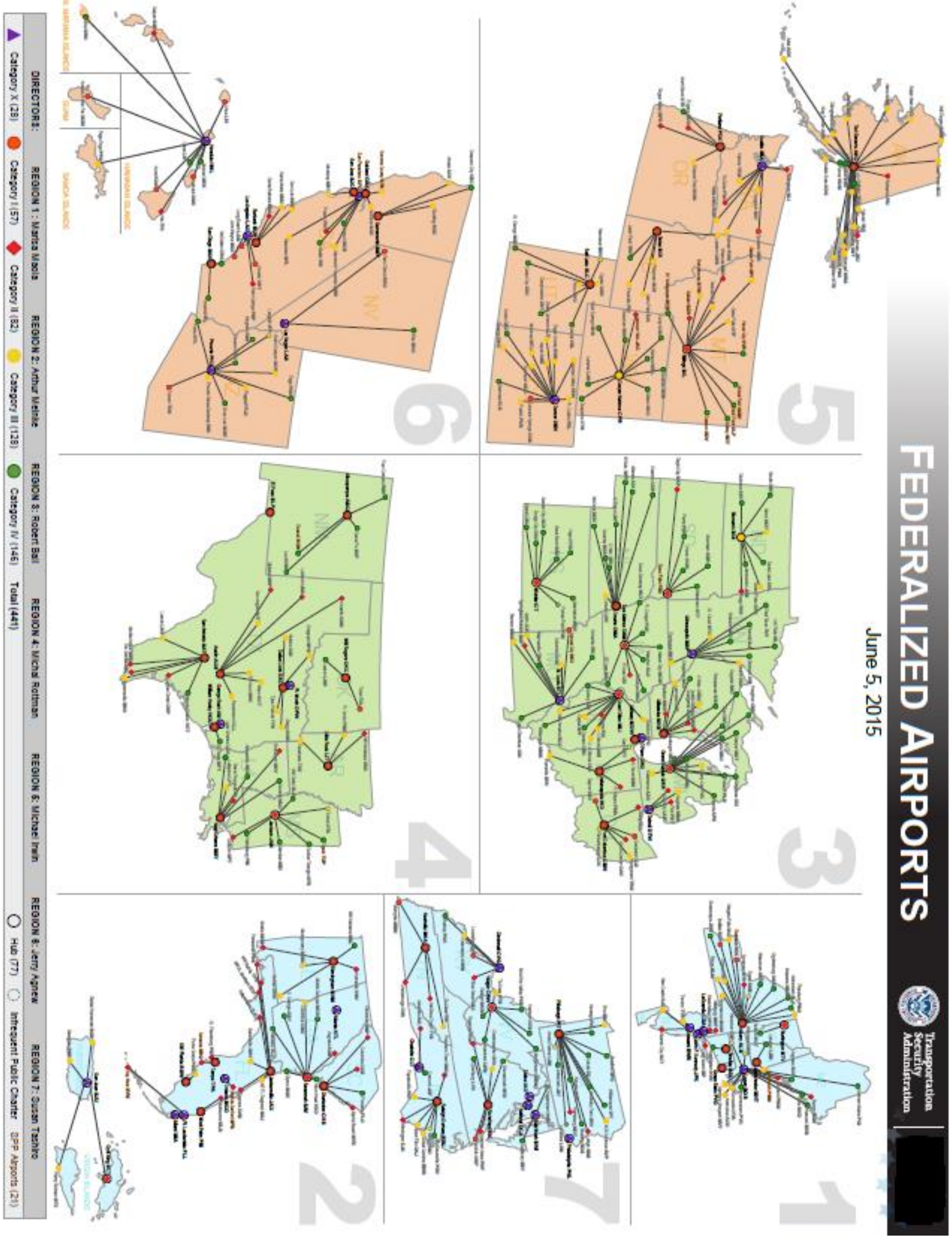
Watkins, M. (2007). *Biometrics: Introduction*. Retrieved from http://www.cippic.ca/biometrics/

Weber, K. (2006). Privacy invasions: New technology that can identify anyone anywhere challenges how we balance individuals' privacy against public goals. *European Molecular Biology Organization, Vol. 7* (Special Issue), S36–S39.

Westin, A. (2002). *Public attitudes toward the use of biometric identification technologies by government and private sector.* Princeton, NJ: Opinion Research International.

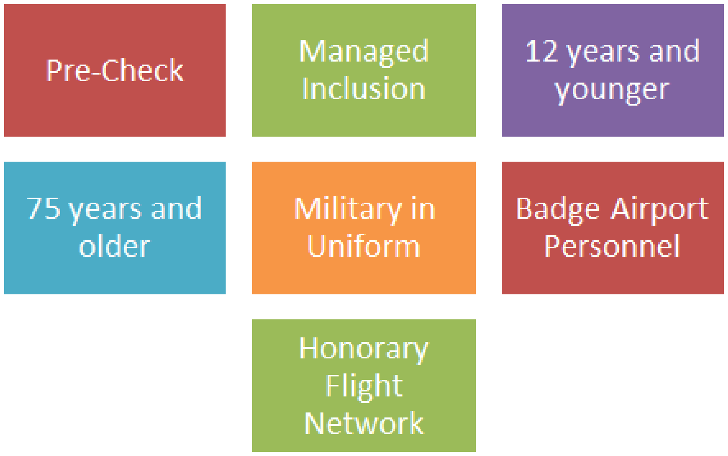
Zorkadis, V., and Donos, P. (2004). On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements. *Information Management & Computer Security, 12*(1), 125–137

Appendix A: TSA Federalized Airports



Appendix B: Seven Categories the TSA Uses for Expedited Screening

