Privacy Impact Assessment

for the

CBP Commercial Telemetry Data Evaluation

DHS Reference No. DHS/CBP/PIA-080

August 12, 2024

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is conducting this Privacy Impact Assessment (PIA) to describe its evaluation of commercially available location data associated with mobile smart devices ("commercial telemetry data") for a period between December 2018 and September 2023. During this time, a small number of users in CBP queried smart device location data owned and maintained by commercial vendors to assess the limited use of commercial telemetry data in support of its border security mission. DHS is conducting this Privacy Impact Assessment to provide public notice about the short-term collection of commercial telemetry data.

CBP no longer collects commercial telemetry data owned and maintained by commercial vendors, though it continues to use the commercial telemetry data retained from its past use of vendors. This Privacy Impact Assessment examines the privacy risks and mitigation measures associated with CBP's collection and use of commercial telemetry data during the evaluation period and describes the ways in which CBP ensured its access and use of this information sustained and did not erode individual privacy protections. It also assesses any potential privacy risks related to CBP's continued use of commercial telemetry data retained from the now-ended engagement with commercial vendors. Should CBP begin using these services in the future, a new Privacy Impact Assessment will be published prior to the collection of such data.

Introduction

CBP's mission is to prevent the entry of terrorists, disrupt the flow of illicit narcotics, secure the borders of the United States, and enforce customs, immigration, and other U.S. laws at the border. Among other things, CBP is responsible for developing and implementing targeting capabilities to identify travelers and cargo which may need additional scrutiny.[1] During the period of December 2018 through September 19, 2023, CBP procured access to various commercial databases that included geolocation data associated with mobile smart devices' Advertising Identifiers (AdIDs).[2] This type of information is generally referred to as "commercial telemetry data (CTD)." Consistent with its law enforcement and national security authorities, CBP accessed commercial telemetry data to support its targeting, vetting, analysis, and illicit network discovery processes.

CBP did not, and does not, acquire or ingest bulk cell phone geolocation information. Consistent with the DHS Fair Information Practice Principles,[3] CBP developed access controls

[1] 6 U.S.C. § 211.
[2] AdIDs are unique user IDs assigned to a mobile device (e.g., smart phone, tablet, computer), or operating environment, to help advertising services personalize their advertisements.
[3] *See* DHS PRIVACY POLICY MEMORANDUM, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (December 29, 2008), *available at*

and user Rules of Behavior to ensure that a small number of approved CBP users accessed the minimum amount of information necessary to conduct law enforcement and national security queries of this commercially-owned data in furtherance of CBP mission sets. CBP conducted targeted queries of commercial telemetry data platforms *only* based on active law enforcement or national security investigations or inquiries. Additionally, on a case-by-case basis, CBP conducted searches in the commercial platforms on behalf of federal and local law enforcement agencies and pursuant to CBP authorities.

CBP's testing and evaluation of access to this data was limited to targeted queries focused on: cross-border criminal activity, activity with an identified terrorist/criminal predicate, protection of CBP personnel and facilities from criminal and terror threats, and/or internal investigation of CBP personnel and contractors. This includes determining what devices were present at locations of interest based on active law enforcement investigations and information.

Understanding that even limited access to this information may raise significant privacy and civil liberties questions, CBP conducted its commercial telemetry data evaluation only within parameters established by CBP policy, developed in consultation with the CBP Office of Chief Counsel and CBP Privacy and Diversity Office. All CBP employees that queried commercial telemetry data were required to review and sign the commercial telemetry data Rules of Behavior (see Appendix A). The Rules of Behavior required all employees that requested access to commercial telemetry data acknowledge strict privacy controls over the access and use of this information. All CBP users granted access to commercial telemetry data required written approval from a supervisor at the GS-13 level or above prior to access to this information, and all access was required to be reviewed every 180 days, prior to any decision to renew.

Beginning in 2020, when access to commercial telemetry data expanded beyond a handful of employees who had been granted an opportunity to test the technology, all CBP users granted access to commercial telemetry data were required to have previously taken CBP training on the use of open-source information, and the employees must have displayed responsible use of open-source information in furtherance of CBP's law enforcement mission. The next phase of approval required the employees to obtain a supervisor signature, and acknowledge and sign the commercial telemetry data Rules of Behavior (see Appendix A) which included the following provisions:

Privacy and Compliance Protection:

- I understand that I have no expectation of privacy while using the system.
- I understand that I am accountable for my actions through automatic system audit logs that record all actions taken while accessing and using the system.

https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.

- I understand that AdID CTD will only be used for the purpose of identifying information relevant to investigating or identifying a criminal violation of a law enforced or administered by CBP and/or a national security concern.
- I understand that AdID CTD may be correlated against public records, open-source data, and/or CBP holdings to identify a specific individual only if there is a reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern.
- I understand that AdID CTD may be used to conduct research on a specific device associated with an individual whose identity is known only if there is reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern.
- I understand that a device-specific query of AdID CTD for a time period greater than 14 days may be conducted only if there is reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern.
- I will protect any personally identifiable information (PII) derived from/or enhanced by, the commercial data research, in accordance with applicable law, including the Privacy Act (where applicable), and CBP and DHS privacy policy.
- I will only collect and use the minimum amount of PII necessary for the defined mission related and official use capacity.
- I will protect sensitive information from disclosure to unauthorized persons or groups.
- I will not retain information describing how a U.S. citizen or lawful permanent resident exercises his or her First Amendment rights, unless such retention is pertinent to and within the scope of an authorized law enforcement activity, expressly authorized by statute, or expressly authorized by the individual about whom the record is maintained.

Non-Compliance:

- I understand that failure to follow these rules will result in consequences for noncompliance, such as verbal or written warnings, removal of system access, reassignment to other duties, disciplinary action, and/or criminal or civil prosecution.
- I further understand that any non-compliance incident may be escalated to a security violation.

What is an advertising identifier (AdID)? How do commercial vendors obtain AdIDs?

An advertising identifier is a pseudo-anonymous unique, user resettable, identifier assigned to a mobile device that allows advertisers to personalize advertisements. The advertising identifier is assigned to a mobile device by the device's operating system (either Apple for iPhones or Google for Android phones).[4] Mobile application developers and advertisers use the AdID to identify a device, often for the purpose of providing targeted advertisements.

