The Impact of the Transportation Security Administration (TSA) Security Technologies on Passenger Privacy and Ethics Concerns

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Mark Schenkel
Spring, 2020

On my honor as a University Student, I have neither given nor received
unauthorized aid on this assignment as defined by the Honor Guidelines
for Thesis-Related Assignments

The Impact of the Transportation Security Administration (TSA) Security Technologies on Passenger Privacy and Ethics Concerns

Introduction

Ever since the deadliest terrorist attacks on American soil on September 11, 2001, airport security changed forever. In response to these terrorist attacks, the Transportation Security Administration (TSA) was formed to help avoid similar future attacks (Smith, 2011). While the cause was noble, there has recently been attention called to concerns that the TSA is overreaching its bounds, perhaps becoming "another federal agency infringing on constitutional rights" (Prince, 2017). This Science, Technology, and Society (STS) topic is important because it sheds light on TSA security procedures that many people partake in on a regular basis. This process is a system that the general public takes for granted when they fly, but citizens' constitutional rights are being violated by invasive technology. This brings into question the personal privacy cornerstone to the democracy in the United States, which is relevant to all American citizens. Due to the fact that the TSA is a federal agency and that there are laws surrounding citizen privacy, the STS framework of Political Technology is a natural fit. This theory guides the creation of the argument to address the STS topic. Overall, the research question is: how do TSA security technologies impact passenger privacy and ethics concerns?

Research Question and Methods

The research question is: How do Transportation Security Administration (TSA) security technologies impact passenger privacy and ethics concerns? To answer this research question, documentary research, historical case studies, and policy analysis methods are used.

Through documentary research, important background information is provided to the reader to set-up the relevant context of the current situation. The information is organized to naturally flow from the formation of the TSA to the current TSA security policies and procedures, with a focus on biometrics. The use of biometrics has recently become quite prevalent in airports and TSA procedures. This groundbreaking technology is not necessarily fully understood by the average flier, so this paper explains what the technology is and how it is implemented by the TSA. The biometric-related information stems from different resources, such as the master's thesis *Airport Passenger Processing Technology: A Biometric Airport Journey* written by Vishra Patel. Also, James O'Reilly, an international expert on privacy protection, writes in his paper about the conflict between the right to personal privacy and homeland security in the War on Terrorism (O'Reilly, 2008). This source sets the stage for where the United States currently stands in the midst of security versus privacy.

Furthermore, historical case studies and policy analysis blend well to create the argument to answer the research question. Citizen examples of privacy being violated by the TSA are cross-checked with current TSA policies. This comparison explores how current procedures are either supported or contrasted by historical case study evidence. For example, in "Fed up with Being Felt up: The Complicated Relationship Between the Fourth Amendment and Tsa's "Body Scanners" and "Pat-Downs," J.D. student Brittany Stancombe analyzes citizen's personal interactions with the TSA. This analysis, along with other passenger testimonies, is compared with current TSA security policy to understand how TSA procedures are possibly breached.

Background Information on STS Topic

The deadliest terrorist attack to ever happen on American soil, 9/11, was the main reason for the creation of the TSA. Four U.S. airliners were hijacked by nineteen terrorists and nearly 3,000 people died (Transportation Security Timeline). Two planes crashed into the World Trade

Center in New York, one into the Pentagon in Washington, D.C., and one into a field in Pennsylvania. As a result of these attacks, President George W. Bush signed into law the Aviation and Transportation Security Act. This monumental legislation created a new federal agency whose purpose was to strengthen the nation’s transportation systems while also ensuring the free movement of commerce and people. Thus, the TSA was born.

Contrary to popular belief, TSA security procedures do not start and end at security checkpoints in the airport. In fact, security procedures start when making an airline reservation and do not end until the end of a flight (Did you know your security doesn’t start or end at the security checkpoint?) Regardless, most of the controversy surrounding TSA security procedures stems from full-body scanners and pat-downs, therefore this paper focuses on those areas of the security process in particular.