The Seven Categories the TSA uses for Expedited Screening at U.S. Airports



Pre-Check

Managed Inclusion

12 years and younger

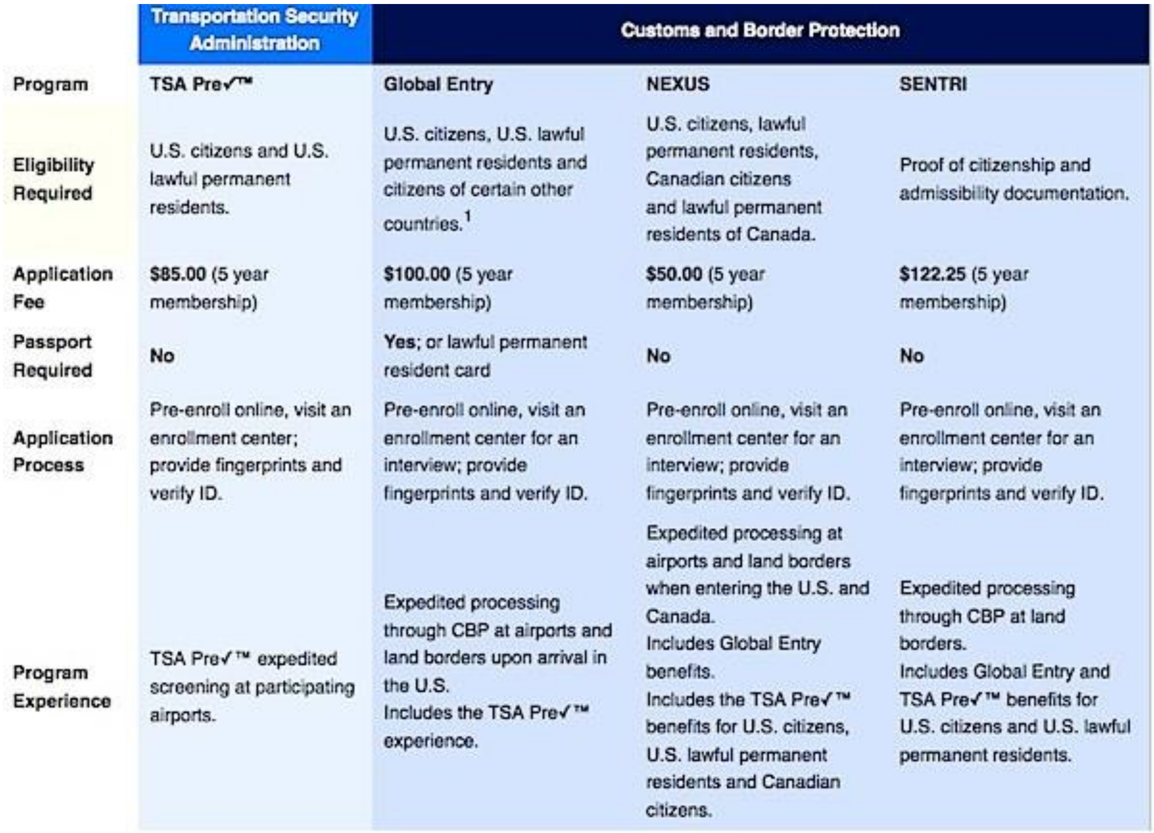
75 years and older

Military in Uniform

Badge Airport Personnel

Honorary Flight Network

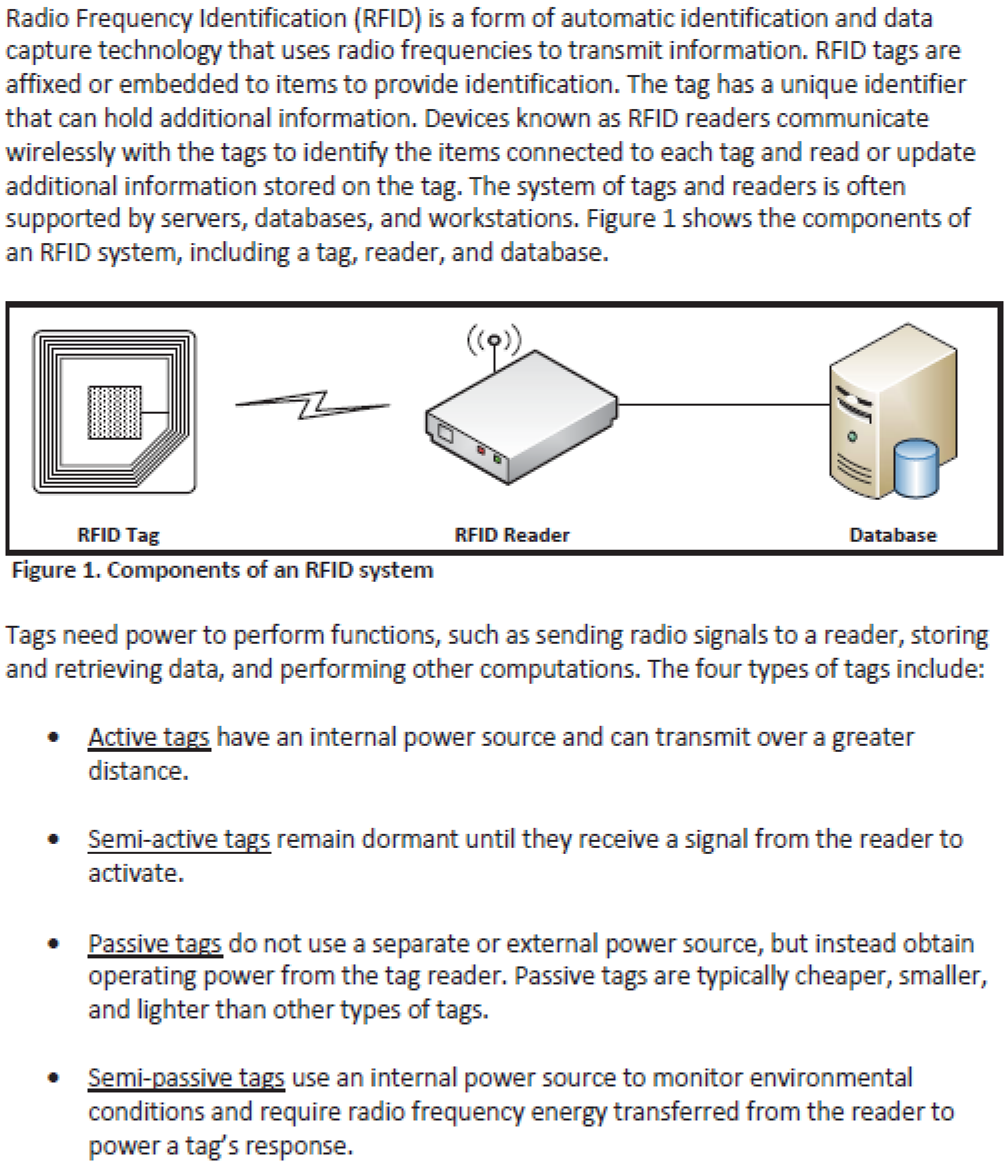
Appendix C: List of the Trusted Traveler Programs in the United States



