



U.S. Department of Transportation Privacy Impact Assessment

**Federal Aviation Administration (FAA)
Office of Information and Technology (AIT)
B4UFLY**

Responsible Official

Erik Amend
System Owner
UAShelp@faa.gov
844-FLY-MYUA

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov



Executive Summary

Federal Aviation Administration's (FAA) B4UFLY mobile application provides unmanned hobbyist aircraft operators (hereafter known as "Users") a tool to determine whether it is safe and legal to fly a small Unmanned Aircraft System (sUAS) within their geographic area.¹ B4UFLY does not collect, generate, or maintain Users' Personally-Identifiable Information (PII). However, Users who choose to download B4UFLY from the Apple App Store or the Google Play Store must first fulfill Apple or Google's registration requirements prior to downloading the application which may include the provision of sensitive personal information.

The FAA developed this Privacy Impact Assessment (PIA) to document the steps taken by the FAA to protect B4UFLY Users' privacy when using the geolocation functionality when using the application and when providing information to the Apple App Store or Google Play Store before downloading the B4UFLY mobile application.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for 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 (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.²

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

¹ See Public Law 112-95, Section 336. (Special Rule for Model Aircraft [FAA Modernization Reform Act]).

² Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

Introduction & System Overview

The FAA's mission is "to provide the safest, most efficient aerospace system in the world."³ The B4UFLY mobile application was developed to address increasing reports of unsafe operations of sUAS near airports, over people, and in close proximity to manned aircraft. B4UFLY offers Users a tool to prevent such unsafe operations of their sUAS. B4UFLY also supports the FAA's primary mission of aviation safety by providing Users with situational awareness of where they should and should not fly, and where there might be conflicts within restricted airspace before they fly. The B4UFLY mobile application provides Users a readily-accessible solution that allows Apple iOS and Google Android Users the opportunity to access sUAS flight safety information in real time using their mobile devices.

Prior to the development and release of the B4UFLY mobile application, Users had to gather and analyze flight restriction data from four separate FAA publicly-available data sources to determine if it was safe to fly:

1. The FAA Special Use and Airspace (SUA) website (<https://sua.faa.gov/sua/siteFrame.app>);
2. The FAA Temporary Flight Restriction (TFR) web site (<http://tfr.faa.gov/tfr2/list.html>);
3. The National Airspace Systems Resources (NASR) 56 day subscription service (<https://nfdc.faa.gov/xwiki/bin/view/NFDC/56+Day+NASR+Subscription>); and
4. The UAS 99.7 Flight Restrictions site (<https://faa.maps.arcgis.com/apps/webappviewer/index.html?id=9c2e4406710048e19806ebf6a06754ad>).

The B4UFLY mobile application pulls flight restriction information from these four data sources and packages the information into a user-friendly and intuitive format; improving User's ability to assess the safety and compliance risks of flying. Users who do not wish use the B4UFLY mobile application can continue to gather and analyze the flight restriction data published on these FAA publicly available data sources.

B4UFLY is a free mobile application available for download from the [Apple App Store](#) or [Google Play Store](#) to Apple iOS and Android mobile devices. Users may access these "stores" from links found on the FAA.gov [B4UFLY website](#),⁴ or by going to the stores directly from their mobile device. The FAA does not require Users to register to use the B4UFLY mobile application or to provide any PII as a condition of downloading and using the application. Use of B4UFLY is voluntary. However, Users who download B4UFLY from the Apple App Store or Google Play Store may be required to provide PII to Apple or Google prior to downloading the B4UFLY application. Neither the Apple App Store nor the Google Play Store provide this PII to the FAA. The only data the FAA receives from Apple or Google is the total number of downloads of the B4UFLY application from their stores.

³ See <https://www.faa.gov/about/mission/>.

⁴ The FAA's [B4UFLY website](#) provides a general overview of B4UFLY and its capabilities. Therefore, as a known major entry point to the FAA website, the FAA clearly and conspicuously provides a link to the FAA's privacy policy. (The FAA privacy policy is available at: <https://www.faa.gov/privacy/>).

Upon launching B4UFLY for the first time, Users are requested to permit the B4UFLY application to turn on their mobile device's geolocation capability for the purposes of populating the B4UFLY map with information specific to their location. The geolocation and Global Positioning System (GPS) information is stored locally on the User's devices and is not transmitted to the FAA. Users are not required to turn on their geolocation, but by not doing so; Users will not receive the most accurate flight information. B4UFLY uses the geolocation of the User's mobile device to populate a map and status indicator to inform the User of whether the area in which they are located (or intend to be located) is safe to fly their sUAS. B4UFLY provides Users the following five flight statuses: 1) "Flight Prohibited"; 2) "Warning – Action required"; (3) "User Caution – check restrictions"; (4) "Data Unavailable"; and (5) "Clear". Users are responsible for flying safely, even when B4UFLY indicates that it is "Clear" to fly.