Application developers use unique AdIDs to gather information on a device's consumer activity, including date/time and location information, without connecting to or using any names, phone numbers, emails, or usernames of device users. Application developers may sell that data to third parties such as vendors or advertisers, who use it to present advertisements on the device. Non-advertisement entities also may purchase this information for other business purposes, such as identifying market trends. In addition to traditional marketing and commercial uses, vendors may also sell this information to law enforcement agencies through different platforms.

Depending on the application and user settings, location data is collected either when the device is on or only when the application is in use. Location data is not collected when a device is off or when a user has opted out of having their location data collected. Mobile device users may opt-out of AdID collection. Users of other mobile operating systems may check with their own providers for how to stop or minimize ad tracking. In addition, users can opt out of, or choose not to opt in to, individual mobile applications.

How did CBP access commercial telemetry data?

When a commercial platform makes such information available to buy, CBP may contract with a commercial platform to query (search) the vendor-owned commercial telemetry data.

Commercial telemetry data was only used for the purpose of identifying information relevant to investigating or identifying irregular travel patterns, conducting device trend analysis, identifying correlations between locations of interest, supporting force protection analysis, identifying insider threats, and investigating national security threats posed by suspected terrorists and Transnational Crime Organizations (TCO) with a nexus to the U.S. border. CBP used commercial telemetry data to correlate against public records, open-source data, or CBP holdings to identify a specific individual only when there was reasonable suspicion of a violation of a criminal law enforced or administered by CBP or a national security concern.

CBP did not ingest bulk commercial telemetry data. Initially, a small number of CBP employees had query-based access to the data through commercial platforms. Within this access,

[4] The AdID is an anonymized identifier that is associated with a mobile smart device but not hardcoded to the device like the Unique Device Identifier (UDID). Apple advertising ID is called the "Identifier for Advertisers" (IDFA) while Google refers to advertising ID as "Google Advertising ID" (AAID).

CBP could not access the commercial data providers' full holdings. Any access or collection by CBP of commercial telemetry data was based on individual queries, typically based on: a) known location of criminal activity, or b) an AdID associated with a known device of interest.[5] As confirmed as part of the CBP evaluation, no single commercial telemetry data vendor has comprehensive coverage of all available cell phone geolocation data globally.

How did CBP link an AdID from a mobile device to a person?

Consistent with legal and privacy policy parameters in the commercial telemetry data Rules of Behavior, CBP users queried AdID information to identify irregular travel patterns, conduct device location analysis (for example, does a device visit a known smuggling stash house multiple times), identify correlations between locations of interest, support force protection analysis, identify insider threats, and investigate national security threats posed by suspected terrorists and Transnational Crime Organizations with a nexus to the U.S. border.

CBP users conducted two different types of searches within commercial telemetry platforms:

1. Location-based searches. CBP users conducted location-based queries (geofences) around known locations of law enforcement interest or travel patterns with a reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or national security concern to identify AdIDs of interest.
2. Device-specific searches. CBP conducted device-specific searches when an AdID or device identifier was already known to be associated with an individual only if there was a reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern. CBP may have obtained device-specific AdID information through its digital forensics programs, such as through the analysis of seized or abandoned devices suspected of involvement in illicit activity or through border searches of electronic devices. CBP may also have obtained this information from devices obtained by the CBP Office of Professional Responsibility for internal investigations.

Information made available to CBP through the commercial telemetry vendors included the overall data elements across the different collections:

[5] There are some cases where CBP may use an AdID collected from a device encountered during CBP law enforcement activities to conduct research on the device. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR U.S. BORDER PATROL DIGITAL FORENSICS, DHS/CBP/PIA-053(a), and U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR CBP BORDER SEARCHES OF ELECTRONIC DEVICES, DHS/CBP/PIA-008(a), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

- Location (displayed as dots on the screen);
- Time and date the AdID was collected by the vendor;[6]
- A persistent device identifier (the AdID);
- Metadata associated with the device's operating system (Windows or Apple/MAC for a computer and Android/Apple for mobile devices);
- Browser type (if user settings permit a browser to collect AdID); and
- Resolution of the number of entities at a location (i.e., whether the signal indicates one device traveling in a line, or 100 devices at singular points in a row).

CBP attempted to correlate these data points provided from the commercial vendor using research and analysis against public records, open-source data, and/or CBP holdings[7] to identify a specific individual only if there was a reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern. Additionally, reasonable suspicion and/or a national security requirement must have been met for CBP to conduct a search on an already known AdID or in cases where CBP was searching more than 14 days' worth of data related to a specific AdID (see Appendix A, Rules of Behavior).

CBP only incorporated and maintained AdID information into CBP systems if the results of the search of the commercial vendor platform were relevant to an ongoing investigation or inquiry. CBP stored the relevant AdID results in its Intelligence Research System-Next Generation (IRS-NG)[8] platform, which is a part of the Automated Targeting System (ATS).[9]

IRS-NG uses the same federated search functionality as the Automated Targeting System. This function allows IRS-NG users to search across many different CBP systems to provide a consolidated view of data about a person or an entity. While the Automated Targeting System Privacy Impact Assessment and subsequent updates provide the exhaustive list of records

[6] There was no real nor near real-time tracking of the data available to CBP; data was delayed by 18-24 hours or more.
[7] "CBP holdings" refers to all information collected and maintained by CBP within its various systems. The most common types of records checked during the AdID correlation process were CBP border crossing records, as well as Electronic System for Travel Authorization (ESTA) and Electronic Visa Update System (EVUS) applications. The most comprehensive description of CBP holdings is in the DHS/CBP/PIA-006(e) Automated Targeting System (ATS) Privacy Impact Assessment (January 2017). *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006(e), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[8] The Intelligence Research System-Next Generation platform Privacy Impact Assessment is under development, and will be published at https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[9] See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

commonly referred to as "CBP holdings," below is a general list of data sources that are searchable via IRS-NG if the user has access to and a need to know the underlying source data.