	Transportation Security Administration	Customs and Border Protection		
Program	**TSA Pre✓™**	**Global Entry**	**NEXUS**	**SENTRI**
Eligibility Required	U.S. citizens and U.S. lawful permanent residents.	U.S. citizens, U.S. lawful permanent residents and citizens of certain other countries.[1]	U.S. citizens, lawful permanent residents, Canadian citizens and lawful permanent residents of Canada.	Proof of citizenship and admissibility documentation.
Application Fee	**$85.00** (5 year membership)	**$100.00** (5 year membership)	**$50.00** (5 year membership)	**$122.25** (5 year membership)
Passport Required	**No**	**Yes**; or lawful permanent resident card	**No**	**No**
Application Process	Pre-enroll online, visit an enrollment center; provide fingerprints and verify ID.	Pre-enroll online, visit an enrollment center for an interview; provide fingerprints and verify ID.	Pre-enroll online, visit an enrollment center for an interview; provide fingerprints and verify ID.	Pre-enroll online, visit an enrollment center for an interview; provide fingerprints and verify ID.
Program Experience	TSA Pre✓™ expedited screening at participating airports.	Expedited processing through CBP at airports and land borders upon arrival in the U.S. Includes the TSA Pre✓™ experience.	Expedited processing at airports and land borders when entering the U.S. and Canada. Includes Global Entry benefits. Includes the TSA Pre✓™ benefits for U.S. citizens, U.S. lawful permanent residents and Canadian citizens.	Expedited processing through CBP at land borders. Includes Global Entry and TSA Pre✓™ benefits for U.S. citizens and U.S. lawful permanent residents.

Courtesy of Department of Homeland Security, Customs and Border Protection (2015)

Appendix D: Radio Frequency Identification (RFID) system used by CBP Trusted Traveler Programs



Radio Frequency Identification (RFID) is a form of automatic identification and data capture technology that uses radio frequencies to transmit information. RFID tags are affixed or embedded to items to provide identification. The tag has a unique identifier that can hold additional information. Devices known as RFID readers communicate wirelessly with the tags to identify the items connected to each tag and read or update additional information stored on the tag. The system of tags and readers is often supported by servers, databases, and workstations. Figure 1 shows the components of an RFID system, including a tag, reader, and database.