TSA uses full-body scanners to safely screen passengers without physical contact for metallic and non-metallic threats, including weapons and explosives, which may be concealed under clothing (Security Screening). Passengers have the opportunity to decline full-body scanners in favor of physical screening, however, some passengers are required to undergo full-body scanners if their boarding pass indicates that they have been selected for enhanced screening prior to their arrival at the security checkpoint. TSA has strict privacy standards when using full-body scanners to protect passenger privacy. Full-body scanners use automated target recognition software that eliminates passenger-specific images and instead auto-detects potential threats by indicating their location on a generic outline of a person.

On the other hand, pat-down procedures are used to determine whether prohibited items or other threats to transportation security are concealed on the person (Security Screening). A passenger may be required to undergo a pat-down procedure if the full-body scanner alarms. Pat-downs may include inspection of the head, neck, arms, torso, legs, and feet. These pat-downs include head coverings and sensitive areas such as breasts, groin, and the buttocks. Pat-downs require sufficient pressure to ensure detection, and areas may undergo a pat-down more than once for the TSA officer to confirm no threat items are detected. TSA officers use the back of the hands for pat-downs over sensitive areas of the body. A passenger receives a pat-down by an officer of the same gender, and officers explain the procedures to the passenger as they conduct the pat-down. Even with these policies in place, passengers may feel that their privacy is being violated. For example, a physical inspection of the groin area for a transgender passenger can be very controversial (Waldron & Medina, 2019).

Lastly, the TSA is experimenting with two kinds of biometric technology: fingerprint scanning and facial recognition. In 2017, pilot programs were implemented at Denver and Atlanta airports' TSA PreCheck lanes (TSA Assessing Innovative Biometric Fingerprint Technology). The biometric authentication technology enables a traveler's fingerprints to serve as both a boarding pass and identity document. The technology matches passenger fingerprints provided at the checkpoint to those that have previously been provided to TSA by travelers when they enrolled in the TSA PreCheck program. During the data collection period, passengers volunteered to present their fingerprints. Fingerprints captured by the technology were deleted after each transaction and the TSA did not make any other uses of the fingerprints.

In 2018, Atlanta Airport tested facial recognition technology with passengers on a volunteer basis (Biometrics Technology). Once a passenger's photo was taken, Custom and Border Protection's (CBP) system attempted to compare that picture to photos in government databases, such as photos obtained from passports or visa applications, to verify the passenger's identity. TSA did not store the photograph. If CBP's system confirmed a match to a photograph in a government database, the passenger’s name and date of birth was sent from the database to a tablet used by the TSA officer. The goal of the fingerprint and facial recognition technology is to automate the security screening process to make the passenger experience more seamless. However, what happens if these databases are breached? Personally identifiable information could be leaked, creating a privacy issue.

The TSA and Political Technologies

The field of STS combines science, technology, and society. In the case of TSA security procedures, the science and technology piece is full-body scanners and pat-downs, and the societal piece is the technologies that are influencing privacy and ethics concerns among the public. There is a gray area between security and privacy, so how far is too far in the name of security? This tension between security technology being too invasive and society’s concerns with personal privacy fuels this topic’s conversation in the field of STS. Due to the fact that the TSA is a federal government agency and there are regulations regarding citizen privacy, the STS theory of Political Technology is a logical framework for this topic.

Langdon Winner is an American political theorist who remarks that technological artifacts can have politics when they become “a way of settling an issue in a particular community” (Winner, 1980). In this case, TSA security procedures are used to ‘settle the issue’ of airport security and domestic terrorism. Winner also states that political technologies are “man-made systems that appear to require, or to be strongly compatible with, particular kinds of political relationships.” Technology such as full-body scanners are certainly man-made, and because the TSA is overseen by the federal government, there are political relationships that must be overcome whenever the TSA wants to implement new policy.