- Official Record: ATS maintains the official record for Passenger Name Records (PNR);[10] Importer Security Filing (10+2 documentation) and express consignment manifest information;[11] results of Cargo Enforcement Exams; Document and Media exploitation (DOMEX);[12] data from the combination of license plate, Department of Motor Vehicle (DMV) registration data, and biographical data associated with a border crossing; certain law enforcement and/or intelligence data, reports, and projects developed by CBP users that may include public source information; and certain information obtained through memoranda of understanding or other arrangements because the information is relevant to the border security mission of the Department.
- Inclusion of Data from other CBP systems: The Automated Targeting System maintains copies of key elements of certain databases to minimize the impact of processing searches on the operational systems and to serve as a backup for certain operational systems, including but not limited to: CBP's Automated Commercial Environment (ACE);[13] Overstay Leads from Arrival and Departure Information System (ADIS);[14] Automated Export System (AES);[15] Advance Passenger Information System (APIS);[16] Border Crossing Information (BCI);[17] Electronic System for Travel Authorization (ESTA);[18] Electronic Visa Update System (EVUS);[19] Global Enrollment

[10] Collected by CBP pursuant to its statutory authority, 49 U.S.C. § 44909, as implemented by 19 CFR 122.49d.
[11] Advance information about cargo and related persons and entities for risk assessment and targeting purposes.
[12] CBP conducts searches of electronic devices consistent with CBP Directive 3340-049A, *Border Search of Electronic Devices*, *available at* https://www.cbp.gov/document/directives/cbp-directive-no-3340-049a-border-search-electronic-devices/.
[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED COMMERCIAL ENVIRONMENT (ACE), DHS/CBP/PIA-003 (2006 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (ADIS), DHS/CBP/PIA-024 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, INTRODUCTION TO THE AUTOMATED EXPORT SYSTEM (AES) (2023), *available at* https://www.cbp.gov/trade/aes/introduction.
[16] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM (APIS), DHS/CBP/PIA-001 (2005 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[17] *See* DHS/CBP-007 Border Crossing Information (BCI), 81 Fed. Reg 89957 (December 13, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION (ESTA), DHS/CBP/PIA-007 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[19] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC VISA UPDATE SYSTEM (EVUS), DHS/CBP/PIA-033 (2016 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

System (GES);[20] I-94 data, Non-Immigrant Information System (NIIS);[21] Seized Asset and Case Tracking System (SEACATS);[22] TECS (not an acronym);[23] data from electronic devices; the Department of Justice's (DOJ) National Crime Information Center (NCIC) and Federal Bureau of Investigation (FBI) Interstate Identification Index (III) hits for manifested travelers;[24] the U.S. Citizenship and Immigration Services' (USCIS) Central Index System (CIS) data received through TECS, and special protected classes[25] data; the U.S. Immigration and Customs Enforcement's (ICE) Student and Exchange Visitor Program (SEVP)[26] and Enforcement Integrated Database (EID),[27] which includes Criminal Arrest Records and Immigration Enforcement Records (CARIER);[28] Electronic Questionnaires for Investigations Processing (e-QIP);[29] historical National Security Entry-Exit Registration System (NSEERS); Flight Schedules and Flight Status OAG data; Social Security Administration (SSA) Death Master File;[30] Terror Screening Data Set (TSDS), which the Automated Targeting System ingests from the Watchlist Service (WLS);[31] Non-immigrant and Immigrant Visa data from Department of State (DOS) Consular

[20] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE GLOBAL ENROLLMENT SYSTEM (GES), DHS/CBP/PIA-002 (2006 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[21] *See* DHS/CBP-016 Nonimmigrant Information System, 80 Fed. Reg 13398 (March 13, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.

[22] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE SEIZED ASSET AND CASE TRACKING SYSTEM (SEACATS), DHS/CBP/PIA-040 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[23] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021 (2016 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[24] *See* U.S. DEPARTMENT OF JUSTICE, PRIVACY IMPACT ASSESSMENT FOR THE NATIONAL CRIME INFORMATION CENTER (NCIC), *available at* https://www.fbi.gov/file-repository/pia-ncic-020723.pdf/view.

[25] Special protected classes of individuals include nonimmigrant status for victims of human trafficking, nonimmigrant status for victims of crimes, and relief for domestic violence victims.

[26] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT AND EXCHANGE VISITOR PROGRAM (SEVP), DHS/ICE/PIA-001 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[27] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2019 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

[28] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 Fed. Reg 72080 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

[29] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, ELECTRONIC QUESTIONNAIRES FOR INVESTIGATIONS PROCESSING (E-QIP), *available at* https://careers.cbp.gov/s/applicant-resources/e-qip.

[30] *See* U.S. SOCIAL SECURITY ADMINISTRATION, SSA DEATH INFORMATION, *available at* https://www.ssa.gov/dataexchange/request_dmf.html.

[31] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006(e), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

Consolidated Database (CCD), Refused Visa data from the Consular Consolidated Database, and the Consular Electronic Application Center (CEAC);[32] and Secure Flight Passenger Data (SFPD) and Master Crew List/Master Non-Crew List data from the Transportation Security Administration (TSA).[33]

- Pointer System: The Automated Targeting System accesses and uses additional databases without ingesting the data, including: CBP's Arrival and Departure Information System (ADIS);[34] U.S. Border Patrol's Enforcement Tracking System (BPETS);[35] Enterprise Geospatial Information Services (eGIS);[36] e3 Biometrics System;[37] U.S. and Non-U.S. Passport Service through TECS; Department of State Consular Consolidated Database; commercial data aggregators (such as LexisNexis); ICE's Enforcement Integrated Database (EID); DHS Automated Biometric Identification System (IDENT);[38] National Law Enforcement Telecommunications System (NLETS), Department of Justice's National Crime Information Center and the results of queries in the FBI's Interstate Identification Index; Interpol; the National Insurance Crime Bureau's (NICB) private database of stolen vehicles; and United States Citizenship and Immigration Services' (USCIS) Person Centric Query System (PCQS).[39]

---

[32] *See* U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE CONSULAR ELECTRONIC APPLICATION CENTER (CEAC) (2021 and subsequent updates), *available at* https://www.state.gov/wp-content/uploads/2021/06/Consular-Electronic-Application-Center-CEAC-PIA.pdf.

[33] *See* U.S. TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE SECURE FLIGHT PROGRAM, DHS/TSA/PIA-018 (2007 and subsequent updates), *available* at https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[34] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (ADIS), DHS/CBP/PIA-024 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[35] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, U.S. BORDER PATROL, PRIVACY IMPACT ASSESSMENT FOR THE BORDER PATROL ENFORCEMENT TRACKING SYSTEM (BPETS/BPETS2), DHS/CBP/PIA-046 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[36] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR ENTERPRISE GEOSPATIAL INFORMATION SERVICES, DHS/CBP/PIA-041 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[37] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR CBP PORTAL (E3) TO ENFORCE/IDENT, DHS/CBP/PIA-012 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[38] DHS is retiring IDENT and replacing it with the Homeland Advanced Recognition Technology System (HART). *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001, AND THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM, DHS/OBIM/PIA-004, *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[39] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC QUERY SERVICE, DHS/USCIS/PIA-010 (2016 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

- Data Manually Processed: The Automated Targeting System is used to manually process certain datasets to identify national security and public safety concerns and correlate records. Currently, DHS conducts this process for those records in the Arrival and Departure Information System that pertain to individuals who may have overstayed their permitted time in the United States.

CBP analysts stored AdID information in an IRS-NG "Workspace" which allowed them to conduct research and analysis against the "CBP holdings" listed above. All AdID information collected as part of this evaluation was retained consistent with the CBP Intelligence Records System (CIRS) System of Records Notice[40] and IRS-NG retention policies and, therefore, may still be in use by CBP.

Legal and Privacy Protections

Collection of information that may identify an individual's location or "pattern of life" when aggregated with other data points raises significant legal and privacy issues.

The Privacy Act expressly prohibits the agency collection of records describing how an individual (defined in the Act as a U.S. citizen or lawful permanent resident) exercises rights guaranteed by the First Amendment. There are exceptions, however, if the record is "pertinent to and within the scope of an authorized law enforcement activity," or if either a statute or the individual about whom the record is maintained expressly authorizes such maintenance.[41] CBP personnel receive training on how to identify First Amendment activity and determine if information involves protected activities, as well as when it is appropriate for CBP personnel to conduct research.

In addition, all CBP users were prohibited from retaining information describing how a U.S. citizen or lawful permanent resident exercises First Amendment rights, unless such retention was pertinent to and within the scope of an authorized law enforcement activity, expressly authorized by statute, or expressly authorized by the individual about whom the record is maintained.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[42] 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. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure

[40] *See* DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 85 Fed. Reg. 80806 (December 14, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[41] 5 U.S.C. § 552a(e)(7).
[42] 5 U.S.C. § 552a.

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[43]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[44] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure the homeland.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[45] and the Homeland Security Act of 2002, Section 222.[46] Given that CBP's use of AdID location data is a program rather than a particular information technology system, this Privacy Impact Assessment is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This Privacy Impact Assessment examines the privacy impact of CBP's evaluation of its access to commercial telemetry data, and continued use of data retained from the evaluation, as it relates to the Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of 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.

CBP is publishing this Privacy Impact Assessment to provide notice to the public about CBP's evaluation of commercial platforms to query AdID device location data and provide transparency to the public regarding how CBP collected, used, stored, and retained commercially available geolocation data. In addition, CBP has previously published relevant System of Records Notices (SORN) that provide public notice that CBP collects information from commercial data providers. Specifically, DHS/CBP-024 CBP Intelligence Record System[47] provides notice for CBP collection of location information from public source data as well as commercial data providers.

---

[43] 6 U.S.C. § 142(a)(2).
[44] *See* PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, "THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY," *available at* https://www.dhs.gov/privacy-policy-guidance.
[45] 44 U.S.C. § 3501 note.
[46] 6 U.S.C. § 142.
[47] *See* DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 85 Fed. Reg. 80806 (December 14, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns. This system of records notice provides notice of CBP's collection and maintenance of "records and information from government data systems or retrieved from commercial data providers in the course of intelligence research, analysis, and reporting, including records of property ownership."

Privacy Risk: There was a risk that individuals did not know that their AdID location data was accessible to CBP via a commercially available information database.

Mitigation: This risk was not mitigated. While CBP is now publishing this Privacy Impact Assessment to provide the public with general notice of this completed project, CBP could not provide direct notice to individuals that their information may become part of CBP's holdings via query of a commercial provider's data.

It was CBP's understanding that the terms of service under which the data was collected disclosed that the data may be sold to a customer base that included public sector customers, and the user must accept the terms of service prior to using/accessing the service or product. Additionally, CBP limited access to this information for the purpose of identifying information relevant to investigating or identifying irregular travel patterns, conducting device trend analysis, identifying correlations between locations of interest, supporting force protection analysis, identifying insider threats, and investigating national security threats posed by suspected terrorists and Transnational Crime Organizations with a nexus to the U.S. border, and did not retain any information unassociated with a law enforcement event.

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's use of PII.

As a part of this commercial telemetry data evaluation, CBP only contracted with commercial platforms that, as a matter of practice through their business contracts to purchase AdID information, only received AdID information from mobile applications that had a privacy policy that disclosed that user location information may be sold or shared with third parties. Additionally, users must have consented to these polices before they could use the mobile application. Finally, users were generally required to opt in to allowing the application to track their location for the application to collect location information.

CBP contracted with commercial vendors that buy and re-sell AdID location information to private and public sector organizations. CBP paid to use a vendor's service to access the vendor-owned platform to access and search AdID location information.

Once a mobile application user acknowledged the terms of service, and (depending on the device) opted in to allowing the application access to location information, it is CBP's understanding that the mobile application would then have access to both the AdID and the device's GPS information.

Individuals could choose not to share their location information with the respective mobile applications. In which case, CBP would not have been able to see that information. Individuals

could also have reset their AdID which, in some cases would have set their AdID to a string of zeros; therefore, the commercial platforms would not display that information to CBP. On some devices, resetting the AdID would create a new unique string of numbers. This made it more difficult for CBP to associate a device across time.

Privacy Risk: There was a risk that individuals did not know how to opt out of their mobile applications from sharing location information with the application and, ultimately, with CBP.

Mitigation: This risk was partially mitigated. As noted, CBP only contracted with platforms that received data from data providers that verified that the information they provided was gathered from individuals who consented to having their location information sold and used by third parties.

However, a risk remained that: a) individuals may not have realized that commercial vendors collect and sell this kind of sensitive tracking information, and b) individuals may not have known how to opt out of this collection. Accordingly, this risk could not be fully mitigated.

Privacy Risk: There is a risk that individuals are unable to access, correct, or amend AdID location data obtained by a commercial provider and retained in a CBP law enforcement system.

Mitigation: This risk is partially mitigated. As noted previously, CBP retained information if it was related to a CBP mission. Once in a CBP law enforcement system, allowing a subject of law enforcement scrutiny to access their information could significantly interfere with and undermine CBP's law enforcement capabilities and authorities for conducting its border security mission. For this reason, relevant CBP systems are exempt under the Privacy Act[48] from providing access, correction, and amendment of records in a law enforcement system. However, CBP evaluates all requests for correction and amendment of records, even in a law enforcement system of records, on a case-by-case basis. Since the results of the queries of the commercial telemetry data retained by CBP were included in law enforcement records associated with law enforcement and border security activities, CBP is exempt from making these records available but will nonetheless process requests for such records on a case-by-case basis.

3. Principle of Purpose Specification

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

CBP's law enforcement and border security responsibilities are set forth in numerous statutes and regulations, including but not limited to the Homeland Security Act of 2002, as amended, codified at 6 U.S.C. § 101, et seq.; the Immigration and Nationality Act, as amended, codified at 8 U.S.C. § 1101, et seq.; and the Tariff Act of 1930, as amended, codified at 19 U.S.C.

[48] For a comprehensive list of all systems that are exempt from certain provisions of the Privacy Act, please *see* Appendix C to Part 5, Title 6 CFR, *available at* https://www.ecfr.gov/current/title-6/chapter-I/part-5.

§ 1202, et seq. CBP is also authorized to investigate misconduct by CBP employees and has certain responsibilities relating to the security of CBP facilities, personnel, and information. See, e.g., 6 U.S.C. § 211(j); 29 U.S.C. § 654(a)(1); 44 U.S.C., Chapter 35, Subchapter II (Information Security); and 41 C.F.R. Part 102-74 (Facility Management).

Consistent with these authorities, CBP queried commercial platforms to access AdID location information for the purpose of identifying information relevant to investigating or identifying irregular travel patterns, conducting device trend analysis, identifying correlations between locations of interest, supporting force protection analysis, identifying insider threats, and investigating national security threats posed by suspected terrorists and Transnational Crime Organizations with a nexus to the U.S. border. CBP retained AdID location data linked to cross-border criminal activity, activity with an identified terrorist/criminal predicate, information relevant to the security of CBP personnel and facilities from criminal and terror threats, and/or internal investigation of CBP personnel and contractors. CBP retained responsive commercial telemetry data consistent with the internal Rules of Behavior that limited uses to only those described above.

Privacy Risk: There was a risk that CBP users may access AdID location data for an unauthorized purpose inconsistent with the Rules of Behavior liming access for certain purposes.

Mitigation: This risk was mitigated. To assist in securing AdID location data against unauthorized access or use, CBP limited the number of individuals who could access the data via the commercial provider. CBP ensured only those who had a specific need to access this information in the performance of their duties, and had supervisor and program management approval, could query the data through a data provider's secure web-based portal. If the query returned information that was relevant to an enforcement activity and consistent with the Rules of Behavior, CBP users could add the AdID information to a record maintained in the IRS-NG system.

The commercial data providers maintained a log of all CBP queries. The query logs were available for review upon request by CBP if a question arose about whether AdID location data was accessed for unauthorized purposes. Anomalies in the audit trail that revealed inappropriate activity were referred to the appropriate DHS or CBP integrity office for further action. The commercial data providers that made the AdID location data available to CBP employed data security technologies comparable to those required of CBP systems to protect the integrity of data from hacking and other risks.

Privacy Risk: There is a risk that CBP could use AdID information collected and maintained in a CBP system for a purpose inconsistent with the original authority for collection.

Mitigation: This risk is mitigated. All users that were granted access to AdID information as part of the commercial telemetry evaluation were required to sign Rules of Behavior that limited

the collection of this information for a specific purpose. Once a CBP user signed the Rules of Behavior, and obtained supervisory approval, users conducted queries consistent with the established parameters. Consistent with legal and privacy policy parameters, CBP used AdID information to identify irregular travel patterns, conduct device trend analysis, identify correlations between locations of interest, support force protection analysis, identify insider threats, and investigate national security threats posed by suspected terrorists and Transnational Crime Organizations with a nexus to the U.S. border.

For AdID information that met the criteria for maintenance within the IRS-NG system, only users with access to that assigned Workspace or intelligence research project may access the AdID. Identifiable AdIDs were not incorporated into larger CBP holdings, nor were/are they made available for the majority of CBP system users to access. In some cases, CBP may have also used vendor-generated maps that may have relied on AdID to map migration routes outside of the United States, but CBP did not collect or maintain AdID in those cases. In limited cases where partner government agencies requested AdID information about specific subjects of law enforcement or national security interest, any information was disclosed consistent with the Routine Uses published in DHS/CBP-024 Intelligence Records System and the CBP Directive for the Domestic Sharing of CBP Information for Law Enforcement and Security Purposes.[49]

4. Principle of Data 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).

Uses of the Information

CBP's evaluation of commercial telemetry data was limited to cross-border criminal activity, activity with an identified terrorist/criminal predicate, security of CBP personnel and facilities from criminal and terror threats, and/or internal investigation of CBP personnel and contractors. CBP accessed this commercially available information through commercial platforms and did not retain information during the evaluation period unless for the purpose of identifying information relevant to investigating or identifying irregular travel patterns, conducting device trend analysis, identifying correlations between locations of interest, supporting force protection analysis, identifying insider threats, and investigating national security threats posed by suspected terrorists and Transnational Crime Organizations with a nexus to the U.S. border. In addition, CBP conducted searches on behalf of federal and local law enforcement agencies in the commercial platforms only on a case-by-case basis, pursuant to CBP authorities.