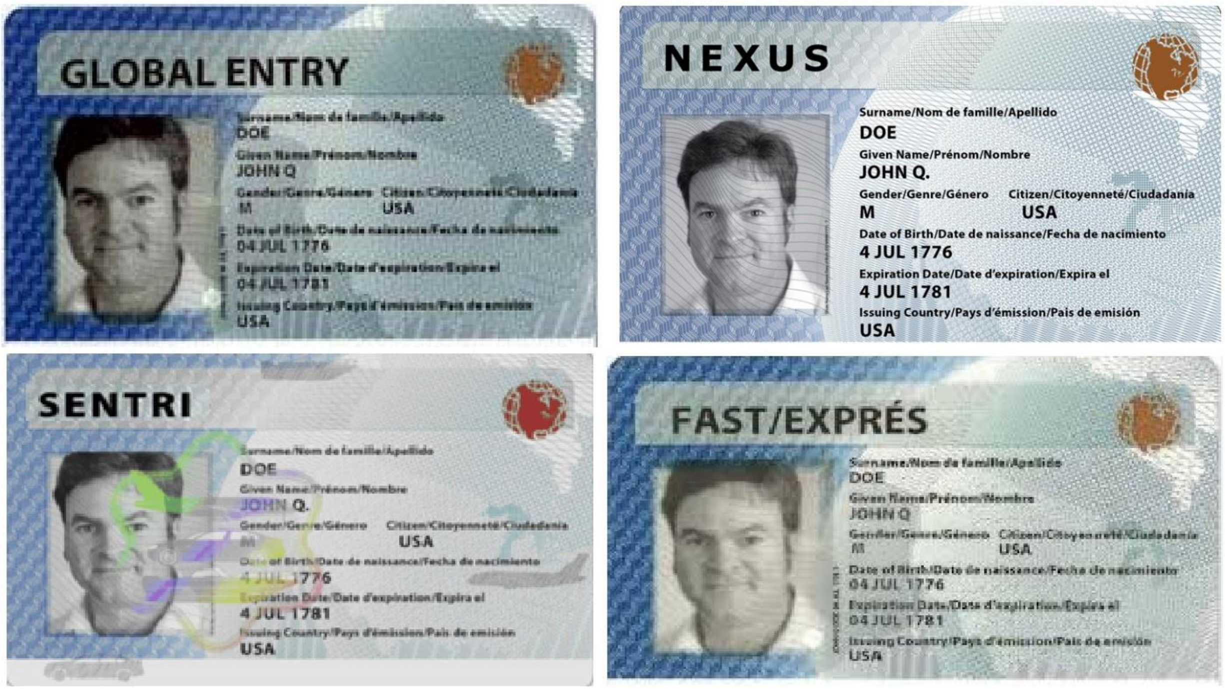
Figure 1. Components of an RFID system

Tags need power to perform functions, such as sending radio signals to a reader, storing and retrieving data, and performing other computations. The four types of tags include:

- Active tags have an internal power source and can transmit over a greater distance.
- Semi-active tags remain dormant until they receive a signal from the reader to activate.
- Passive tags do not use a separate or external power source, but instead obtain operating power from the tag reader. Passive tags are typically cheaper, smaller, and lighter than other types of tags.
- Semi-passive tags use an internal power source to monitor environmental conditions and require radio frequency energy transferred from the reader to power a tag's response.

Courtesy of Department of Homeland Security, Office of Inspector General (2014)

Appendix E: Sample of CBP Trusted Traveler Program Cards



GLOBAL ENTRY

Surname/Nom de famille/Apellido
DOE
Given Name/Prénom/Nombre
JOHN Q
Gender/Genre/Género Citizen/Citoyenneté/Ciudadania
M USA
Date of Birth/Date de naissance/Fecha de nacimiento
04 JUL 1776
Expiration Date/Date d'expiration/Expira el
04 JUL 1781
Issuing Country/Pays d'émission/Pais de emisión
USA

NEXUS

Surname/Nom de famille/Apellido
DOE
Given Name/Prénom/Nombre
JOHN Q.
Gender/Genre/Género Citizen/Citoyenneté/Ciudadania
M USA
Date of Birth/Date de naissance/Fecha de nacimiento
4 JUL 1776
Expiration Date/Date d'expiration/Expira el
4 JUL 1781
Issuing Country/Pays d'émission/Pais de emisión
USA

