Privacy Impact Assessment
for

Automated Wait Time (AWT) Technology

DHS/TSA/PIA-037

August 3, 2012

Contact Point
Eric Chin
Branch Manager, Office of Security Operations
Transportation Security Administration
eric.chin@dhs.gov

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Transportation Security Administration (TSA) will test and deploy systems automating the collection of information to calculate passenger average wait time in the checkpoint queue. TSA's Automated Wait Time (AWT) system utilizes information broadcasted from Bluetooth®[1]-enabled devices carried by individuals in the general checkpoint queuing area to calculate wait times and deploy resources, as appropriate, to reduce delays in checkpoint queues. In the interest of transparency to the public, this Privacy Impact Assessment (PIA) is conducted pursuant to Section 222 of the Homeland Security Act to assess privacy risk from the AWT system. In order to ensure that AWT systems sustain and do not erode privacy protections, TSA developed and implemented processes that give effect to the Fair Information Practice Principles while generating statistical data used for improving checkpoint operations.

Introduction

A consequence of securing our nation's airports has been the creation of checkpoints fed by lines of people who must wait in line to be cleared for entry into the sterile areas of a terminal. These lines ebb and flow throughout the day and peak during holidays and other popular travel periods. Wait time data is an important element in evaluating the effectiveness of TSA's staffing models in order to effectively manage these lines. TSA has used manual processes to collect wait time data, but such processes are a labor-intensive utilization of the screening workforce and rely on small sample sizes that cannot be used to generate comprehensive staffing models. Further, reliance on the screening workforce unnecessarily distracted screening officers from their primary mission of providing passenger security. Accordingly, TSA discontinued the manual wait time collection practices.

Section 1612 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, requires TSA to "recruit and hire such personnel in the Administration as may be necessary (1) to provide appropriate levels of aviation security; and (2) to accomplish that goal in such a manner that the average aviation security-related delay experienced by airline passengers is reduced to a level of less than 10 minutes." TSA issued a Request for Information to identify automated solutions to assist in measuring wait time and meet this mandate. The AWT system will not require any interaction between the TSA screening force and passengers. It will interact with personal devices carried by passengers by measuring the flow of certain electronic devices as they move through the queue and checkpoint to seamlessly calculate wait time. Such systems are used in several airports in the United Kingdom and Europe, and at the border with Canada to measure wait times for vehicle traffic.

[1] Bluetooth® is a registered trademark of Bluetooth SIG, Inc.

Benefits of an AWT system include: effective management of the screening workforce by allowing them to focus on their core mission; obtaining information to optimize checkpoints to reduce congestion and meet statutory mandates; the potential to segment checkpoints to determine whether different configurations are more efficient; and displaying wait times to assist travelers in their interactions with the checkpoint queue.

This PIA provides information on TSA plans for AWT and assesses the privacy impact associated with those plans. AWT relies on detecting signals broadcast to the public by individual devices and calculating a wait time as the signal passes sensors positioned to cover the area in which passengers may wait in line. Sensors will be placed in or near the checkpoint queuing area, however, airport configurations vary and since queuing areas are not segregated, it is likely that other individuals broadcasting a Bluetooth signal may also be captured by a sensor. The device owner can configure the signal to prevent it from broadcasting to anyone in the area, so individuals seeking to opt out of the TSA AWT may do so by placing their device in a non-discoverable or hidden mode (which allows basic functionality of the device to remain), or by turning it off in the queuing area. Further, while the signal being publicly broadcast is already anonymous to TSA, TSA ensures anonymity by applying a one-way hash at the sensor to convert the signal upon receipt so that TSA cannot reverse the conversion. The sensor does not retain the original MAC address. The hashed address will be retained for two hours in order to identify and eliminate signals that may inaccurately impact data quality; for example, signals from persons who repeatedly pass the sensors (such as from TSA employees working at the checkpoint) and signals collected by only a single sensor (such as from someone standing near a checkpoint queue, but who does not actually enter the queue to generate a matched start/end hashed signal) would introduce errors to the average wait time. It is unlikely that a security queue would extend to two hours, but a two hour retention allows for that possibility. The retention period of the hashed MAC address is configurable by TSA and is expected to remain set at two hours for data quality purposes.