[49] CBP DIRECTIVE NO. 4320-033, Domestic Sharing of CBP Information for Law Enforcement and Security Purposes (May 24, 2021). On file with the DHS and CBP privacy offices.

CBP only queried AdID location data in commercial platforms to support investigative and law enforcement activities consistent with CBP statutory authorities, federal law, and DHS policy. CBP was limited to only viewing AdIDs, the GPS coordinates associated with those AdIDs, the date and time of AdID collection, and limited metadata related to the device's operating system. Additionally, to view an extended timeline of AdID location information, CBP personnel were required to have reasonable suspicion of a violation of criminal law enforced or administered by CBP. CBP personnel would only incorporate into and maintain AdID location information in CBP records if the results of the search were relevant to an ongoing investigation. In those cases, CBP primarily maintained the information in its IRS-NG platform.

Data Retention by the Project

AdID location data collected as part of the evaluation was retained in accordance with the applicable retention policies. Users input relevant information and analysis into CBP's IRS-NG or other appropriate CBP system if the information was determined to be useful in connection with CBP's legitimate law enforcement or border security mission. CBP also input relevant information into IRS-NG to track cases and results of research and analysis, as appropriate. Commercially available AdID location data obtained from data providers' platforms was only incorporated into CBP records if relevant to the law enforcement purpose for which the user accessed the AdID location data. CBP personnel did not maintain records that describe how a U.S. citizen or lawful permanent resident exercises First Amendment rights unless such retention was pertinent to and within the scope of an authorized law enforcement activity, expressly authorized by statute, or expressly authorized by the individual about whom the record was maintained.

CBP will retain this data for 20 years, which is consistent with the retention schedule as specified in the relevant System of Records Notice.[50] The purpose of retention limits is to allow CBP users seeking to conduct additional analysis and research regarding border security or law enforcement matters access to sufficient historical data to identify trends, patterns, and potentially viable information or leads, while not retaining data for so long as to result in the unnecessary or excessive acquisition of information. CBP did not and will not continue to retain in its records the results of its queries of AdID location data unless the information is determined to be useful in connection with its legitimate law enforcement or border security mission. These limitations and requirements will help to ensure access to and retention of AdID location data are compatible with the purpose for which the data was originally collected and to minimize the risk of over-collection of this data.

Privacy Risk: There was a risk of over-collection if CBP collected commercial telemetry data about individuals who were not under suspicion or subjects of investigation.

[50] *See* DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 85 Fed. Reg. 80806 (December 14, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

Mitigation: This risk was partially mitigated. While the commercial telemetry data procured by CBP was available for purchase by anyone, CBP imposed its own data minimization controls by policy. CBP imposed strict limitations on collection and use of this data through the Rules of Behavior. CBP only queried commercial telemetry data for the purpose of identifying irregular travel patterns, conducting device trend analysis, identifying correlations between locations of interest, supporting force protection analysis, identifying insider threats, and investigating national security threats posed by suspected terrorists and Transnational Crime Organizations with a nexus to the U.S. border. CBP users only conducted device-specific research and/or correlated commercial telemetry data with other CBP information if there was reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern.

CBP used commercial platforms to conduct location-based searches around areas of interest in furtherance of CBP's mission sets to identify devices in those areas. CBP was then able to follow device locations to determine travel patterns or, with reasonable suspicion of a crime or national security concern, attempt to identify the owner of the device. For example, CBP conducted location-based queries to identify devices located at known stash houses or devices that transited the border between ports of entry.

In addition, while the commercial vendor platforms displayed all device information emitting from a location of interest, including mobile devices, gaming consoles, smart appliances, and vehicles, CBP was only authorized to access, collect, use, and retain AdID information related to its mission.

Privacy Risk: There was a risk that CBP's collection of commercial telemetry data may have constituted an over-collection of sensitive information.

Mitigation: This risk was partially mitigated. Access to commercial telemetry data gave CBP the ability to drop a "geofence" around certain locations of law enforcement or national security interest. Of course, not every AdID included in response to a location-based CBP query on a commercial platform was connected to a law enforcement or national security interest. Consistent with the Rules of Behavior, all device-specific queries of AdID commercial telemetry data for a time period greater than 14 days could be conducted only if there was reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern.

CBP used commercial telemetry data to correlate against public records, open-source data, or CBP holdings to identify a specific individual only when there was reasonable suspicion of a violation of a criminal law enforced or administered by CBP or a national security concern. When CBP submitted a location-based query to a vendor platform, the information made available to CBP was not linked to, nor did it provide any biographic information on, the device owner, such

as device owner's name, phone number(s), social security number, email address(es), social media, and/or application usernames.

Additionally, CBP closely adhered to DHS policy prohibiting the consideration of race or ethnicity in investigation, screening, and law enforcement activities in all but the most exceptional instances. Accordingly, consistent with law and DHS policy, commercial telemetry data could not and may not be collected, accessed, used, or retained to target or monitor an individual solely on the basis of actual or perceived race or ethnicity.[51]

Privacy Risk: There was a risk that CBP improperly collected information protected by the First Amendment of the U.S. Constitution.

Mitigation: This risk was mitigated. All CBP users were prohibited from retaining information describing how a U.S. citizen or lawful permanent resident exercises First Amendment rights, unless such retention was pertinent to and within the scope of an authorized law enforcement activity, otherwise expressly authorized by statute, or expressly authorized by the individual about whom the record is maintained.

Prior to collecting AdID location data, CBP employees determined whether the information was protected by the First Amendment of the U.S. Constitution, and whether the collection of data was permissible under the Privacy Act, as applicable. CBP personnel received training to distinguish between First Amendment protected activities and credible threats.

In addition, the Privacy Act expressly prohibits the agency collection of records describing how an individual (defined in the Act as a U.S. citizen or lawful permanent resident) exercises rights guaranteed by the First Amendment. There are exceptions, however, if the record is "pertinent to and within the scope of an authorized law enforcement activity," or if either a statute or the individual about whom the record is maintained expressly authorizes such maintenance.[52] CBP personnel received training from the Office of Chief Counsel and the CBP Privacy and Diversity Office on how to identify First Amendment activity and determine if information involved protected activities, such as protests, or if the information constituted credible threats for which CBP personnel could take action.