In addition, James Poulos, a political scientist from the Claremont Institute, states that "we tend to focus on the remarkable quantitative leaps forward in speed, scale, volume, and accessibility of information made possible by the advances of this era … yet our reflections on what such changes will mean — and especially on the effects they are likely to have on our political life — have generally been superficial" (Poulos, 2016). He calls for a deeper look into the impacts of technology on politics. Particularly in the field of aviation and TSA, there has not been much research done on the effects of security technology on passenger privacy. Thus, that is the focus of this paper.

The framework of Political Technology is used to guide the answer to the research question. TSA policy is examined in two ways: what is written by the TSA and how it is implemented in passenger testimonies. The similarities and differences found between these two sets of analysis are the basis for the answer to the research question. Other considerations, such as scholarly articles and papers that address the issues of security versus privacy, are also used as evidence.

Results and Discussion

There are two main components that impact passenger privacy and ethics concerns: a breach of personal data and a violation of sensitive physical space. In terms of a breach of personal data, the TSA PreCheck program is gathering personal information about passengers, including biometric data. As these databases grow, it is not a question of 'if' but 'when' a hack will occur. Unfortunately, biometrics that are stolen are impossible to recover (Patel, 2018). This information is even more sensitive than just a name or date of birth because biometric data is unique to every individual, whereas more generic information is not as personally identifiable. In terms of the violation of private physical space, there are multiple examples of passengers and even pilots who have testimonies of the TSA invading their personal space. Passengers who represent a minority, including ethnic, religious, and LGBTQ+ passengers, have also spoken out about not being properly accommodated (Waldron & Medina, 2019). Some of these cases have even been taken to court as a violation of the Fourth Amendment. These data and physical infringements demonstrate that the TSA must establish a balance between the level of intrusiveness in its security policies and the government interest in securing U.S. flights.

To begin with personal data, TSA PreCheck is an expedited airport security screening process that is just one of the ways the TSA collects personal information about passengers. PreCheck passengers can get through security checkpoints faster by not having to remove their shoes, laptops, liquids, belts, or light jackets (TSA PreCheck). However, with the expansion of this program, privacy experts warn against giving up personal data for a fast trip through a checkpoint (Jansen, 2014). Jay Stanley, a senior policy analyst at the American Civil Liberties Union (ACLU), says that TSA's assessments will either be "based on a laughable amount of information about people and will only be providing an illusion of security, or they will be so intrusive that the government will basically be doing background checks on everyone who flies" (Jansen, 2014). This assessment demonstrates how politics and the government are involved with the technology that the TSA uses for its security screenings. The data that passengers provide for security purposes are being stored in databases that the government owns. Langdon Winner, an American political theorist, states that a technology can be inherently political if it correlates with particular kinds of political relationships (Winner, 1980). In this case, the political relationship forms when biometric passenger data is held by a government agency.

Unfortunately, these databases are prone to hacking. In the words of Jeremy Epstein, the CEO of a blockchain startup, “any security expert will tell you a hack is not a question of “if,” just a question of “when” (Epstein, 2019). Just recently in June 2019, the U.S. Customers and Border Patrol (CBP) had “a data breach in which tens of thousands of images of travelers…were hacked” (Baran, 2019). The breach comes just as CBP and TSA have been working to expand the use of biometric technology to help verify travelers’ identities, which includes both facial and fingerprint recognition (Baran, 2019). In his master’s thesis about airport passenger processing technology, Vishra Patel explains that “it is easy to steal biometric data through hacking” and that “the threat of identity fraud is always present” (Patel, 2018). He also states that “if a system is compromised and the biometric credentials are leaked, the revocability of biometric data is impossible” (Patel, 2018). Here again, it is evident that this is a case of Political Technology because the government is being held responsible for personally identifiable information about the general public. If the government servers are hacked, the government’s constituents are put at risk. The way in which the TSA carries out their procedures stem directly from laws passed by the federal government. While such programs like TSA PreCheck are more efficient in terms of shorter wait times, the tradeoff with an increased security risk needs to be recognized.