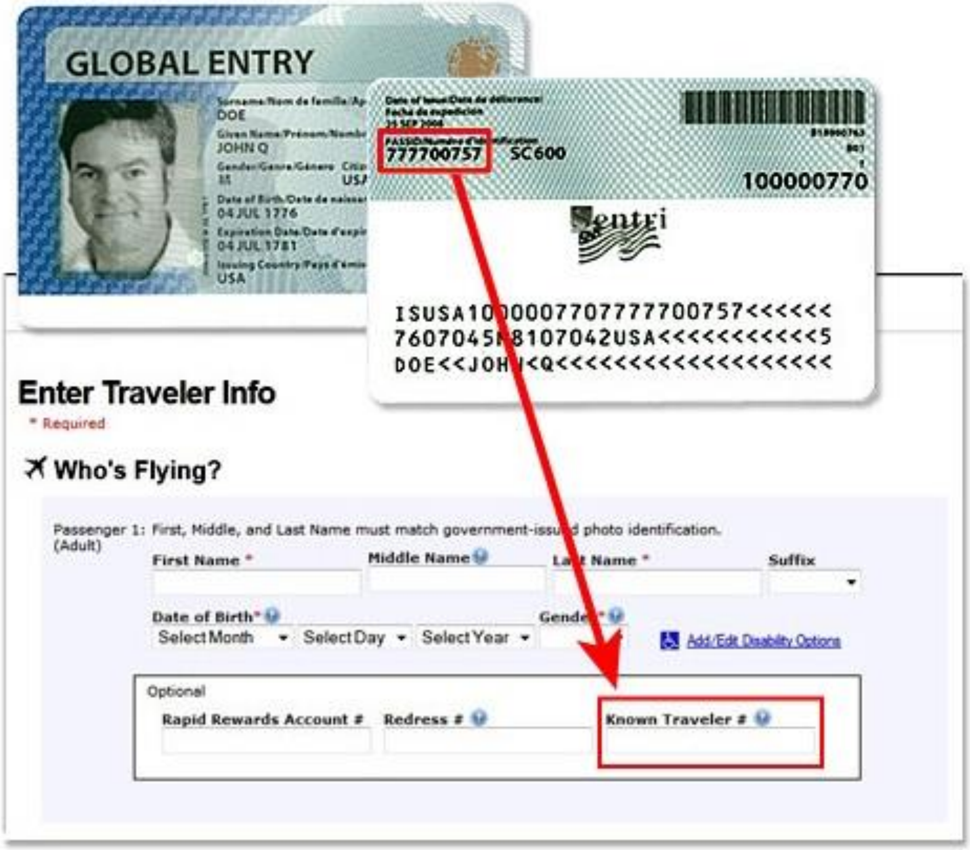
SENTRI

Surname/Nom de famille/Apellido
DOE
Given Name/Prénom/Nombre
JOHN Q.
Gender/Genre/Género Citizen/Citoyenneté/Ciudadania
M USA
Date of Birth/Date de naissance/Fecha de nacimiento
4 JUL 1776
Expiration Date/Date d'expiration/Expira el
4 JUL 1781
Issuing Country/Pays d'émission/Pais de emisión
USA

FAST/EXPRÉS

Surname/Nom de famille/Apellido
DOE
Given Name/Prénom/Nombre
JOHN Q
Gender/Genre/Género Citizen/Citoyenneté/Ciudadania
M USA
Date of Birth/Date de naissance/Fecha de nacimiento
04 JUL 1776
Expiration Date/Date d'expiration/Expira el
04 JUL 1781
Issuing Country/Pays d'émission/Pais de emisión
USA

Appendix F: The CBP Trusted Traveler Programs with the TSA Pre-✓™ System


GLOBAL ENTRY
Surname/Nom de famille/Ap
DOE
Given Name/Prénom/Nombr
JOHN Q
Gender/Genre/Género
USA
Date of Birth/Date de naissan
04 JUL 1776
Expiration Date/Date d'expir
04 JUL 1781
Issuing Country/Pays d'émis
USA
Date of Issue/Date de délivrance/
Fecha de expedición
PASSID/Numéro d'identification
777700757
SC600
100000770
Sentri
ISUSA10000077077777700757<<<<<<
7607045M8107042USA<<<<<<<<<<<<5
DOE<<JOHN<Q<<<<<<<<<<<<<<<<<<<<<

Enter Traveler Info

* Required

Who's Flying?

Passenger 1: (Adult) First, Middle, and Last Name must match government-issued photo identification.

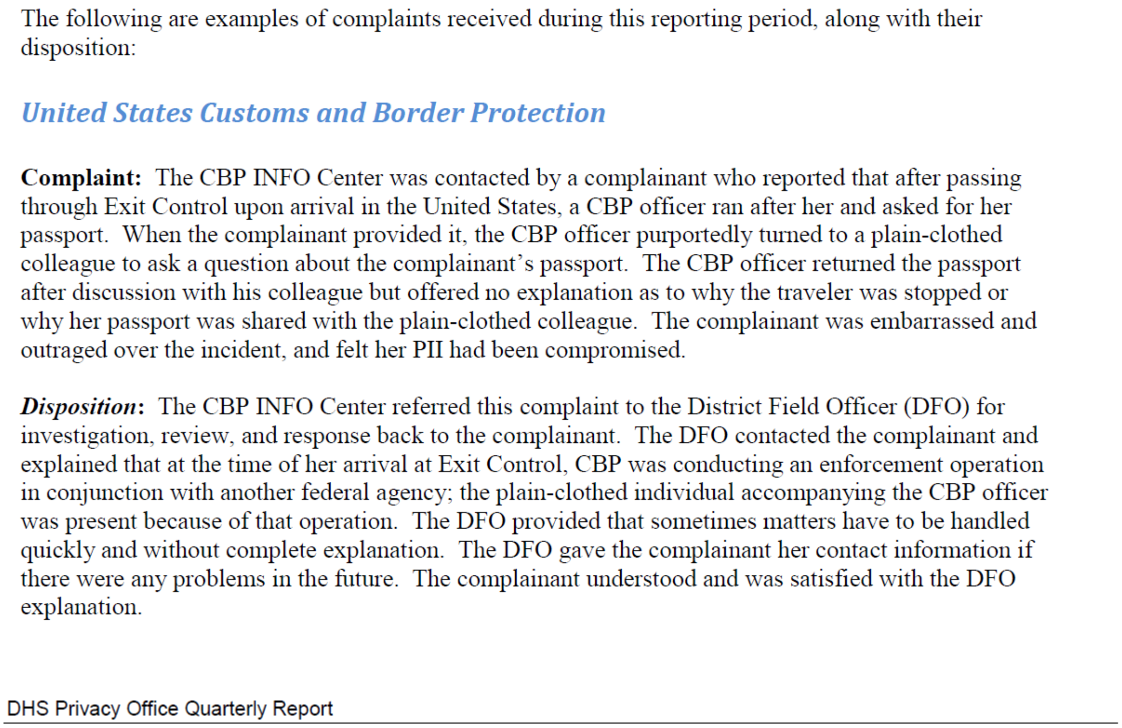
First Name * | Middle Name | Last Name * | Suffix

Date of Birth* Select Month Select Day Select Year | Gender* | Add/Edit Disability Options

Optional

Rapid Rewards Account # | Redress # | Known Traveler #

Appendix G: Samples of Privacy Complaints

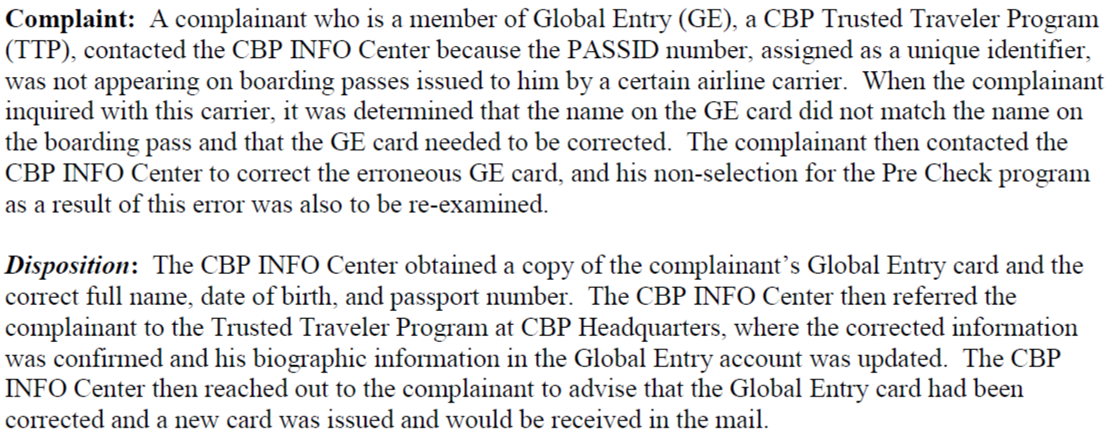


The following are examples of complaints received during this reporting period, along with their disposition:

United States Customs and Border Protection

Complaint: The CBP INFO Center was contacted by a complainant who reported that after passing through Exit Control upon arrival in the United States, a CBP officer ran after her and asked for her passport. When the complainant provided it, the CBP officer purportedly turned to a plain-clothed colleague to ask a question about the complainant's passport. The CBP officer returned the passport after discussion with his colleague but offered no explanation as to why the traveler was stopped or why her passport was shared with the plain-clothed colleague. The complainant was embarrassed and outraged over the incident, and felt her PII had been compromised.