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.

Once a CBP user gained access to a commercial AdID platform they could begin to conduct queries in furtherance of CBP mission sets only consistent with the parameters in the Rules of

[51] *See* CBP Policy on Nondiscrimination in Law Enforcement Activities and all other Administered Programs, *available at* www.cbp.gov.
[52] 5 U.S.C. § 552a(e)(7).

Behavior. Consistent with legal and privacy policy parameters, CBP used AdID information to identify irregular travel patterns, conduct device trend analysis, identify correlations between locations of interest, support force protection analysis, identify insider threats, and investigate national security threats posed by suspected terrorists and Transnational Crime Organizations with a nexus to the U.S. border.

CBP may have correlated location information gained from research and analysis of AdID location data against public records, open-source data, and/or CBP holdings to identify a specific individual only if there was reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern. Additionally, reasonable suspicion and/or national security requirements must have been met for CBP to conduct a search on an already known AdID or in cases where CBP was searching more than 14 days' worth of data related to a specific AdID (see Appendix A, Rules of Behavior).

Once approved for access to commercial telemetry data platforms, CBP users conducted location-based queries (geofences) and queries of known AdIDs within the platform. All queries were captured by the platforms and were available for audit by CBP program managers. The platform vendors were only permitted access to CBP query logs when CBP requested maintenance or access to additional audit records. During the evaluation, platform vendors were limited to providing CBP with up to three years of historical data related to an AdID. The commercial platforms accessed by CBP removed AdID data from display on a rolling three-year basis.

CBP used the limited AdID location data it collected under this evaluation to support its law enforcement, national security, and border security missions, to include limited, case-by-case assistance to other DHS and domestic law enforcement partners when supported by CBP authorities. CBP maintains and uses AdID location data linked to cross-border criminal activity, activity with an identified terrorist/criminal predicate, security of CBP personnel and facilities from criminal and terror threats, and/or internal investigation of CBP personnel and contractors. CBP may share information with domestic law enforcement partners when that information is necessary for furthering an existing investigation.

If a domestic law enforcement partner requested CBP to conduct research using AdID location information, CBP analyzed whether there was a border nexus or other authority that allowed CBP to conduct a query. CBP did not rely on the authority of other agencies to conduct searches, and all searches were required to abide by CBP's Rules of Behavior.

Privacy Risk: There is a risk that any personally identifiable information collected by CBP through the evaluation will be retained by CBP for longer than necessary.

Mitigation: This risk is mitigated. AdID location information is stored as part of analyst Workspaces in IRS-NG, with access limited to only those granted access by the Workspace owner.

IRS-NG Workspace records are maintained consistent with the DHS NI-563-07-016 records schedule of the DHS Office of Intelligence and Analysis for Raw Reporting Files.

Additionally, CBP will retain raw, unevaluated information on threat reporting originating from operational data and supporting documentation that is not covered by another existing DHS system of records for thirty (30) years, pursuant to the System of Records Notice for the CBP Intelligence Reporting System.[53] CBP will retain finished intelligence and associated background material for products identifying imminent homeland security threats, assessments providing intelligence analysis on specific topics, intelligence reporting to senior leadership, intelligence summaries about current intelligence events, and periodic reports containing intelligence awareness information for specific region, sector, or subject/area of interest as permanent records and will transfer the records to the National Archives and Records Administration (NARA) after twenty (20) years.

Privacy Risk: There was a risk that CBP inappropriately accessed AdIDs via a commercial telemetry vendor on behalf of a partner government agency.

Mitigation: This risk was mitigated. In limited circumstances, CBP assisted other domestic law enforcement agencies with cross-border criminal investigations during the evaluation. Following a request from a partner law enforcement agency, CBP assisted only in cases with a clear border security nexus. CBP relied on its own authorities to conduct queries, and all domestic requests involved criminal, cross-border investigations.

6. Principle of Data Quality and Integrity

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

Commercial telemetry data has inherent data quality issues. For example, devices may be used by multiple individuals, or a "burner" device may be used a few times and discarded, making it difficult to accurately link to an individual. In addition, multiple individuals may reside at the same location, possibly hundreds or thousands of individuals if the residence is a multi-family dwelling unit like an apartment building.

CBP only contracted with commercial platforms that developed methods to identify and correct inaccurate data; however, challenges like the ones noted above cannot be fully mitigated. As a law enforcement agency, CBP often encounters data of uncertain reliability or which requires additional research to determine its relevance and/or credibility. CBP compared information accessed through a commercial telemetry vendor against other open-source information, as well as other public and government sources, to assess accuracy and reliability of the data. CBP did not

[53] *See* DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 85 Fed. Reg. 80806 (December 14, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.

make operational or enforcement decisions based solely on AdID information during the evaluation.

Privacy Risk: There is a risk that the data maintained by the commercial telemetry vendors and then accessed, retained, and used by CBP is inaccurate, untimely, or incomplete.

Mitigation: This risk is partially mitigated. While CBP cannot control the accuracy, quality, or integrity of the data maintained by the commercial vendors with which it contracted, as noted previously, CBP then required and still requires users of the data to independently assess its accuracy, timeliness, and reliability prior to any collection, retention, or use. Additionally, CBP did not and does not make operational or enforcement decisions based solely on AdID information accessed and retained during the evaluation. Further, CBP only contracted with vendors that it understood to uphold the terms of service under which the data was collected, which disclosed that the data may be sold to a customer base that included public sector customers, and for which the user must accept the terms of service prior to using/accessing the service or product.

Privacy Risk: There was a risk and there remains a risk that AdID location data may be inaccurately linked to individuals.

Mitigation: This risk is partially mitigated. CBP partially mitigates this risk by reviewing information from multiple other data type sources, such as open-source reporting, as well as other public and government sources to corroborate the information. Additionally, CBP authorized users with access to AdID location data participated in extensive training to help them analyze information responsive to database queries. Finally, users were not and are not permitted to make operational and enforcement decisions based solely on AdID location data.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

While the commercial data providers provided their own data security controls, CBP vendors were required to comply with all CBP data security requirements. Additionally, CBP limited access to AdID location data to authorized CBP users who completed training, had a need to access AdID location data for their work, reviewed guidelines, agreed to specific Rules of Behavior, and were approved to use it by a supervisor. Only information deemed relevant to CBP's border security mission or law enforcement activity was retained in CBP systems.