In addition, Department of Homeland Security (DHS) audits revealed that there are serious persistent problems with the TSA’s handling of information technology (IT) security protocols (Blue, 2016). The final report from the DHS Office of Inspector General outlines how there are “servers running software with known vulnerabilities, no incident report process in place, and zero physical security protecting critical IT systems from authorized access” (Blue, 2016). The Security Technology Integrated Program (STIP) is a data management system that connects airport screening equipment to centralized servers (Blue, 2016). The TSA has not been following DHS guidelines for handling STIP equipment, and risks a “potential loss of confidentiality, integrity, and availability of TSA’s automated explosive, passenger, and baggage screening programs" (Blue, 2016). Federal government regulations are being compromised at the expense of the general public’s security, which is a major contributor to how TSA security procedures are a mishandled Political Technology.

Furthermore, beyond the data, there are physical privacy violations that have occurred at TSA security checkpoints in airports. These violations have occurred to people who have medical conditions, who are people of color, who are of certain religious backgrounds, and who identify with the LGBTQ+ community.

Passengers who travel with medical devices, such as pacemakers, diabetic pumps, or bladder drainage bags can have a very difficult and invasive experience at TSA checkpoints. Inevitably, their medical devices set-off the body-scanners, resulting in further screening and pat-downs. For example, in 2010, bladder cancer survivor Thomas Sawyer was selected for additional screening after his body scan set-off alarms, and he requested to be searched in private (Stancombe, 2011). “Despite warnings given by Mr. Sawyer to the TSA officer about the [urostomy] bag, the officer continued the pat-down, burst the bag, and urine spilled all over Mr. Sawyer’s clothing” (Stancombe, 2011). Similarly, Cathy Bossi, a breast cancer survivor, was “forced to remove her prosthetic breast during an enhanced pat-down” (Stancombe, 2011). However, according to official TSA procedure, passengers should not have to remove their prosthetic devices (Disabilities and Medical Conditions). This is a clear example of a TSA procedural violation, but unfortunately not a rare case for passengers traveling with medical devices. People with such devices will likely have a chance of being subjected to further screening every time they fly (Stancombe, 2011). Even government officials, who are able to bypass heightened security because they are considered federal law enforcement officers, are fed-up with the TSA. Jesse Ventura, former Governor of Minnesota, has a titanium hip replacement and filed a lawsuit against the TSA seeking an injunction, while “asking the court to deem the TSA’s enhanced security unconstitutional” (Stancombe, 2011). Again, the notion of Political Technology is shown very clearly because a government agency must handle lawsuits over a controversial technology that it is employing.

Along with passengers, pilots are also frustrated with their experiences. Captain Dave Bates states that the enhanced security screening is “a demeaning experience” (Stancombe, 2011). He is even worried about the professional appearance of having a uniformed pilot be screened in front of other passengers, recommending that “such screening is performed in an out-of-view area to protect their privacy and dignity” (Stancombe, 2011). This evidence shows how all parties involved in the security screening process are affected, not just passengers.

There are also concerns for people of certain color and religious affiliations. A report by ProPublica suggests that full-body scanners have trouble identifying potential threats in thick hair and certain head coverings (Medina, 2019). Black passengers who wear their hair naturally – or who wear it in styles that are typically associated with black culture, like braids or dreadlocks – seem to be disproportionately targeted (Del Valle, 2019). In other words, the machines that were created to determine whether or not a potential threat exists were not designed with people of color in mind. This is another clear example of a mishandled Political Technology. The politics and regulations behind the TSA’s full-body scanner technology has negative effects on the public, specifically a minority group. However, according to TSA security procedures, agents have the discretion to pat-down passengers if “an individual’s hair looks like it could contain a prohibited item or is styled in a way an officer cannot visually clear it" (Burns, 2016). Regardless of whether it was intentional, the scanners were not built to take into account certain forms of self-presentation, and unfortunately that oversight is resulting in potential racist profiling.

Furthermore, transgender and gender nonconforming passengers say that they have been pressured to expose their genitals during TSA searches (Waldron & Medina, 2019). These incidences stem from shortcomings in the TSA's technology and insufficient training of its staff. In September 2018, transgender woman Terra Fox set-off alarms of a full-body scanner that showed a yellow box over her groin (Waldron & Medina, 2019). Fox said that she told the officers that she is a transgender woman and that the scanner was simply detecting her genitals. Fox asked to be patted down by a woman, but the female officers near her refused to do it. Two male officers brought her to a private room and instructed her to pull down her leggings and show them her genitals. She complied, but the screening lasted so long that she missed her flight. She mentioned that the experience has taken a toll on her. "Every time I travel, I have to cry and feel humiliated," she said (Waldron & Medina, 2019). According to TSA policy, passengers will "receive a pat-down by an officer of the same gender" (Security Screening). Fox identifies as a female but was screened by male agents. This is another clear violation of TSA policy. Unfortunately, full-body scanners are "programmed to look for penises on passengers scanned as male and breasts on passengers scanned as female" (Waldron & Medina, 2019). Here again, the scanner technology was not built for the correct audience. The regulations behind the scenes of this technology were created without taking into account passengers who identify as transgender, similar to the previous example of black passengers and their hair styles. The TSA needs to fix this ethical violation with updated policies and procedures. In February 2019, the TSA rolled out a new online transgender awareness training for its agents and is studying options for better technology (Waldron & Medina, 2019). However, lawmakers have said that the improvements have taken too long for a federal agency that interacts with the public more than many others. This goes to show that the TSA is failing some of its constituents and is not creating new regulations fast enough to keep up with its technology.

However, not all citizens and lawmakers are upset with the new procedures. It is important to remember that everyone is entitled to their own point of view, so everyone does not agree that there are privacy concerns. Former director of security at Northwest Airlines, John Laird, said that "it's a small liberty to give up for the safety of all" and that "pat-downs and body-scanners are designed to help TSA detect hidden and dangerous items such as explosives" (Stancombe, 2011). Safety is always a concern, and one does not need to look much further than the events of September 11, 2001 to remember why these security measures are in-place. Nonetheless, there is a fine line between security and privacy, so perhaps security screening procedures should be revisited.

For passengers who wish to challenge the TSA in their searches, the Fourth Amendment is their weapon of choice. The Fourth Amendment guarantees protection against unreasonable searches and seizures (U.S. Const. amend. IV). The right to privacy, on the other hand, has been recognized by the Supreme Court as one of the unenumerated rights of the due process clause of the Fifth and Fourteenth Amendments (Taylor, 2013). However, a "special needs" exception to the right against unreasonable searches and seizures has been found to exist by the United States Supreme Court (Michigan v. Sitz, 1990). It is this exception that allows searches to be conducted in airports without probable cause or the need for warrants to be issued (Taylor, 2013). Yet many still argue that full-body scanners and pat-downs violate the right to privacy. The ACLU has been concerned that the "TSA's use of pat-downs have led to substantial numbers of complaints about groping passengers' breasts, buttocks, and genitalia…passengers expect privacy underneath their clothing" (The Transportation Security Administration's Airline Passenger and Baggage Screening). The bottom line is that the Supreme Court still must deal with the issue of whether the use of TSA security technology is reasonable and ethical.

In conclusion, the TSA violates passenger privacy and ethics concerns through a breach of personal data and a violation of sensitive physical space. Many sources of evidence, as mentioned above, support this claim. Passengers cannot trust the databases that are supposed to store their personal information, which leads to a lack of trust in the TSA to protect their privacy. In addition, passenger testimonies reveal that travelers, especially those in minority groups, do not feel safe when they fly because their personal privacy is disregarded at the expense of security. This tradeoff represents an ethical issue. The TSA must balance the threat of terrorism with security procedures designed to stop those threats. As of today, that balance is not equal, leading to a compromise of passenger privacy and ethics concerns.

There are a few different limitations of this project, including the timeline of research and the information available about the topic. This paper was written in a nine-month period which naturally limits the depth and scope of the research question and topic. A more thorough analysis could be conducted if more time allowed. Also, the length of the research paper is approximately 12-15 pages, which confines the background information, explanation, and analysis to be concise and to-the-point. In addition, there has not been a significant amount of information published about this topic, especially regarding biometric data collection, which is where the TSA is focusing its future efforts. Biometric technology, as well as how to store and secure such information, is an up-and-coming field in the context of airport security. In the future, more analysis will have been conducted concerning the effectiveness of such practices. This analysis can be used to better answer a similar research question.

In terms of future work, research could be conducted about what airport security procedures are in other countries. The United States has had issues in the past with airport security, but other countries have better track records. A recommendation could be put forth as to what a new American security procedure would look like based on analysis of international airport security. In her paper *Touched by an Agent*, Courteney Taylor provides some preliminary analysis of this concept by examining Australian, Nigerian, and Israeli airport security systems (Taylor, 2013). This paper could be used as a starting point for additional research. Furthermore, some critics argue that the U.S. is engaging in “security theater,” or “the appearance of safety” (Levenson, 2014). The annual budget for the TSA exceeds $7 billion, so if the TSA drastically reduced its procedures that are simply alluding security, there would be a major savings to the government and taxpayers (Carey, 2018). Therefore, a future research paper could explore whether or not current TSA policies are even effective, let alone ethical, at stopping terrorist attacks.

Conclusion

To conclude, the TSA impacts privacy and ethics concerns through breaches of personal data and physical space. Numerous passenger testimonies and other concrete evidence from federal agencies have shown this to be true, and it is information that citizens who fly should take into consideration. Passengers deserve to know their rights when they go to the airport, even though most people take airport security for granted. This research sheds light on the fact that airport security procedures are far from perfect, and that because we live in a country that is ruled by and for the people, we have the power to make a difference.

References

Baran, M. (2019, June 11). Thousands of Traveler Photos Were Obtained in a U.S. Customs Data Breach. Retrieved February 19, 2020, from https://www.afar.com/magazine/thousands-of-traveler-photos-were-obtained-in-a-us-customs-data-breach

Biometrics Technology. (n.d.). Retrieved October 1, 2019, from https://www.tsa.gov/biometrics-technology.

Blue, V. (2016, May 20). The TSA is Failing Spectacularly at Cybersecurity. Retrieved February 19, 2020, from https://www.engadget.com/2016/05/20/the-tsa-is-failing-spectacularly-at-cybersecurity/?guccounter=1

Burns, B. (2016, April 21). Travel Tips In Over 140 Characters: Hair Pat-downs. Retrieved February 19, 2020, from https://www.tsa.gov/blog/2016/04/21/asktsa-travel-tips-over-140-characters-hair-pat-downs

Carey, L. (2018, April 13). Trump's Proposed FY 2019 Budget Request Leaves TSA Short, Oversight Subcommittee Says. Retrieved February 19, 2020, from https://transportationtodaynews.com/news/9053-trumps-proposed-fy-2019-budget-request-leaves-tsa-short-oversight-subcommittee-says/

Del Valle, G. (2019, April 17). How Airport Scanners Discriminate Against Passengers of Color. Retrieved from https://www.vox.com/the-goods/2019/4/17/18412450/tsa-airport-full-body-scanners-racist

Did you know your security doesn't start or end at the security checkpoint? (n.d.). Retrieved October 1, 2019, from https://www.tsa.gov/sites/default/files/resources/layers_of_security_factsheet.pdf.