Bluetooth

Bluetooth is a short-range wireless technology allowing enabled devices to communicate with each other. Each Bluetooth-enabled device is assigned a unique 48-bit Media Access Control (MAC) address by the device manufacturer to allow other devices to recognize and establish communications. Unless disabled, devices continuously broadcast their MAC addresses in order to alert other Bluetooth-enabled devices to their presence. Bluetooth signals from devices not operating in discovery mode or from devices that are turned off cannot be detected.

The most common Bluetooth-enabled devices carried by individuals in the checkpoint environment are wireless headsets, cell phones, and personal entertainment technologies. TSA cannot associate an individual's identity with the MAC address. First, while the MAC address is unique to the device, most manufacturers and vendors do not retain information associating the

MAC address with the individual user.[2] Second, as discussed below, the sensor automatically hashes any MAC address at the sensor in a manner that precludes TSA from reversing the conversion of the address. Further, TSA deletes the hashed signal at two hours and only retains statistical data to understand the average wait time (e.g., wait time, time of day, location).

AWT System

Each AWT system includes multiple sensors and a local Central Control Server (CCS). Local airport requirements and configurations determine the number and placement of sensors, which focus on the expected queuing area and detect the Bluetooth signals necessary for wait time calculations. The local CCS is a computer that performs the calculations in a TSA-secured facility at each airport location. The AWT sensors will detect Bluetooth signals emanating from devices carried by individuals as they enter and exit data collection zones within the checkpoint queue. Immediately upon detecting a Bluetooth signal, the sensors will convert the MAC address using a one-way hash function and transmit the hashed MAC address and associated timestamp to the CCS. The one-way hash prevents TSA from reversing the conversion of the original MAC address. The original MAC address is not retained by the sensor.

The CCS calculates the difference in timestamps for each hashed MAC address set to determine the wait time (aggregate data) and deletes the hashed address within two hours of receipt. The aggregate wait time data will be used to develop checkpoint staffing and configuration models.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. Section 222 of the Homeland Security Act of 2002, Pub. L. No. 107-296, states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974 and shall assure that technology sustains and does not erode privacy. 6 U.S.C § 142(a)(2)

In response to this obligation, the DHS Privacy Office has developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act, which encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS'

[2] It may be possible that a manufacturer or vendor may retain the MAC address in a way that would be associated with the user if the user registered their product with the manufacturer or vendor. TSA does not have access, and will not seek access, to such information. The MAC address will in any event be hashed at the sensor so that TSA cannot identify, access, or retain the actual MAC address.

mission to preserve, protect, and secure. Given the particular technologies and the scope and nature of their use, TSA used the DHS Privacy Office FIPPS PIA template.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

TSA does not collect PII as part of the AWT. This PIA and information on the TSA website provide information to the public on AWT. Further, notice will be provided at the airport as discussed below.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS' use of PII.

AWT relies on detecting the Bluetooth signal broadcast by Bluetooth-enabled devices, not on the collection of PII. Individuals who do not wish to participate, or have their Bluetooth signal detected, can turn their broadcast function off (so that they can continue to use their device), or turn the entire device off. TSA will post signs to inform individuals in the airport of AWT.

Signage such as the following or substantially similar will be used:

> ***Help us calculate checkpoint wait times.***
>
> *TSA is using Bluetooth technology in this area to calculate wait times. If you do not wish to participate, you can turn off your Bluetooth device or disable the Bluetooth feature. TSA will encrypt Bluetooth addresses and delete all data within two hours. For more information please see the TSA website (www.tsa.gov).*

TSA expects to deploy a monitor to display the calculated wait time for checkpoints at airports where AWT is deployed.

In addition, TSA will provide information concerning its AWT system on the TSA website (www.tsa.gov) and expects to develop a public outreach campaign to inform the public of the AWT program.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII, to include images, and specifically articulate the purpose or purposes for which the PII is intended to be used.

TSA will not collect PII as part of AWT. The AWT system is designed so that it cannot collect PII for the purposes of calculating checkpoint queue wait times or for any other purpose. Automated wait time collection supports TSA's need to allocate and deploy resources to achieve the provisions of the Implementing Recommendations of the 9/11 Commission Act of 2007, which direct TSA "(1) to provide appropriate levels of aviation security; and (2) to accomplish that goal in such a manner that the average aviation security-related delay experienced by airline passengers is reduced to a level of less than 10 minutes." Pub. L. No. 110-53, § 1612(6).

4. Principle of Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The AWT system is designed so that it cannot collect PII. The AWT system is intended to detect the MAC addresses of passengers in the checkpoint queue; however, all discoverable Bluetooth signals in the detection radius of the sensors will also be detected. Sensors will be placed in locations intended to capture the expected ebb and flow of the checkpoint queue, but airport configurations are not standard and checkpoint queues are typically not segregated from other populations that may pass by a sensor while shopping, walking past a checkpoint, or waiting for a passenger.

The sensor hashes the MAC address and sends it to the CCS for the AWT calculation. The MAC address is not retained by the sensor, and the hashed MAC address is retained at the CCS for two hours in order to permit the system to identify and eliminate signals that may inaccurately impact data quality. For example, signals from persons who repeatedly pass the sensors (such as from TSA employees working at the checkpoint) and signals collected by only a single sensor (such as from someone standing near a checkpoint queue, but who does not actually enter the queue to generate a matched start/end hashed signal) would introduce errors to the average wait time, and will be deleted. The retention period of the hashed MAC address is configurable by TSA and is expected to remain set at two hours for data quality purposes. Any privacy risk

associated with the retention period is mitigated by the one-way hash of the MAC address, which at any rate was being publicly broadcast by the individual when picked up by the sensor.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

The AWT system is designed to calculate checkpoint queue average wait times. AWT data are not used for any other purpose than as discussed in this PIA. Average wait time calculations will be shared for statistical purposes, and checkpoint staffing and configuration. Individual MAC addresses are not retained and therefore cannot be used for any purpose other than conversion by one-way hash, and the hashed address is only used to calculate wait time. The MAC address does not identify the individual, and is further obfuscated by being immediately hashed such that TSA cannot identify the original MAC address. The hashed address is deleted at two hours.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII, including images, is accurate, relevant, timely, and complete, within the context of each use of the PII.

TSA will not collect PII for the purposes of calculating checkpoint queue wait times or for any other purpose. The AWT system uses only that information which is publicly broadcast by a passenger's Bluetooth-enabled device. Accordingly, it is accurate, timely, and complete, and is directly relevant to wait time calculations. The original MAC address picked up by the sensor is immediately hashed with a one-way encryption at the sensor. The hash function does not affect the accuracy or relevance of the underlying signal. The hashed MAC address is retained for two hours to mitigate data quality or integrity issues that may exist if the system detects a single unmatched signal from a passer-by, or repeated matched signals from an officer working at the checkpoint. The AWT system deletes the unmatched signal, and notes the repeated signal so that it can be deleted from the average wait time calculation. This is an acceptable data quality risk.

7. Principle of Security

Principle: DHS should protect PII, including images, through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

AWT does not collect PII. MAC addresses are converted using a 256-bit one-way hash at the sensor before they are transmitted to the CCS, and are not retained by the sensor. The hashed MAC

addresses are transmitted between the sensors and the CCS by a secure wireless connection. The CCS deletes the converted MAC address within two hours. Thereafter, only statistical wait time information will be retained, which further mitigates data security and individual privacy issues. Statistical wait times will be displayed on the monitors at checkpoints or elsewhere to assist passengers. In addition, the AWT sensors and CCS will be secured in a manner consistent with National Institute of Science and Technology (NIST) standards.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, including images, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

TSA staff responsible for operating the AWT technology and program undergo privacy and Privacy Act training developed by the DHS Privacy Office. Supervisors will ensure that policies and procedures are fully enforced. In addition to administrative controls imposed by the operating protocols, technical controls also enforce accountability.

Conclusion

AWT technology has the potential to significantly improve TSA's collection of queue wait time data, providing critical information for management of the checkpoint and assistance to the public. The operating protocols of data encryption and limited retention timeframes are strong privacy protections that permit operational objectives to be achieved. TSA will update this PIA as needed if there are changes in the technologies or operational protocols for AWT.

Responsible Officials

Eric Chin
Planning Branch Manager, Office of Security Operations
Transportation Security Administration
eric.chin@dhs.gov

Approval Signature

/Original signed copy on file with DHS Privacy Office/

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security