Further, AdID location data is maintained in an access controlled and auditable system. Authorized CBP users are granted access on a "need to know" basis.

Privacy Risk: There is a risk that an unauthorized individual without a legitimate need to know may access AdID location data now maintained in CBP systems.

Mitigation: This risk is mitigated. Only a limited number of authorized CBP personnel, with a need to know, had access to AdID location data collected and maintained by CBP as part of this initiative. The location information was and is stored as part of analyst Workspaces in IRS-NG, with access limited to only those granted access by the Workspace owner. In addition, CBP employees must pass a full background investigation and be trained regarding the access, use, maintenance, and dissemination of AdID location data before being given access to the system maintaining the information. Employees must have an official need to know to access the information. This need to know is confirmed by requiring supervisory approval before CBP employees or contractors may access AdID location data and before information is shared outside of CBP.

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, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The commercial platform providers maintained audit trails which were made available to appropriate CBP personnel for review as necessary. All retained AdID information was stored in a CBP system of record, with audit logs at the individual authorized-user level. All audit logs were and remain subject to review at any time by CBP oversight offices and system managers as appropriate. CBP audit logs captured: 1) the identity of the user initiating the query; 2) the AdID location data queried; and 3) the date and time of the inquiry. This data was also captured, thereby enhancing the usefulness of the audit trail data. The primary goal of maintaining audit logs is to deter and discover any abuse or misuse of AdID location data. Any abuse or misuse of AdID location data will be reported and subject to disciplinary action, as appropriate.

Before being granted access to AdID location data, authorized CBP users completed training regarding relevant policy requirements and associated privacy, civil rights, and civil liberties safeguards. This supplemented existing mandatory training required of all CBP personnel on data security, data privacy, integrity awareness, and records management. Authorized CBP users were limited in number on a need to know basis and authorized by appropriate CBP management. Authorized CBP users also reviewed and acknowledged strict guidelines and Rules of Behavior.

Privacy Risk: There was a risk that AdID location data may be accessed routinely (even when not needed) without appropriate controls and oversight through the vendors' platforms and now through CBP systems.

Mitigation: This risk is partially mitigated. As discussed, CBP implemented internal policies and training emphasizing the requirement to query and use AdID location data only when in support of a law enforcement or border security purpose. Audit trails captured sufficient usage

data to allow the identification of CBP users who did not comply with these policies who then faced appropriate ramifications.

Contact Official

Executive Director
National Targeting Center

Responsible Official

Debra Danisek
Privacy Officer
Office of the Commissioner
U.S. Customs and Border Protection
Privacy.cbp@cbp.dhs.gov

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
Privacy@hq.dhs.gov

Appendix A

CBP Rules of Behavior for "Advertising ID Efficacy Pilot"

May 2020

The following Rules of Behavior will apply to all U.S. Customs and Border Protection (CBP) employees, contractors, and persons utilizing any of the three platforms identified for use in the efficacy pilot regarding the use of commercial telemetry data associated with AdID (referred to herein as "AdID CTD"). Once signed, this agreement is valid for 180 days and users will be required to renew access if access is required.

Hardware and Software Applications:

- I understand that I am given access to only those platforms for which I require access to perform my official duties and for purposes that are consistent with applicable law and policy.
- I will not attempt to use systems or applications that I am not authorized to access, or which violate CBP or DHS policy or guidance.
- I will only access the platform for which I require access to perform mission-related tasks as part of my official duties and for purposes that are consistent with applicable law and policy.
- I will only use approved equipment (government issued/obtained in the course of official duties, stand-alone, etc.) and approved internet connections to access commercial data service applications and web portals.
- I will not attempt to manipulate the commercial platform(s) in any way other than the manner in which the applications are provided by CBP.
- I will log off the platform when I complete an authorized task or before departing the workstation where I logged on.

Privacy and Compliance Protection:

- I understand that I have no expectation of privacy while using the system.
- I understand that I am accountable for my actions through automatic system audit logs that record all actions taken while accessing and using the system.

- I understand that AdID CTD will only be used for the purpose of identifying information relevant to investigating or identifying a criminal violation of a law enforced or administered by CBP and/or a national security concern.
- I understand that AdID CTD may be correlated against public records, open-source data, and/or CBP holdings to identify a specific individual only if there is a reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern.
- I understand that AdID CTD may be used to conduct research on a specific device associated with an individual whose identity is known only if there is reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern.
- I understand that a device-specific query of AdID CTD for a time period greater than 14 days may be conducted only if there is reasonable suspicion of a violation of a criminal law enforced or administered by CBP and/or a national security concern.
- I will protect any personally identifiable information (PII) derived from/or enhanced by, the commercial data research, in accordance with applicable law, including the Privacy Act (where applicable), and CBP and DHS privacy policy.
- I will only collect and use the minimum amount of PII necessary for the defined mission related and official use capacity.
- I will protect sensitive information from disclosure to unauthorized persons or groups.
- I will not retain information describing how a U.S. citizen or lawful permanent resident exercises his or her First Amendment rights, unless such retention is pertinent to and within the scope of an authorized law enforcement activity, expressly authorized by statute, or expressly authorized by the individual about whom the record is maintained.

Non-Compliance:

- I understand that failure to follow these rules will result in consequences for noncompliance, such as verbal or written warnings, removal of system access, reassignment to other duties, disciplinary action, and/or criminal or civil prosecution.
- I further understand that any non-compliance incident may be escalated to a security violation.

Incident Reporting:

I will promptly report suspected or confirmed IT security incidents (e.g., compromise of usernames and passwords or infection with malware, Trojans, or key logging software), as per the DHS Handbook for Safeguarding Sensitive PII and the Privacy Incident Handling Guide (PIHG), and report privacy incidents (e.g. loss or compromise of PII) to my immediate supervisor and/or OPR.

Acknowledgment Statement:

I acknowledge that I have read the above Rules of Behavior, I understand them, and I will comply with them. I understand that failure to comply with these rules could result in a verbal or written warning, removal of system access, and reassignment to other duties, criminal or civil prosecution, or termination.