Disabilities and Medical Conditions. (n.d.). Retrieved February 19, 2020, from https://www.tsa.gov/travel/special-procedures

Epstein, J. (2019, March 16). A Massive Biometric Breach is Only a Matter of Time. Retrieved February 19, 2020, from https://venturebeat.com/2019/03/16/a-massive-biometric-breach-is-only-a-matter-of-time/

Jansen, B. (2014, February 23). Privacy Concerns Swirl Around TSA Pre-Check Program. Retrieved February 19, 2020, from https://www.usatoday.com/story/travel/flights/2014/02/23/tsa-pre-check-expedited-aclu-epic/5208359/

Levenson, E. (2014, January 31). The TSA Is in the Business of 'Security Theater,' Not Security. Retrieved February 19, 2020, from https://www.theatlantic.com/national/archive/2014/01/tsa-business-security-theater-not-security/357599/

Medina, B. (2019, April 17). TSA Agents Say They're Not Discriminating Against Black Women, But Their Body Scanners Might Be. Retrieved February 19, 2020, from https://www.propublica.org/article/tsa-not-discriminating-against-black-women-but-their-body-scanners-might-be?utm_content=buffer9d49d&utm_medium=social&utm_source=twitter&utm_campaign=buffer

Michigan v. Sitz, 496 U.S. 444, 448-51 (1990)

O'Reilly, J. T. (2008). Don't Stick Your Head in the Sand. *Vital Speeches of the Day*, *74*(6), 258–266.

Patel, V. (2018). *Airport Passenger Processing Technology: A Biometric Airport Journey* (unpublished Master's thesis, Embry-Riddle Aeronautical University). Retrieved from https://commons.erau.edu/cgi/viewcontent.cgi?article=1384&context=edt

Poulos, J. (2016). Technology and Political Theory. Retrieved January 27, 2020, from https://www.nationalaffairs.com/publications/detail/technology-and-political-theory

Prince, E. J. (2017, May 10). Does the TSA Go too Far? Retrieved from https://merionwest.com/2017/05/10/should-we-even-have-the-tsa/.

Security Screening. (n.d.). Retrieved October 1, 2019, from https://www.tsa.gov/travel/security-screening.

Smith, M. (2011, September 1). *September 11 and the Transportation Security Administration*. Retrieved from https://americanhistory.si.edu/blog/2011/09/september-11-and-the-transportation-security-administration.html

Stancombe, B. R. (2011). Fed up with Being Felt up: The Complicated Relationship Between the Fourth Amendment and Tsa's "Body Scanners" and "Pat-Downs." *Cumberland Law Review*, *42*(1), 181–215.

Taylor, C. L. (2013). Touched by an Agent: Why the United States Should Look to the Rest of the World for a New Airport Security Scheme and Stop Using Full-Body Scanners. *Houston Journal of International Law*, *35*(2), 503–536.

The Transportation Security Administration's Airline Passenger and Baggage Screening, Senate, 109th Cong. (2006). Retrieved February 19, 2020, from https://www.govinfo.gov/content/pkg/CHRG-109shrg63551/html/CHRG-109shrg63551.htm

Transportation Security Timeline. (n.d.). Retrieved October 1, 2019, from https://www.tsa.gov/timeline.

TSA Assessing Innovative Biometric Fingerprint Technology. (2017, June 13). Retrieved January 26, 2020, from https://www.tsa.gov/news/releases/2017/06/13/tsa-assessing-innovative-biometric-fingerprint-technology

TSA PreCheck. (n.d.). Retrieved February 19, 2020, from https://www.tsa.gov/precheck

U.S. Const. amend. IV.

Waldron, L., & Medina, B. (2019, August 26). When Transgender Travelers Walk Into Scanners, Invasive Searches Sometimes Wait on the Other Side. Retrieved February 19, 2020, from https://www.propublica.org/article/tsa-transgender-travelers-scanners-invasive-searches-often-wait-on-the-other-side

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, *109*(1,), 121–136.