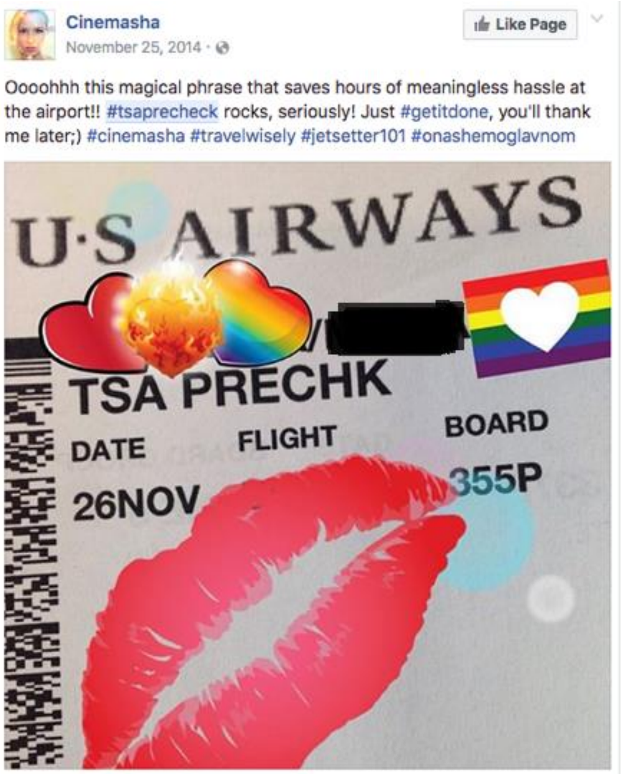
***Disposition*:** The CBP INFO Center referred this complaint to the District Field Officer (DFO) for investigation, review, and response back to the complainant. The DFO contacted the complainant and explained that at the time of her arrival at Exit Control, CBP was conducting an enforcement operation in conjunction with another federal agency; the plain-clothed individual accompanying the CBP officer was present because of that operation. The DFO provided that sometimes matters have to be handled quickly and without complete explanation. The DFO gave the complainant her contact information if there were any problems in the future. The complainant understood and was satisfied with the DFO explanation.



Complaint: A complainant who is a member of Global Entry (GE), a CBP Trusted Traveler Program (TTP), contacted the CBP INFO Center because the PASSID number, assigned as a unique identifier, was not appearing on boarding passes issued to him by a certain airline carrier. When the complainant inquired with this carrier, it was determined that the name on the GE card did not match the name on the boarding pass and that the GE card needed to be corrected. The complainant then contacted the CBP INFO Center to correct the erroneous GE card, and his non-selection for the Pre Check program as a result of this error was also to be re-examined.

***Disposition*:** The CBP INFO Center obtained a copy of the complainant's Global Entry card and the correct full name, date of birth, and passport number. The CBP INFO Center then referred the complainant to the Trusted Traveler Program at CBP Headquarters, where the corrected information was confirmed and his biographic information in the Global Entry account was updated. The CBP INFO Center then reached out to the complainant to advise that the Global Entry card had been corrected and a new card was issued and would be received in the mail.

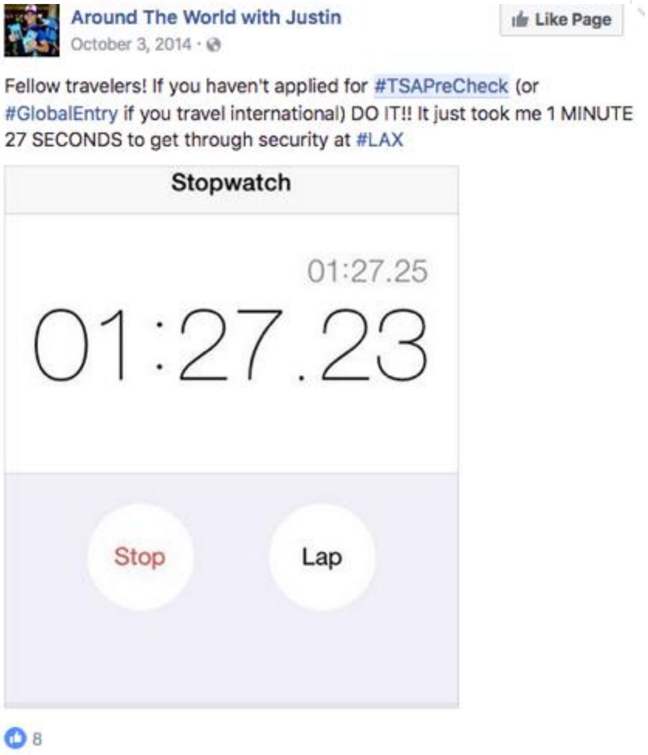
Appendix H: Samples of Social Media Posts



Cinemasha

November 25, 2014 ·

Oooohhh this magical phrase that saves hours of meaningless hassle at the airport!! #tsaprecheck rocks, seriously! Just #getitdone, you'll thank me later;) #cinemasha #travelwisely #jetsetter101 #onashemoglavnom



Around The World with Justin

October 3, 2014 ·

Fellow travelers! If you haven't applied for #TSAPreCheck (or #GlobalEntry if you travel international) DO IT!! It just took me 1 MINUTE 27 SECONDS to get through security at #LAX