B4UFLY's "Planning Mode" feature supports Users in planning future flights. By manually inputting a flight's anticipated geolocation coordinates and their day/time of flight the User is able to determine if it will be safe to fly in the designated time and place. Users are responsible for verifying the safety of their flight during actual flights. Users can also view surrounding airport locations and other restricted areas based on their geolocation input.

The B4UFLY "[Contact Us](#)" web-form enables Users to contact the FAA directly and provide feedback on B4UFLY's performance and to provide suggestions for improvement. Users are requested to but not required provide the FAA their email address if they wish to engage the FAA to contact them regarding their comments and feedback. The form is submitted outside of B4UFLY and the application does not collect or store any of this information.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provides a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3⁵, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations⁶.

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

⁵ <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

⁶ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf

The FAA does have measures in place to ensure Users are aware of B4UFLY. The FAA.gov B4UFLY website provides Users a general overview of B4UFLY and its capabilities. The B4UFLY Privacy Notice makes potential Users aware that the B4UFLY application does not collect, use, maintain, or disseminate Users' PII.⁷ The publication of this PIA further demonstrates the FAA's commitment to provide notice into B4UFLY. B4UFLY is not a Privacy Act system of records; and therefore, is not subject to any of the Department's published system of records notices.

Users accessing the stores from the FAA website, are presented with a pop-up screen notifying the individual that they are leaving a government website and that the stores are not part of the FAA environment. The warning notice advises Users that once they leave the FAA environment, the FAA cannot guarantee the accuracy or completeness of information presented, that they are subject to the privacy and security policies of the external site's sponsor, and that they are no longer protected by federal privacy law.

Individual Participation and Redress

DOT should provide a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision making process regarding the collection and use of their PII and be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

B4UFLY does not collect personal information, and is not a Privacy Act system of records. Users of the application must follow the protocols for the Apple App Store or Google Play Store for the correction, amendment, or deletion of information pertaining to themselves that was submitted to Apple or Google via their given registration processes. Users must consent to the use of geolocation data for the purposes of populating the B4UFLY map with information specific to their location. This geolocation data transmitted to FAA is not associated with the individual who submits it. Although the geolocation data is not associated with individual Users, Users may withdraw their consent for the use of geolocation data at any time by turning-off the B4UFLY application's geolocation function.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which its collects, uses, maintains, or disseminates PII.

The FAA B4UFLY mobile application is a tool to determine whether it is safe to fly within a geographic area. Geolocation information gathered by the B4UFLY application is not used for any other purpose. The information collected by B4UFLY does not include and is not associated with any PII. Information required to download the app through the Apple App Store or the Google Play Store is not shared with FAA.

⁷ For information regarding how feedback form information collected on the FAA's website through the "Contact Us" link is used, please see the FAA Hotline Information System (FHIS) PIA available at: <https://www.transportation.gov/individuals/privacy/faa-hotline-information-system-fhis>.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

B4UFLY does not collect, use, maintain, or disseminate PII. Although PII is required by the Apple App Store or Google Play Store in order to download B4UFLY, neither Apple nor Google shares PII with the FAA.

FAA maintains only the number of downloads of the B4UFLY application. This information is provided by Apple and Google, and is retained and disposed of in accordance with National Archives and Records Administration (NARA), General Records Schedule (GRS) 3.1, General Technology Management Records. These records are retained in accordance with NARA GRS 3.1, Item 30, and are destroyed 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

FAA does not collect, use, maintain, or disseminate any PII from B4UFLY Users. Users may be requested to provide PII to the Apple App Store or Google Play Store in order to register with them and download B4UFLY. Neither Apple nor Google shares with the FAA the PII collected by them through the Apple App Store or the Google Play Store.

For information regarding the use of the PII from feedback forms, please see the FAA Hotline Information System (FHIS) PIA available at: <https://transportation.gov/privacy>.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

FAA does not collect, use, maintain, or disseminate PII from B4UFLY Users. Users that use links on the FAA.gov B4UFLY website to navigate to the Apple App Store or Google Play Store to download the B4UFLY application are advised that FAA cannot guarantee the accuracy or completeness of information presented on the external sites. If a User finds an error in information pertaining to him or her in the Apple App Store or the Google Play Store, he or she will have to follow the Apple App Store or Google Play Store protocol to update that information. Neither Apple nor Google provides any of this information to the FAA.

Security

DOT shall implement administrative, technical, and physical measures protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The FAA will employ tools to ensure that B4UFLY does not modify the settings of a User's mobile device without the User's consent.

The FAA will perform security analysis for future releases to further safeguard the PII of B4UFLY Users. Both Apple and Google also perform security analyses, independent of the FAA, to ensure that all of their mobile applications do not contain malicious software that will harm Users' mobile devices.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

The FAA's Office of Information & Technology, Information Security & Privacy Service, Security Governance Division is responsible for the administration of FAA Order 1370.121, FAA Information Security and Privacy Program and Policy. FAA Order 1370.121 establishes FAA privacy policies, based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347,) the FISMA, DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance. In addition to these, additional procedures will be consistently applied, especially as they relate to the access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and security privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of B4UFLY consistent with the requirements of OMB Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Erik Amend
System Owner

Approval and Signature

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer